Chapter 5. Modular Arithmetic

5.1 Definitions and Properties of Modular Arithmetic

Congruency

If n is positive and $n|(a-b)$, we say that a is **congruent** to b modulo n and we write $a \equiv b \mod(n)$. If a is not congruent to b modulo n, we write $a \not\equiv b \mod(n)$.

Does $m \geq 2$ here? Why or why not.

Let m, a, and b be three integers, with $m \geq 2$.

DEFINITION 46. a is **congruent to** b **modulo** $m \iff m|(a-b)$. (Equivalently, a and b have the same remainder when divided by m in the Euclidean Algorithm.) The notation for this is "$a \underset{(m)}{\equiv} b$" or "$a \equiv b \pmod{m}$".

Next, "$\underset{(m)}{\equiv}$" respects addition, subtraction, and multiplication: if $a \underset{(m)}{\equiv} b$ and $c \underset{(m)}{\equiv} d$, then:

- $a + c \underset{(m)}{\equiv} b + d$;
- $-c \underset{(m)}{\equiv} -d$ ($\implies a - c \underset{(m)}{\equiv} b - d$); and
- $ac \underset{(m)}{\equiv} bd$.

Repeatedly using these shows also that

- $f(a) \underset{(m)}{\equiv} f(b)$ for any polynomial f with integer coefficients.

Proposition 2.2 (Elementary properties of congruences). *Let $a, b, c, d \in \mathbf{Z}$, $m \in \mathbf{N}$.*

(i) *If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $a + c \equiv b + d \bmod m$.*

(ii) *If $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $ac \equiv bd \bmod m$.*

(iii) *If $a \equiv b \bmod m$, then $a^n \equiv b^n \bmod m$ for any $n \in \mathbf{N}$.*

(iv) *If $a \equiv b \bmod m$, then $f(a) \equiv f(b) \bmod m$ for any polynomial $f(n)$ with integer coefficients.*

(v) *If $a \equiv b \bmod m$, then $a \equiv b \bmod d$ for any positive divisor d of m.*

Theorem 2.1 *Let a, b, c, d denote integers. Then:*

(1) $a \equiv b \pmod m$, $b \equiv a \pmod m$, and $a - b \equiv 0 \pmod m$ are equivalent statements.
(2) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.
(3) If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$.
(4) If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $ac \equiv bd \pmod m$.
(5) If $a \equiv b \pmod m$ and $d \mid m$, $d > 0$, then $a \equiv b \pmod d$.
(6) If $a \equiv b \pmod m$ then $ac \equiv bc \pmod{mc}$ for $c > 0$.

If $a \equiv b \pmod m$ then $a^n \equiv b^n \pmod m$ for all positive integers n.

$ca \equiv cb \pmod m$ if and only if $a \equiv b \pmod{m/(c,m)}$

(v) Show that for any prime p and any $a, b \in \mathbb{Z}$ we have

$$a^p + b^p \equiv (a + b)^p \pmod p.$$

(vi) Show that for any natural number m and any $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{m^n}$, where $n \in \mathbb{N}$, we have $a^m = b^m \pmod{m^{n+1}}$.

Therefore the binomial theorem modulo a prime becomes

$$(a+b)^p = a^p + b^P \pmod{p}$$

The result can easily be extended to the powers of sums of three or more terms:

$$(a_1 + a_2 + \ldots + a_r)^p \equiv a_1^p + a_2^p + \ldots + a_r^p \pmod{p}$$

If we let $a_1 = a_2 = \ldots = a_r = 1$, we obtain Fermat's lesser theorem:

$$r^p \equiv r \pmod{p}$$

THEOREM 4.7 If $ac \equiv bc \pmod{m}$ and $(c, m) = d$, then $a \equiv b \pmod{m/d}$.

THEOREM 4.8 If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_k}$, then $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$.

COROLLARY 4.5 If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_k}$, where the moduli are pairwise relatively prime, then $a \equiv b \pmod{m_1 m_2 \cdots m_k}$. ■

$x \equiv y \pmod{m_i}$ for $i = 1,2, \ldots, r$ if and only if $x \equiv y \left(\mathrm{mod}[m_1, m_2, \ldots, m_r]\right)$.

Theorem 2.3

(1) $ax \equiv ay \pmod{m}$ *if and only if* $x \equiv y \left(\mathrm{mod}\ \dfrac{m}{(a, m)}\right)$.

(2) If $ax \equiv ay \pmod{m}$ *and* $(a, m) = 1$, *then* $x \equiv y \pmod{m}$.

(3) $x \equiv y \pmod{m_i}$ *for* $i = 1, 2, \cdots, r$ *if and only if* $x \equiv y \pmod{[m_1, m_2, \cdots, m_r]}$.

Proof of (3) [Niven, Zuckerman page 16]

Definition 1.4 *The integers $a_1, a_2, \cdots, a_n$, all different from zero, have a common multiple b if $a_i | b$ for $i = 1, 2, \cdots, n$. (Note that common multiples do exist; for example the product $a_1 a_2 \cdots a_n$ is one.) The least of the positive common multiples is called the* least common multiple, *and it is denoted by $[a_1, a_2, \cdots, a_n]$.*

(3) If $x \equiv y \pmod{m_i}$ for $i = 1, 2, \cdots, r$, then $m_i | (y - x)$ for $i = 1, 2, \cdots, r$. That is, $y - x$ is a common multiple of $m_1, m_2, \cdots, m_r$, and therefore (see Theorem 1.12) $[m_1, m_2, \cdots, m_r] | (y - x)$. This implies $x \equiv y \pmod{[m_1, m_2, \cdots, m_r]}$.

If $x \equiv y \pmod{[m_1, m_2, \cdots, m_r]}$ then $x \equiv y \pmod{m_i}$ by Theorem 2.1 part 5, since $m_i | [m_1, m_2, \cdots, m_r]$.

Theorem 1.12 *If b is any common multiple of $a_1, a_2, \cdots, a_n$, then $[a_1, a_2, \cdots, a_n] | b$. This is the same as saying that if h denotes $[a_1, a_2, \cdots, a_n]$, then $0, \pm h, \pm 2h, \pm 3h, \cdots$ comprise all the common multiples of $a_1, a_2, \cdots, a_n$.*

Theorem 2.1 *Let a, b, c, d denote integers. Then:*

(1) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $a - b \equiv 0 \pmod{m}$ are equivalent statements.
(2) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
(3) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
(4) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
(5) If $a \equiv b \pmod{m}$ and $d | m$, $d > 0$, then $a \equiv b \pmod{d}$.
(6) If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$ for $c > 0$.

$x \equiv y \pmod{m_i}$ for $i = 1,2, \ldots, r$ if and only if $x \equiv y \left(\mathrm{mod}[m_1, m_2, \ldots, m_r]\right)$.

Theorem 4. *Let $N = \overline{a_{n-1}\dots a_1 a_0}$ be an n–digit positive integer, where a_0 is the number of units, a_1 be the number of tens, and so on. Then*

(i) $N \equiv a_0 + a_1 + \cdots + a_{n-1} \pmod 3$
(ii) $N \equiv a_0 + a_1 + \cdots + a_{n-1} \pmod 9$
(iii) $N \equiv a_0 - a_1 + \cdots + (-1)^{n-1} a_{n-1} \pmod{11}$
(iv) $N \equiv \overline{a_1 a_0} \pmod 4$, *where* $\overline{a_1 a_0}$ *is the number formed by two last digits of* N
(v) $N \equiv \overline{a_2 a_1 a_0} \pmod 8$, *where* $\overline{a_2 a_1 a_0}$ *is the number formed by three last digits of* N

EXAMPLE 49. Let $n \in \mathbb{N}$, and write $n = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^k a_k$. We have

$$10 \underset{(9)}{\equiv} 1 \implies 10^j \underset{(9)}{\equiv} 1 \implies n \underset{(9)}{\equiv} a_0 + a_1 + \cdots + a_k,$$

so that $9|n \iff 9$ divides the sum of the digits of n. On the other hand,

$$10 \underset{(11)}{\equiv} -1 \implies 10^j \underset{(11)}{\equiv} (-1)^j \implies n \underset{(11)}{\equiv} a_0 - a_1 + \cdots + (-1)^k a_k$$

reveals that $11|n \iff 11$ divides the *alternating* sum of the digits of n.

5.2 Theorems of Fermat, Euler, and Wilson

Theorem
Let p be a prime. A positive integer m is its own inverse modulo p if and only if p divides $m + 1$ or p divides $m - 1$.

Wilson's Theorem
If p is a prime number, then p divides $(p - 1)! + 1$.

Euler's Phi (or Totient) Function

Euler's product formula

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

An equivalent formulation for $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where $p_1, p_2, \ldots, p_r$ are the distinct primes dividing *n*, is:

$$\varphi(n) = p_1^{k_1 - 1}(p_1 - 1)\, p_2^{k_2 - 1}(p_2 - 1) \cdots p_r^{k_r - 1}(p_r - 1).$$

☞ "In order words, $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n." (page 68, textbook)

Section 2.6 Euler's Theorem (pp 68-72)

***Definition* 7** (Euler's Phi Function) Let $n \in \mathbb{Z}$ with $n > 0$. The *Euler phi-function*, denoted $\phi(n)$, is the function defined by

$$\phi(n) = \left| \left\{ x \in \mathbb{Z} : 1 \leq x \leq n; (x, n) = 1 \right\} \right|$$

where $\left| \left\{ \text{set } A \right\} \right|$ is the notation for the cardinality of set A, *i.e.* the number of elements in set A.

☞ "In order words, $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n." (page 68, textbook)

☞ "Note that n will be relatively prime to itself if and only if $n = 1$." (page 68, textbook)

☞ Example 12(c). "If p is a prime number, then *all* positive integers less than p are relatively prime to p. Inasmuch as there are $p - 1$ such numbers, we have $\phi(p) = p - 1$." (page 69, textbook)

***Theorem* 3.3:** Let p be a prime number and let $a \in \mathbb{Z}$ with $a > 0$. Then $\phi(p^a) = p^a - p^{a-1}$.

e.g. $\phi(4) = \phi(2^2) = 2^2 - 2^1$. Check: $2 = 4 - 2$? Yes.

$\phi(8) = \phi(2^3) = 2^3 - 2^2$. Check: $4 = 8 - 4$? Yes.

$\phi(9) = \phi(3^2) = 3^2 - 3^1$. Check: $6 = 9 - 3$? Yes.

***Theorem* 3.4:** Let $n \in \mathbb{Z}$ with $n > 0$. Then

$$\phi(n) = n \cdot \prod_{p|n,\ p \text{ prime}} \left(1 - \frac{1}{p}\right)$$

(TI159) Determine the number of elements of S that are in simplest form if

$$S = \left\{\frac{1}{144}, \frac{2}{144}, \frac{3}{144}, \ldots, \frac{142}{144}, \frac{143}{144}\right\}.$$

Solution

Start by counting the number of numbers from 1 to 143 that have 2 or 3 as a factor. The number that have two as a factor is $\frac{144}{2} - 1 = 71$. *The number that have 3 as a factor is* $\frac{144}{3} - 1 = 47$. *However, note that we have double counted the numbers with 2 and 3 as a factor. There are* $\frac{144}{6} - 1 = 23$. *Thus, we have 143 – 71 – 47 +23 =* $\boxed{48}$ *numbers.*

■

Using Euler's Phi Function:

$$\phi(144) = \phi(2^4 3^2) = 144\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 144\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 48.$$

Euler's Theorem

If m is a positive integer and a is an integer such that $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \ (mod\ m)$$

where ϕ is Euler's ϕ-function.

Fermat's Theorem

If p is a prime and a is a positive integer with $p \nmid a$, then $a^{p-1} \equiv 1 \ (mod\ p)$.

Order of a mod m, written ord$_m$ a

The order of a mod m (with a and m relatively prime) is the smallest positive integer x such that $a^x \equiv 1 \pmod{m}$.

We know from Euler's Theorem that $a^{\phi(m)} \equiv 1 \pmod{m}$ therefore (by definition)

$$\text{ord}_m\ a \leq \phi(m).$$

$$\phi(1132) = 564$$

$$564 = 2^2 \cdot 3^1 \cdot 47^1$$

order$_{1132}$(51)=94

order$_{1132}$(45)=6

order$_{1132}$(29)=47

$$45^6 \bmod(1132) = 1$$

$$29^{47} \bmod(1132) = 1$$

$$47 = 32 + 8 + 4 + 2 + 1$$

$$29^1 \bmod(1132) = 29$$

$$29^2 \bmod(1132) = 841$$

$$29^4 \bmod(1132) = (841 \cdot 841) \bmod(1132) = 913$$

$$29^8 \bmod(1132) = (913 \cdot 913) \bmod(1132) = 417$$

$$29^{16} \bmod(1132) = 693$$

$$29^{32} \bmod(1132) = 281$$

$$29^{47} \bmod(1132) = (29^{32} \cdot 29^8 \cdot 29^4 \cdot 29^2 \cdot 29^1) \bmod(1132)$$

$$= (281 \cdot 417 \cdot 913 \cdot 841 \cdot 29) \bmod(1132)$$

$$= 1$$

Exercises

1) Show that $10! + 1$ is divisible by 11.

2) What is the remainder when $5!\,25!$ is divided by 31?

3) What is the remainder when 5^{100} is divided by 7?

4) Show that if p is an odd prime, then $2(p-3)! \equiv -1(mod\ p)$.

5) Find a reduced residue system modulo 2^m, where m is a positive integer.

6) Show that if $a_1, a_2, \ldots, a_{\phi(m)}$ is a reduced residue system modulo m, where m is a positive integer with $m \neq 2$, then $a_1 + a_2 + \ldots + a_{\phi(m)} \equiv 0\ (mod\ m)$.

7) Show that if a is an integer such that a is not divisible by 3 or such that a is divisible by 9, then $a^7 \equiv a\ (mod\ 63)$.

EXAMPLE 50 (Fast powering algorithm). To compute $5^5 \pmod{11}$, we need not actually compute 5^5 and then apply the Euclidean Algorithm. Rather, apply EA at each step:

$$\begin{aligned}
5^2 &= 25 \underset{(11)}{\equiv} 3 \\
5^3 = 5^2 \cdot 5 &\underset{(11)}{\equiv} 3 \cdot 5 = 15 \underset{(11)}{\equiv} 4 \\
5^4 = 5^3 \cdot 5 &\underset{(11)}{\equiv} 4 \cdot 5 = 20 \underset{(11)}{\equiv} 9 \\
5^5 = 5^4 \cdot 5 &\underset{(11)}{\equiv} 9 \cdot 5 = 45 \underset{(11)}{\equiv} 1.
\end{aligned}$$

But if we want (say) 5^{13}, this is wasteful. Instead, compute

$$5^2 \underset{(11)}{\equiv} 3, \quad 5^4 = (5^2)^2 \underset{(11)}{\equiv} 3^2 = 9, \quad 5^8 = (5^4)^2 \underset{(11)}{\equiv} 9^2 = 81 \underset{(11)}{\equiv} 4$$

$$\implies 5^{13} = 5^{8+4+1} \underset{(11)}{\equiv} 4 \cdot 9 \cdot 5 = 180 \underset{(11)}{\equiv} 4.$$

(In fact, using Fermat's theorem below will give an even faster shortcut.) The general algorithm here for finding $a^e \pmod{m}$ is to write the exponent in binary, compute all the a^{2^i} you need, then multiply them together. This reduces us from computing e multiplications to $\leq 2 \log_2 e$ multiplications mod m.[1]

What is he talking about when he says using the Euclidean algorithm to find $5^5 \bmod 11$?

$$5^5 \bmod 11 = x \Leftrightarrow 5^5 = 11k + x \Leftrightarrow$$

DEFINITION 57. (a) [Euler's phi-function][2] $\phi(m) := |(\mathbb{Z}/m\mathbb{Z})^*| = \#\{a \in \{0,1,\ldots,m-1\} \mid (m,a) = 1\}$.

(b) A **reduced residue system (mod m)** is a set of $\phi(m)$ integers relatively prime to m, with no two in the same mod-m-residue class (e.g. $\{a \in \{0,1,\ldots,m-1\} \mid (m,a) = 1\}$).

Example

2^{29} is a 9-digit integer with distinct digits. What digit (from 0 to 9) does it ***not*** contain? (Source: 2010 Lehigh University High School Math Contest, Problem #34)

Solution

Let $2^{29} = a_8 10^8 + a_7 10^7 + \cdots + a_1 10^1 + a_0$.

Let k be the single digit in $\{0,1,2,\ldots,9\}$ that 2^{29} does not include. Then

$$a_8 + a_7 + \cdots a_1 + a_0 = (9+8+7+6+5+4+3+2+1+0) - k = 45 - k.$$

We know from the divisibility rule for 9 that

$$2^{29} \bmod(9) = (a_8 + a_7 + \cdots a_1 + a_0) \bmod(9) = (45-k) \bmod(9) = (0-k) \bmod(9).$$

We can see that $\gcd(2,9) = 1$ so we can apply Euler's Theorem to determine that

$$2^{\phi(9)} \equiv 1 \bmod(9)$$

where $\phi(9) = 9\left(1 - \frac{1}{3}\right) = 6$. So

$$2^{29} \equiv (2^6)^4 \cdot 2^5 \equiv 1^4 \cdot 2^5 \equiv 32 \equiv 5 \equiv -4 \bmod(9).$$

Hence $-k = -4$ or $k = 4$. That is, the missing digit is 4. Using a calculator (which was not allowed on this contest) we can see that in fact $2^{29} = 536870912$.

■

Example (Source: 2009 Lehigh University High School Math Contest, Problem #17)

What is the remainder when 3^{2009} is divided by 21?

Solution

We cannot directly apply Euler's Theorem as we did in the previous example because the necessary condition $\gcd(3,21) \stackrel{?}{=} 1$ for the theorem to hold is not met.

We can circumvent this problem by using the result

$$x \equiv y \pmod{m_i} \text{ for } i = 1,2,\dots,r \text{ if and only if } x \equiv y \left(\mathrm{mod}[m_1, m_2, \dots, m_r]\right)$$

of the previous chapter.

Notice that $[7,3] = 7 \cdot 3 = 21$ because 7 and 3 are relatively prime. So, it follows from this result that

$$x \equiv y \bmod(21) \Leftrightarrow x \equiv y \bmod(7) \text{ **and** } x \equiv y \bmod(3).$$

Note that $\phi(7) = 6$ and hence $3^6 \equiv 1 \bmod(7)$ by Euler's Theorem. Thus,

$$3^{2009} \bmod(7) \equiv \left((3^6)^{334} \cdot 3^5\right) \bmod(7) \equiv \left(1 \cdot 5\right) \bmod(7) \equiv 5 \bmod(7).$$

And clearly

$$3^{2009} \equiv 0 \bmod(3).$$

But there *appears* to be a problem because to apply the above result we needed $3^{2009} \bmod(7)$ and $3^{2009} \bmod(3)$ to be congruent to the ***same*** value but we found $3^{2009} \bmod(7) \equiv 5$ and $3^{2009} \bmod(3) \equiv 0$.

Fortunately, there is a simple fix. We note that $5 \equiv 12 \bmod(7)$ and $3 \equiv 12 \bmod(3)$. Hence,

$$3^{2009} \equiv 12 \bmod(7) \text{ **and** } 3^{2009} \equiv 12 \bmod(3) \Longrightarrow 3^{2009} \equiv 12 \bmod(21).$$

Therefore, we get a remainder of 12 when we divide 3^{2009} by 21.

■

Note: In the next chapter we will introduce the ***Chinese Remainder Theorem*** which will generalize the approach taken in this last example.

The next example shows that Euler's Theorem is *often* but ***not always*** the best tool for finding $a^b \bmod n$.

Example (Source: 1999 Lehigh University High School Math Contest, Problem #34)

What is the remainder when $6^{83} + 8^{83}$ is divided by 49?

Solution

At first glance it is tempting to see this as an application of Euler's Theorem and to separately find $6^{83} \bmod 49$ and $8^{83} \bmod 49$. But at first glance this also has the appearance of a time-consuming approach because $\phi(49) = 42$ which means

$$6^{83} \bmod 49 = (6^{42} \cdot 6^{41}) \bmod 49 = \left(6^{\phi(49)} \cdot 6^{41}\right) \bmod 49 = 6^{41} \bmod 49$$

and we are still facing the problem of finding $6^{41} \bmod 49$.

Are there any clues for a better approach? If we notice the disguised 7's we can rewrite the problem as

$$\left((7-1)^{83} + (7+1)^{83}\right) \bmod 7^2.$$

This form suggests expanding the binomial terms and looking for cancellation. It also suggests that the remaining terms will involve a factor of 7^j which is convenient when working mod 7^2.

$$\begin{aligned}(7-1)^{83} + (7+1)^{83} &= \sum_{j=0}^{83} \binom{83}{j} 7^j (-1)^{83-j} + \sum_{j=0}^{83} \binom{83}{j} 7^j (1)^{83-j} \\ &= \sum_{j=0}^{83} \binom{83}{j} 7^j \left((-1)^{83-j} + (1)^{83-j}\right) \\ &= \sum_{\substack{j=0 \\ j \text{ odd}}}^{83} \binom{83}{j} 7^j \left((-1)^{83-j} + (1)^{83-j}\right)\end{aligned}$$

$$= \sum_{\substack{j=0 \\ j \text{ odd}}}^{83} \binom{83}{j} 7^j \cdot 2$$

$$= 2\binom{83}{1} 7^1 + 7^3 \sum_{\substack{j=3 \\ j \text{ odd}}}^{83} \binom{83}{j} 7^{j-3} \cdot 2.$$

It follows that

$$\begin{aligned}\left((7-1)^{83} + (7+1)^{83}\right) \bmod 7^2 &= 2\binom{83}{1} 7^1 \bmod 7^2 + 7^3 \sum_{\substack{j=3 \\ j \text{ odd}}}^{83} \binom{83}{j} 7^{j-3} \cdot 2 \bmod 7^2 \\ &= 2\binom{83}{1} 7^1 \bmod 7^2 = 1162 \bmod 7^2 \\ &= 35.\end{aligned}$$

■

THEOREM 60 (Euler). $(a, m) = 1 \implies a^{\phi(m)} \underset{(m)}{\equiv} 1.$

COROLLARY 61 (Fermat's "Little" Theorem). *Let a be an integer, and p a prime not dividing a. Then* $a^{p-1} \underset{(p)}{\equiv} 1.$

2.5 Fermat's Theorem

Theorem 2.14 (Fermat's Little Theorem)**.** *Let p be a prime number. Then, for any integer a satisfying $(a, p) = 1$,*

$$a^{p-1} \equiv 1 \bmod p. \tag{2.5}$$

Corollary 2.15 (Fermat's Little Theorem, Variant)**.** *Let p be a prime number. Then, for any integer a,*

$$a^{p} \equiv a \bmod p. \tag{2.6}$$

Corollary 2.16 (Inverses via Fermat's Theorem)**.** *Let p be a prime number, and let a be an integer such that $(p, a) = 1$. Then $\overline{a} = a^{p-2}$ is an inverse of a modulo p.*

Remark. In contrast to Wilson's Theorem, Fermat's Theorem does not have a corresponding converse; in fact, there exist numbers p that satisfy the congruence in Fermat's Theorem, but which are compositive. Such "false positives" to the Fermat test are rare, but they do exist, movitating the following definition:

Method 2: Fermat's Little Theorem

There are several ways to deal with large exponents more efficiently, one of which is to leverage the so-called **Fermat's Little Theorem** (FLT), which asserts that:

> Given a prime modulus p and any non-zero integer n (i.e., $n \not\equiv 0 \pmod{p}$), we have that $n^{p-1} \equiv 1 \pmod{p}$.

In other words, when the modulus is a *prime* number, any non-zero number, when raised to the *predecessor* of the modulus, will be congruent to 1. While FLT has profound implications in number theory, its immediate usefulness for us is that it allows for fast calculations within *prime* moduli.

For example, since 31 is a prime number, any non-zero number raised to 30 will be congruent to 1 in mod 31 (e.g., $2^{30} \equiv 1 \pmod{31}, 15^{30} \equiv 1 \pmod{31}$). In practice, this means that a big number such as 234^{567} can be reduced in mod 31 as follows:

$$234^{567} \equiv [(31)7 + 17]^{567} \equiv 17^{567} \equiv 17^{(30)18+27} \equiv (17^{30})^{18}17^{27} \equiv 17^{27} \pmod{31}$$

As you can see here, in the case of *prime modulus*, the base can always be reduced so that it is smaller than the modulus, and the exponent smaller than the *predecessor* of the modulus. Once there, we can resort again to brute force to further simplify the expression:

$$17^2 \equiv 289 \equiv 10, 17^4 \equiv 100 \equiv 7, 17^8 \equiv 49 \equiv 18 \pmod{31}$$

$$17^{16} \equiv 324 \equiv 14, 17^{24} \equiv (17^{16})17^8 \equiv (14)18 \equiv 4 \pmod{31}$$

$$17^{26} \equiv (17^{24})17^2 \equiv (4)10 \equiv 9 \pmod{31}$$

$$\therefore 17^{27} \equiv (17^{26})17 \equiv (9)17 \equiv 153 \equiv 29 \pmod{31}$$

That is, $234^{567} \equiv 29 \pmod{31}$!

Before we get overly excited about FLT though, it is to be emphasized that this theorem only works when we have a *prime* modulus. In fact, we even know that the same theorem is *false* if the modulus were *composite*. and the search for more general techniques would lead us to yet another standard trick…

2.6 Euler's Theorem

Definition 2.18 (Reduced residue system)**.** *Let $m \in \mathbf{N}$. A set of integers is called a* ***reduced residue system modulo*** *m, if (i) its elements are pairwise incongruent modulo m, and (ii) every integer n with $(n, m) = 1$ is congruent to an element of the set. Equivalently, a reduced residue system modulo m is the subset of a complete residue system consisting of those elements that are relatively prime with m.*

Definition 2.19 (Euler phi-function)**.** *Let $m \in \mathbf{N}$. The* ***Euler phi-function****, denoted by $\varphi(m)$, is defined by*

$$\varphi(m) = \#\{1 \leq n \leq m : (n, m) = 1\},$$

i.e., $\varphi(m)$ is the number of elements in a reduced system of residues modulo m.

Proposition 2.20. *If $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ is a reduced residue system modulo m, then so is the set $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$, for any integer a with $(a, m) = 1$.*

Theorem 2.21 (Euler's generalization of Fermat's theorem)**.** *Let $m \in \mathbf{N}$. Then, for any integer a such that $(a, m) = 1$,*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{2.7}$$

3.3 The Euler phi function and the Carmichael Conjecture

Definition 3.3 (Euler phi function)**.** *The Euler phi function is defined by*

$$\varphi(n) = \#\{1 \leq m \leq n : (m, n) = 1\}.$$

Proposition 3.4 (Properties of $\varphi(n)$)**.**

(i) *(Multiplicativity) The Euler phi function is multiplicative (though not completely multiplicative).*

(ii) *(Explicit formula) For any $n \in \mathbf{N}$,*

$$\varphi(n) = \prod_{p^\alpha || n} p^{\alpha-1}(p-1) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

2.4 Wilson's Theorem

Theorem 2.12 (Wilson's Theorem)**.** *Let p be a prime number. Then*

$$(p-1)! \equiv -1 \bmod p. \tag{2.4}$$

Theorem 2.13 (Converse to Wilson's Theorem)**.** *If p is an integer ≥ 2 satisfying* (2.4)*, then p is a prime number.*

Remark. The converse to Wilson's Theorem can be stated in contrapositive form as follows: *If n is composite, then $(n-1)!$ is* ***not*** *congruent to -1 modulo n.* In fact, the following much stronger statement holds: *If $n > 4$ and n is composite, then* $(n-1)! \equiv 0 \bmod n$. Thus, for $n > 4$, $(n-1)!$ is congruent to either -1 or 0 modulo n; the first case occurs if and only if n is prime, and the second occurs if and only if n is composite.

Example 8. What is the remainder of the division of $N = 375 \cdot 2^{100} - 35^{87}$ by 6 ?

Solution. Here we stop writing the references to the parts of Theorem 3, but we do use them constantly. All congruences below are modulo 6. We have: $375 \equiv 3 \pmod 6$, $2^{100} = (2^5)^{20} = 32^{20} \equiv 2^{20} = (2^5)^4 = 32^4 \equiv 2^4 = 16 \equiv 4 \pmod 6$. Also, since $35 \equiv -1 \pmod 6$, then $35^{87} \equiv (-1)^{87} = -1 \pmod 6$. Therefore $N = 375 \cdot 2^{100} - 35^{87} \equiv 3 \cdot 4 - (-1) = 13 \equiv 1 \pmod 6$. Since $0 \leq 1 < 6$, the remainder of the division of N by 6 is 1.

To find the remainder of the division of the product $32517 \cdot 5328$ by 14, we can first divide each factor by 14 with remainder, then multiply the obtained remainders, and then divide their product by 14. Using congruences, this can be written as: $32517 \equiv 9 \pmod{14}$, $5328 \equiv 8 \pmod{14}$, and

$$32517 \cdot 5328 \equiv 9 \cdot 8 = 72 \equiv 2 \pmod{14}$$

(here we used (vi) and (viii)).

Example 8. What is the remainder of the division of $N = 375 \cdot 2^{100} - 35^{87}$ by 6 ?

Solution. Here we stop writing the references to the parts of Theorem 3, but we do use them constantly. All congruences below are modulo 6. We have: $375 \equiv 3 \pmod 6$, $2^{100} = (2^5)^{20} = 32^{20} \equiv 2^{20} = (2^5)^4 = 32^4 \equiv 2^4 = 16 \equiv 4 \pmod 6$. Also, since $35 \equiv -1 \pmod 6$, then $35^{87} \equiv (-1)^{87} = -1 \pmod 6$. Therefore $N = 375 \cdot 2^{100} - 35^{87} \equiv 3 \cdot 4 - (-1) = 13 \equiv 1 \pmod 6$. Since $0 \leq 1 < 6$, the remainder of the division of N by 6 is 1.

ELEMENTS OF NUMBER THEORY: LECTURE NOTES, FELIX LAZEBNIK, pg. 12

Exercise Set 3

8. Prove that the sum of squares of three integers cannot give remainder 7 when divided by 8. Are there three integers x, y, z such that $x^2+y^2+z^2 = 23654009839$?

Solution

(8) First investigate what can be a remainder of the division of a square of an integer by 7.

$$23654009839 \bmod 8 \equiv 839 \bmod 8 = (8(104) + 7) \bmod 8 = 7$$

$0^2 \bmod 8 = 0$	$1^2 \bmod 8 = 1$	$2^2 \bmod 8 = 4$
$3^2 \bmod 8 = 1$	$4^2 \bmod 8 = 0$	$5^2 \bmod 8 = 1$
$6^2 \bmod 8 = 4$	$7^2 \bmod 8 = 4$	

But there is no combination of three of {0,1,4} sampling with replacement that can equal 7.

9. Are there integers x, y, z such that $x^3 + y^3 + z^3 = 1234567894$? (*Hint*: Think about the corresponding congruence modulo 9.)

Solution

(9) A hint has already been given. First investigate what can be a remainder of the division of a cube of an integer by 9.

Niven, Zuckermann

8. Prove that any number that is a square must have one of the following for its units digit: $0, 1, 4, 5, 6, 9$.
9. Prove that any fourth power must have one of $0, 1, 5, 6$ for its units digit.

5.3 Largest Integer that Divides Integer Polynomial $f(n)$ for all n

Complete Residue System

A set $A = \{a_1, a_2, \ldots, a_n\}$ of n integers is a **complete residue system** mod(n) if every integer in $\mathbb{Z}$ is congruent mod(n) to exactly one of the a_j's in A.

Equivalently, the set $A = \{a_1, a_2, \ldots, a_n\}$ of n integers is a complete residue system $(\text{mod } n)$ if each element of A mod(n) is distinct. That is, $n \nmid |a_j - a_i|$ for any $1 \leq i < j \leq n$.

Theorem. Every set of n consecutive integers is a complete residue system mod(n).

Proof

Consider the set $A = \{a_1, a_2, \ldots, a_n\} = \{c+1, c+2, c+3, \ldots, c+n\}$ for integers c and n. In this case for any $1 \leq i < j \leq n$, we have

$$|a_j - a_i| = |(c+j) - (c+i)| = |j - i| < n.$$

Hence, $n \nmid |a_j - a_i|$.

■

As a particular example of this theorem, the set of integers $A = \{0,1,2, \ldots, n-1\}$ is a complete residue system mod(n). The set $\{0,1,2, \ldots, n-1\}$ is generally referred to as the set of **least nonnegative residues** mod(n).

Theorem. For all integers c and all integers $n > 0$, exactly one of the consecutive integers $\{c+1, c+2, c+3, \ldots, c+n\}$ is divisible by n.

Proof

By the previous theorem, the set of integers $A = \{a_1, a_2, \ldots, a_n\} = \{c+1, c+2, c+3, \ldots, c+n\}$ is a complete residue system mod(n). Hence (exactly) one of these elements is congruent to 0 mod(n). That is $n|(a_j - 0)$ for exactly one of the elements in $A = \{a_1, a_2, \ldots, a_n\}$.

In other words, $n|(c+j)$ for exactly one $j \in \{1,2, \ldots, n\}$.

■

Theorem $(n+1)(n+2)\cdots(n+k)$ is divisible by $k!$ for all integers $n \geq 0$ and $k \geq 1$.

Proof

$$\frac{(n+1)(n+2)\cdots(n+k)}{k!} = \frac{n! \cdot (n+1)(n+2)\cdots(n+k)}{n! \cdot k!}$$

$$= \frac{(n+k)!}{n! \cdot k!} = \binom{n+k}{k}.$$

But we know that the binomial coefficient $\binom{n+k}{k}$ equals the number of ways to select k objects without replacement from a set of $n+k$ distinct objects and is necessarily a positive integer. That is $k!\,|(n+1)(n+2)\cdots(n+k)$.

■

If gcd$(6,n) = 1$, then $n^2 - 1$ is divisible by 24.

Proof

$$\gcd(6,n) = 1 \Longrightarrow n = 6k+1 \text{ or } 6k+5.$$

Case 1. $n = 6k+1$. Then $n^2 - 1 = (36k^2 + 12k + 1) - 1 = 12k(3k+1)$. If k is even then k is divisible by 2. If k is odd, then $3k+1$ is divisible by 2. So in general, $k(3k+1)$ is divisible by 2 and hence $n^2 - 1 = 12k(3k+1)$ is divisible by 24.

Case 2. $n = 6k+5$. Then $n^2 - 1 = (36k^2 + 60k + 25) - 1 = 12(3k^2 + 5k + 2) = 12(3k+2)(k+1)$. If k is even then $3k+2$ is divisible by 2. If k is odd then $k+1$ is divisible by 2. So in general, $(3k+1)(k+1)$ is divisible by 2 and hence $n^2 - 1 = 12(3k+1)(k+1)$ is divisible by 24.

■

Note that from the previous result it follows immediately that $p^2 - 1$ is divisible by 24 for all prime $p > 3$.

Furthermore, it also follows that $p^2 - q^2$ is divisible by 24 for all prime $p, q > 5$.

> $p^2 - q^2 = (p^2 - 1) - (q^2 - 1)$ and because 24 divides both $p^2 - 1$ and $q^2 - 1$ it must divide their difference.

■

Example

2. (AHSME 1960) Let m and n be any two odd numbers, with n less than m. What is the largest integer which divides all possible numbers of the form $m^2 - n^2$?

Solution

First, factor the difference of squares.

$$(m+n)(m-n)$$

Since m and n are odd numbers, let $m = 2a + 1$ and $n = 2b + 1$, where a and b can be any integer.

$$(2a + 2b + 2)(2a - 2b)$$

Factor the resulting expression.

$$4(a + b + 1)(a - b)$$

If a and b are both even, then $a - b$ is even. If a and b are both odd, then $a - b$ is even as well. If a is odd and b is even (or vise versa), then $a + b + 1$ is even. Therefore, in all cases, 8 can be divided into all numbers with the form $m^2 - n^2$.

This can be confirmed by setting $m = 3$ and $n = 1$, making $m^2 - n^2 = 9 - 1 = 8$. Since 8 is not a multiple of 3 and is less than 16, we can confirm that the answer is $\boxed{\textbf{(D)}}$.

■

Example (Source: 2022 Lehigh University High School Math Contest, Problem #4)

Find the prime number p such that $p^2 - 1$ has exactly 10 divisors (including 1 and $p^2 - 1$)?

Solution

Suppose the prime factorization of $p^2 - 1$ is $p^2 - 1 = 2^a 3^b 5^c 7^d 11^e \cdots$. Then

$p \neq 2$ and $p \neq 3$ because neither $2^2 - 1 = 5$ nor $3^2 - 1 = 8$ have 10 factors. Therefore, by the previous example, $p^2 - 1$ is divisible by $24 = 2^3 \cdot 3^1$.

Therefore, the prime factorization has the form

$$p^2 - 1 = 2^{3+a}3^{1+b}5^c7^d11^e \cdots$$

where $a, b, c, d, e, \cdots$ are nonnegative integers.

From this factorization and hence $p^2 - 1$ has $(3 + a + 1)(1 + b + 1)(c + 1)(d + 1)(e + 1) \cdots$ factors. But we are told that $p^2 - 1$ has $10 = 2 \cdot 5$ factors.

Thus,

$$2 \cdot 5 = (4 + a)(2 + b)(c + 1)(d + 1)(e + 1) \cdots$$

for some nonnegative integers $a, b, c, d, e, \cdots$. Clearly the only possibility is $a = 1, b = c = d = \cdots = 0$.

That is, $p^2 - 1 = 2^4 3 = 48$. Thus, $p^2 = 49$ and $p = 7$.

■

Example

Both $2n$ and $2n + 2$ are divisible by 2 and exactly one of $2n$ and $2n + 2$ is divisible by 4.

Proof

Clearly both $2n$ and $2n + 2$ are divisible by 2.

Now consider $(2n) \bmod (4)$

Suppose n is odd. Then $2n = 2(2k + 1) = 4k + 2$ and $(2n) \bmod (4) = 2$. And in this case $(2n + 2) \bmod (4) = 0$. That is, $(2n + 2)$ is divisible by 4.

Suppose n is even. Then $2n$ is divisible by 4. And in this case $(2n + 2) \bmod (4) = 2$.
So, exactly one of $2n$ and $2n + 2$ is divisible by 4.

■

Find the largest positive integer b such that

$$f(n) = n(2n + 1)(n^2 - 1)(4n^2 + 4n)$$

is divisible by b for all integers $n > 1$.

Solution

We can rewrite $f(n)$ as

$$f(n) = 4 \cdot \big((n-1)n(n+1)\big) \cdot \big(n(n+1)(2n+1)\big) = 4 \cdot g(n) \cdot h(n).$$

First note that $g(n) = (n-1)n(n+1)$ is the product of 3 consecutive integers and hence is divisible by both 2 and 3.

Second, note that exactly one of the two factors n and $(n+1)$ in $h(n)$ must be divisible by 2 because they are consecutive.

Finally, we I claim that exactly one of the three factors n, $(n+1)$ and $(2n+1)$ in $h(n)$ must be divisible by 3. To see why, consider the three cases for $n \bmod(3)$ separately.

If $n \equiv 0 \bmod(3)$, then n is divisible by 3 while $(n+1)$ and $(2n+1)$ are not.

If $n \equiv 1 \bmod(3)$, then $(2n+1)$ is divisible by 3 while n and $(n+1)$ are not.

If $n \equiv 2 \bmod(3)$, then $(n+1)$ is divisible by 3 while n and $(2n+1)$ are not.

Therefore, in all cases exactly on of the factors n, $(n+1)$ and $(2n+1)$ is divisible by 3.

We have now shown that

$$f(n) = 4 \cdot \underbrace{\big((n-1)n(n+1)\big)}_{\text{divisible by 2 and 3}} \cdot \underbrace{\big((n-1)n(n+1)\big)}_{\text{divisible by 2 and 3}}.$$

Thus, $f(n)$ is always divisible by $b = 4 \cdot (2 \cdot 3) \cdot (2 \cdot 3) = 144$.

■

Mu Alpha Theta National Convention 2004, Number Theory Test, Alpha Division, Problem #18

Find the largest integer that evenly divides $n^5 - 5n^3 + 4n$ for all integers n.

A. 24 B. 60 C. 120 D. 240 E. NOTA

Solution

18. **C** Since $n^5 - 5n^3 + 4n = (n-2)(n-1)(n)(n+1)(n+2)$, we know the product is divisible by 3, 5, and 8. (Note that for $n = 3$, our product equals 120.)

■

Open Number Theory **MAθ National Convention 2015**

21) Find the largest integer that evenly divides $n^5 - 5n^3 + 4n$ for all integers n.

A) 24 B) 60 C) 120 D) 240 E) NOTA

Solution

21. C: Since $n^5 - 5n^3 + 4n = n(n-2)(n-1)(n+1)(n+2)$, the product will be divisible by 3,5, and 8.

■

27) For integers B and C, if $(B+2)(C+3)$ is even, then $4BC$ must be divisible by:

A) 4 B) 8 C) 9 D) 12 E) NOTA

Solution

27. A: Since $(B+2)(C+3)$ is even, either $(B+2)$ is even, which implies B is even, or $(C+3)$ is even, which implies C is odd. If B is even, then the product $4BC$ is divisible by at least 8. If C is odd (and assuming B is odd as well), then the only factors of 2 in the product $4BC$ would come from 4. Thus, 4 is the only factor that must be a factor of $4BC$

■

What is the largest integer that divides $n^6 - n^2$, for all integers n.

Solution

$$n^6 - n^2 = n^2(n^4 - 1) = n^2(n^2 - 1)(n^2 + 1) = n^2(n-1)(n+1)(n^2+1).$$

We first notice that 2 is a divisor of $n^6 - n^2$ for all n because the two successive numbers $(n-1)$ and n both divide $n^6 - n^2$.

Then we notice that 3 is a divisor for all n because the three successive numbers $(n-1), n$ and $(n+1)$ each divide $n^6 - n^2$.

Also 4 is a divisor for all n because 2 divides $n(n-1)$ and 2 divides $n(n+1)$. Therefore, 4 divides $n(n-1) \cdot n(n+1) = n^2(n-1)(n+1)$.

From Fermat's Theorem we know that for all prime $p \nmid n$, $n^{p-1} \equiv 1 \pmod{p}$. This means that $p|(n^{p-1} - 1)$ for all prime $p \nmid n$.

Therefore $5|(n^4 - 1)$ for all n such that $5 \nmid n$. But $n^6 - n^2 = n^2(n^4 - 1)$ and hence it follows that $5|(n^6 - n^2)$ for all n such that $5 \nmid n$.

But what is $5|n$? That is, $n = 5k$ for some integer k. In this case

$$n^6 - n^2 = n^2(n^4 - 1) = (5k)^2\left((5k)^4 - 1\right)$$

which is divisible by 5. So $5|(n^6 - n^2)$ for all n.

We have shown that $3, 4$ and 5 all divide $n^6 - n^2$ for all n. Therefore $3 \times 4 \times 5 = 60$ divides $n^6 - n^2$ for all n.

■

What is the largest integer which must evenly divide all integers of the form $n^5 - n$?
https://math.stackexchange.com/questions/1622741/what-is-the-largest-integer-which-must-evenly-divide-all-integers-of-the-form-n

Find the largest natural number m such that $n^3 - n$ is divisible by m for all n.
https://math.stackexchange.com/questions/948511/find-the-largest-natural-number-m-such-that-n3-n-is-divisible-by-m-for-all-n

Find the largest number that $n(n^2 - 1)(5n + 2)$ is always divisible by.
https://math.stackexchange.com/questions/4185314/find-the-largest-number-that-nn2-15n2-is-always-divisible-by

Prove that 2730 divides $n^{13} - n$ for all integers n.
https://math.stackexchange.com/questions/1387239/prove-that-2730-divides-n13-n-for-all-integers-n

Problem 1 (Homework) *Prove that in every Pythagorean triple (a, b, c) at least one of the numbers a, b, c is divisible by 5.*

All the conjectures formulated above are true for all primitive Pythagorean triples. The reader is invited to prove them all.

Exactly one of x, y is divisible by 3.
Exactly one of x, y is divisible by 4.
Exactly one of x, y, z is divisible by 5.
The largest number that always divides xyz is 60.

Saint Mary's College Mathematics Contest Problems
48. Take any number in base 5. Rearrange the digits and find the difference between the original number and the rearranged number. What is the largest integer that ALWAYS divides the difference?
Solution

Niven

13. Prove that $n^2 - n$ is divisible by 2 for every integer n; that $n^3 - n$ is divisible by 6; that $n^5 - n$ is divisible by 30.

14. Prove that if n is odd, $n^2 - 1$ is divisible by 8.

Theorem 1.21 *The product of any k consecutive integers is divisible by k!.*

26. Show that the product of three consecutive integers is divisible by 504 if the middle one is a cube.

2. (a) If 1 is added to a product of twin primes, prove that a perfect square is always obtained.

(b) Show that the sum of twin primes p and $p + 2$ is divisible by 12, provided that $p > 3$.

Total Gadha's Complete Book of

NUMBER SYSTEM

If n is an odd natural number, what is the highest number that always divides $n \times (n^2 - 1)$?

Answer: $n \times (n^2 - 1) = (n - 1) \times n \times (n + 1)$, which is a product of three consecutive numbers. Since n is odd, the numbers (n – 1) and (n + 1) are both even. As they are two consecutive even numbers one of these numbers will be a multiple of 2 and the other will be a multiple of 4. Hence, their product is a multiple of 8. Since one out of every three consecutive numbers is a multiple of 3, one of the three numbers will be a multiple of three. Hence, the product of three numbers will be a multiple of $8 \times 3 = 24$.

Hence, the highest number that always divides $n \times (n^2 - 1)$ is 24.

For every natural number n, the highest number that $n \times (n^2 - 1) \times (5n + 2)$ is always divisible by is
(a) 6 (b) 24 (c) 36 (d) 48

Answer:
Case 1: If n is odd, $n \times (n^2 - 1)$ is divisible by 24 as proved in the earlier question.

Case 2: If n is even, both (n − 1) and (n + 1) are odd. Since product of three consecutive natural numbers is always a multiple of 3 and n is even, the product $n \times (n^2 - 1)$ is divisible by 6. Since n is even 5n is even. If n is a multiple of 2, 5n is a multiple of 2 and hence 5n + 2 is a multiple of 4. If n is a multiple of 4, 5n + 2 is a multiple of 2. Hence, the product $n \times (5n + 2)$ is a multiple of 8.

Hence, the product $n \times (n^2 - 1) \times (5n + 2)$ is a multiple of 24.

Five Hundred Mathematical Challenges, Barbeau, Klamkin, Moser, Problem #333
Prove that, for all natural numbers n, $2^{2n} + 24n - 10$ is divisible by 18.
Solution

Second solution (direct). The quantity is obviously divisible by 2. Computing modulo 9 we have

$$2^{2n} + 24n - 10 \equiv (3-1)^{2n} + 6n - 1$$
$$\equiv (-2n \cdot 3 + 1) + 6n - 1 = 0.$$

and hence

$$2^{2n} + 24n - 10 \equiv 0 \pmod{18}.$$

$$(3-1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} 3^i (-1)^{2n-i}$$

$$= \binom{2n}{0} 3^0 (-1)^{2n} + \binom{2n}{1} 3^1 (-1)^{2n-1} + \sum_{i=2}^{2n} \binom{2n}{i} 3^i (-1)^{2n-i}$$

$$= \binom{2n}{0} 3^0 (-1)^{2n} + \binom{2n}{1} 3^1 (-1)^{2n-1} + 9 \sum_{i=2}^{2n} \binom{2n}{i} 3^{i-2} (-1)^{2n-i}$$

$$= 1 + \big(-3(2n)\big) + 9 \sum_{i=2}^{2n} \binom{2n}{i} 3^{i-2} (-1)^{2n-i}$$

$$= 1 - 6n + 9\sum_{i=2}^{2n} \binom{2n}{i} 3^{i-2}(-1)^{2n-i}$$

■

2008 Mu Alpha Theta National Convention **Open Number Theory**

22. How many positive values of k satisfy the following condition?
For any integer x, at least one of x, x^2-1, x^2+1 must be divisible by k.

A. 0 B. 1 C. 2 D. 4 E. NOTA

Solution

22. **D**. First of all, it is trivially true that they are all divisible by 1. Then, since $x^2-1=(x-1)(x+1)$, $(x-1)\mid(x^2-1)$ and since x and $(x-1)$ are consecutive, at least one must be divisible by 2. Similar argument for 3: $x-1, x, x+1$. Finally, since $x(x^2-1)(x^2+1)=x^5-x$ and $x \equiv x^5 \bmod 5$, that product must be divisible by 5, and since 5 is prime, at least one of the 3 terms must be divisible by 5. So there are 4 values of k: 1, 2, 3, 5.

Fermat's Theorem

If p is a prime and a is a positive integer with $p \nmid a$, then $a^{p-1} \equiv 1 \ (mod\ p)$.

Because 5 is prime, it follows from Fermat's Theorem that $x^4 \equiv 1 \pmod 5$ for all $x \nmid 5$. Therefore, $x^5 \equiv x \pmod 5$ for $x \nmid 5$ But we can also see that $x^5 \equiv x \pmod 5$ when $x|5$ because they both sides equal $0 \pmod 5$.

So, it is immediate from Fermat's Theorem that $a^p \equiv a \pmod p$ for all positive integer a and all p prime.

Consequently, $p|(a^p - a)$ for all positive integer a and all p prime.

■

5.4 Last Digits Problems

The last 3 digits of $(456789)^{5432}$ are the same as the last 3 digits of $(789)^{5432}$ because

$$(456789)^{5432}\,\mathrm{mod}(1000) = (456000+789)^{5432}\,\mathrm{mod}(1000)$$

$$= \left(\sum_{j=0}^{5432}\binom{5432}{j}(456\cdot 10^3)^j(789)^{5432-j}\right)\mathrm{mod}(1000)$$

$$= \sum_{j=0}^{5432}\left(\binom{5432}{j}(456\cdot 10^3)^j(789)^{5432-j}\,\mathrm{mod}(1000)\right)$$

$$= \binom{5432}{0}(456\cdot 10^3)^0(789)^{5432-0}\,\mathrm{mod}(1000)$$

$$+\sum_{j=1}^{5432}\left(\binom{5432}{j}(456\cdot 10^3)^j(789)^{5432-j}\,\mathrm{mod}(1000)\right)$$

$$= (789)^{5432}\,\mathrm{mod}(1000)$$

$$+\sum_{j=1}^{5432}\left(\binom{5432}{j}(456)^j(10^3)^{j-1}(789)^{5432-j}\cdot 1000\cdot \mathrm{mod}(1000)\right)$$

$$= (789)^{5432}\,\mathrm{mod}(1000) + \sum_{j=1}^{5432}(0) = (789)^{5432}\,\mathrm{mod}(1000).$$

■

(TT012)

2. If $(2137)^{753}$ is multiplied out, what will be the units digit in the final product?

Solution

For those who know modular arithmetic,

$(2137)^{753} \equiv 7^{753} \mod 10$

$\equiv (7^4)^{188} \cdot 7 \equiv (2401)^{188} \cdot 7$

$\equiv 1^{188} \cdot 7 \equiv 7 \mod 10$

Otherwise,

$[213(10)+7]^{753}$ expanded by the binomial thm

$= [213(10)]^{753} + 753[213(10)]^{752} \cdot 7 + \cdots$

$+ 753[213(10)] \cdot 7^{752} + 7^{753}$

All but the last term end in 0, so we only need to worry about 7^{753}, and as above $7^{753} = (2401)^{188} \cdot 7$ which ends in $1 \cdot 7$

■

Example

Find the ten's digit t and the unit's digit u for the number 7^{55} when written in standard notation. (Source: MSHSML 1t024)

Solution

The problem of finding the last digit(s) of a number of the form a^r comes up regularly. A general approach is to look for a pattern in the final digits in the initial cases $a^1, a^2, a^3, a^4, \ldots$.

In this problem notice that $7^1 = 7, 7^2 = 49, 7^3 = 343, 7^4 = 2301, \ldots$.

We could continue but the result $7^4 = 2301$ looks "special" because it ends in the last two digits "01". Why is this special? Because $(\cdots 01) \times (\cdots 01)$ ends with $(\cdots 01)$ again. Why? Consider $\cdots dcba01 \times \cdots dcba01$.

$$\cdots dcba01 \times \cdots dcba01 = (\cdots dcba00 + 1) \times (\cdots dcba00 + 1)$$

$$= (\cdots dcba)^2 \cdot 10^4 + 2(\cdots dcba) \cdot 10^2 + 1$$

$$= \left((\cdots dcba)^2 \cdot 10^4 + 2(\cdots dcba)\right) \cdot 10^2 + 1$$

It follows that the last two digits of $(7^4)^k$ are "01" for every $k = 1,2,3, \ldots$.

Furthermore, by the same sort of argument the last two digits of $(\cdots 01) \times (\cdots ab)$ are "ab".

Therefore,

$$7^{55} = (7^4)^{13} \cdot 7^3 = (\cdots 01) \times (\cdots 43) = (\cdots 43).$$

Therefore, the last two digits of 7^{55} are "43". That is $t = 4$ and $u = 3$.

■

2.5.1 Application of Fermat's Little Theorem to Finding the Last Digit of a^b

If you remember, we found the last digits in Section 2.4, but we did it empirically. Here we will apply Fermat's Little Theorem to finding the last digit or the last two digits of "big" numbers.

Problem 99

What is the last digit of 2^{1995}?

Problem 102

Find the remainder of $2^{7^{2018}}$ divided by 352.

Solution. This problem can be rewritten using congruence as

$$2^{7^{2018}} \equiv x \,(mod 352)\,, \quad 0 \leq x < 352. \tag{2.37}$$

2.6.1 Application of the Euler's Formula to Finding the Last Digits of a^b

Problem 103

What are the last two digits of 2^{2009}?

Solution. First we will find the last digits of the numbers using Theorem 13:

$$\begin{aligned} 2^4 &\equiv 1 \pmod 5 \\ (2^4)^{502} &\equiv 1 \pmod 5 \\ 2^1 &\equiv 2 \pmod 5 \\ 2^{2009} &\equiv 2 \pmod 5. \end{aligned}$$

Hence, the last digit of 2^{2009} is 2.

■

(1T844)

Find the last two integers of 1983^{1984}.

Solution

Much work can be avoided by those who know a little modular arithmetic:

$1983 = 83 \bmod 100$

Euler's Theorem says $83^{\phi(100)} = 83^{40} = 1 \bmod 100$

$(1983)^{1984} = (1983^{40})^{49}(1983)^{24} = (83^{40})^{49}(83)^{24} = 83^{24} \bmod 100$

Now use $(83)^2 = 6889 = 89 \bmod 100$; similarly, $89^2 = 21 \bmod 100$;

$(21)^2 = 41 \bmod 100$; $41^3 = 21 \bmod 100$

Then $83^{24} = [83^2]^{12} = [89^2]^6 = [21^2]^3 = 41^3 = 21 \bmod 100$

■

(1T855)

5. Find the last two digits of 19^{85}.

Solution

Those who know Euler's Theorem will write $19^{\phi(100)} \equiv 1 \bmod 100$. Since $\phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$, we see that

$19^{85} = 19^{40} \cdot 19^{40} \cdot 19^{5} \equiv 19^{5} \bmod 100$

(a) $19^2 = 361 \equiv 61 \bmod 100$

(b) $19^5 = 19^2 \cdot 19^2 \cdot 19 \equiv 61 \cdot 61 \cdot 19 \equiv 99 \bmod 100$

Those struggling through life without modular arithmetic and Euler will (until they remedy this defect) have to make multiple computations of the form on lines (a) and (b)

■

(TI854)

4. What are the last two digits of $(1983)^{1962}$?

Solution

$1983 \equiv 83 \bmod 100$. Since 83 is prime, $83^{\phi(100)} \equiv 1 \bmod 100$

$\phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 40.$

$(83)^{1962} = \left[(83)^{40}\right]^{49} \cdot (83)^2 \equiv (83)^2 \bmod 100$

$\equiv 89 \bmod 100$

■

(5D084)

4. Let $k = 2^{2009} + 2009^2$. Compute the units digit (ones' place) of $k^{2009} + 2009^k$.

Solution

The units digit of the powers of 2 *repeat in the cycle* 2, 4, 8, 6, ... *Since* $2009 \equiv 1 \bmod 4$, *and* 2009^2 *ends in a* 1, ***k****'s units digit is* 3. *Now consider* $(.....3)^{2009} + 2009^{(.....3)}$.

The units digit of the powers of 3 *repeat in the cycle* 3, 9, 7, 1, ... *Since* $2009 \equiv 1 \bmod 4$, $(.....3)^{2009}$ *ends in a* 3. *The units digit of* 2009^k *is* 9, *since k is odd.* 3 + 9 ends in a **2**.

■

5.5 Modular Exponentiation

Modular Exponentiation

Modular exponentiation is a less efficient method for determining the remainder when b^n is divided by m. It is based on the binary representation of $n = (n_k n_{k-1} \ldots n_1 n_0)_{\text{two}}$, successive squaring, the least residue of b^{n_i}, where $0 \leq i \leq k$, and Theorems 4.4 and 4.5:

$$b^n = b^{n_k 2^k + n_{k-1} 2^{k-1} + \cdots + n_0} \equiv b^{n_k 2^k} \cdot b^{n_{k-1} 2^{k-1}} \cdots b^{n_0} \pmod{m}$$

The following example illustrates this method.

EXAMPLE 4.10 Compute the remainder when 3^{247} is divided by 25.

SOLUTION

First, notice that $247 = 11110111_{\text{two}}$. Now find the least residues of 3^2 and its successive squares modulo 25:

$$\begin{aligned} 3^2 &\equiv 9 \pmod{25} & 3^4 = 9^2 &\equiv 6 \pmod{25} \\ 3^8 \equiv 6^2 &\equiv 11 \pmod{25} & 3^{16} \equiv 11^2 &\equiv 21 \pmod{25} \\ 3^{32} \equiv 21^2 &\equiv 16 \pmod{25} & 3^{64} \equiv 16^2 &\equiv 6 \pmod{25} \\ 3^{128} \equiv 6^2 &\equiv 11 \pmod{25} \end{aligned}$$

(128 is the largest power of 2 contained in 247.)

Then

$$\begin{aligned} 3^{247} &= 3^{128+64+32+16+4+2+1} \\ &= 3^{128} \cdot 3^{64} \cdot 3^{32} \cdot 3^{16} \cdot 3^4 \cdot 3^2 \cdot 3^1 \\ &\equiv 11 \cdot 6 \cdot 16 \cdot 21 \cdot 6 \cdot 9 \cdot 3 \pmod{25} \\ &\equiv 11 \cdot (6 \cdot 16) \cdot 21 \cdot (6 \cdot 9) \cdot 3 \pmod{25} \\ &\equiv [11 \cdot (-4)] \cdot [(-4) \cdot 4] \cdot 3 \equiv 6 \cdot 9 \cdot 3 \equiv (6 \cdot 9) \cdot 3 \pmod{25} \\ &\equiv 4 \cdot 3 \equiv 12 \pmod{25} \end{aligned}$$

Thus, 12 is the desired remainder. ■

The amount of work in such a problem can be greatly reduced if we introduce negative residues, as the following example shows.

EXAMPLE 4.11 Find the remainder when 3^{181} is divided by 17.

SOLUTION

We have

$$\begin{aligned} 3^2 &\equiv 9 \pmod{17} & 3^4 &\equiv -4 \pmod{17} & 3^8 &\equiv -1 \pmod{17} \\ 3^{16} &\equiv 1 \pmod{17} & 3^{32} &\equiv 1 \pmod{17} & 3^{64} &\equiv 1 \pmod{17} \\ 3^{128} &\equiv 1 \pmod{17} \end{aligned}$$

Therefore:

$$\begin{aligned} 3^{181} &= 3^{128} \cdot 3^{32} \cdot 3^{16} \cdot 3^4 \cdot 3^1 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 13 \cdot 3 \pmod{17} \\ &\equiv 5 \pmod{17} \end{aligned}$$

Thus, the desired remainder is 5. ■

Find the least positive residue of 12^{345} in mod 35.

Method 1: Brute-Force Attack

Without any sophisticated mathematical machinery, the conceptually-easiest approach is just to calculate the powers of 12 — incrementally — until we get to 12^{345}. Sounds easy enough? Let's jump in and give it a try!

$$12^2 \equiv 144 \equiv 144 - 4(35) \equiv 4 \pmod{35}$$

$$12^3 \equiv (12^2)12 \equiv (4)12 \equiv 48 \equiv 13 \pmod{35}$$

$$12^4 \equiv (12^2)^2 \equiv 4^2 \equiv 16 \pmod{35}$$

$$12^5 \equiv (12^3)12^2 \equiv (13)4 \equiv 52 \equiv 17 \pmod{35}$$

$$12^6 \equiv (12^2)(12^2)(12^2) \equiv (4)(4)(4) \equiv 64 \equiv -6 \pmod{35}$$

$$12^7 \equiv (12^6)12 \equiv (-6)12 \equiv -72 \equiv -2 \pmod{35}$$

Ouf… Finally we get some small numbers! Can we do better though? Yes! In fact, we can prove that *in this case*, we will eventually get to 1 (this is due to the fact that because 12 is coprime with the modulus 35). However, there is a catch — we actually don't know when that will happen! We can, of course, proceed with computations and just pray for its prompt occurrence:

$$12^8 \equiv (12^7)12 \equiv (-2)12 \equiv -24 \equiv 11 \pmod{35}$$

$$12^9 \equiv (12^7)(12^2) \equiv (-2)(4) \equiv -8 \pmod{35}$$

$$12^{10} \equiv (12^7)(12^3) \equiv (-2)(13) \equiv -26 \equiv 9 \pmod{35}$$

$$12^{11} \equiv (12^7)(12^4) \equiv (-2)(16) \equiv -32 \equiv 3 \pmod{35}$$

$$12^{12} \equiv (12^{11})12 \equiv (3)12 \equiv 36 \equiv 1 \pmod{35}$$

Thank goodness! Looks like that we are lucky this time! By the way, there is a reason why we didn't skip the exponents (for example, we could have calculated 12^8 from 12^4 directly quite easily), but let's solve our original question first shall we?

$$12^{345} \equiv 12^{12(28)+9} \equiv (12^{12})^{28}12^9 \equiv (1)^{28}(-8) \equiv -8 \equiv 27 \pmod{35}$$

See… if we skipped the exponents, would we have known that $12^9 \equiv -8$? 😉

■

Saint Mary's College Mathematics Contest Problems

284. What powers of 2 give a remainder of 15 when divided by 17 ?

Solution

■

Mu Alpha Theta National Convention 2002, Number Theory Test, Alpha Division, Problem # 24

For how many positive integers m less than 1000 is $m^{3^{10}-3^9} - 1$ by 3^{10} ?

Solution

24. **B** Clearly no m which are multiples of 3 can have powers which are only 1 more than a multiple of 3^{10}. For other m, we use Euler's generalization of Fermat's Theorem since $(m, 3^{10}) = 1$:

$$m^{\phi(3^{10})} \equiv 1 \pmod{3^{10}}$$

Since $\phi(3^{10}) = 3^{10}(1 - 1/3) = 3^{10} - 3^9$, we have

$$m^{3^{10}-3^9} \equiv 1 \pmod{3^{10}}$$

for all $m < 1000$ which are not divisible by three. There are $2/3(999) = 666$ such integers.

■

5.6 Towers of Powers Modulo m

Towers of Powers Modulo m

The technique of finding remainders using congruences can be extended to numbers with exponents, which are towers of powers, as the following example demonstrates.

EXAMPLE 4.12 Find the last digit in the decimal value of $1997^{1998^{1999}}$.

SOLUTION

First, notice that $a^{b^c} = a^{(b^c)}$. Let N denote the given number. The last digit in N equals the least residue of N modulo 10.

Since $1997 \equiv 7 \pmod{10}$, let us study the various powers of 7: $7^1 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$, $7^4 \equiv 1 \pmod{10}$, $7^5 \equiv 7 \pmod{10}$ and clearly a pattern emerges:

$$7^a \equiv \begin{cases} 1 \pmod{10} & \text{if } a \equiv 0 \pmod{4} \\ 7 \pmod{10} & \text{if } a \equiv 1 \pmod{4} \\ 9 \pmod{10} & \text{if } a \equiv 2 \pmod{4} \\ 3 \pmod{10} & \text{if } a \equiv 3 \pmod{4} \end{cases}$$

Now let us look at 1998. Since $1998 \equiv 2 \pmod{4}$, $1998^n \equiv 2^n \pmod{4}$, so if $n \geq 2$, then $1998^n \equiv 0 \pmod{4}$. Thus, since $1999 \geq 2$, $1998^{1999} \equiv 0 \pmod{4}$, so $N \equiv 1 \pmod{10}$. In other words, the last digit in the decimal value of N is 1. ■

Towers of Powers Modulo m (see article in The College Mathematics Journal)

EXAMPLE 4.8 Find the remainder when 16^{53} is divided by 7.

SOLUTION

First, reduce the base to its least residue: $16 \equiv 2 \pmod{7}$. So, by Theorem 4.5, $16^{53} \equiv 2^{53} \pmod{7}$. Now express a suitable power of 2 congruent modulo 7 to a number less than 7: $2^3 \equiv 1 \pmod{7}$. Therefore,

$$\begin{aligned} 2^{53} &= 2^{3 \cdot 17 + 2} = (2^3)^{17} \cdot 2^2 \\ &\equiv 1^{17} \cdot 4 \pmod{7} \\ &\equiv 4 \pmod{7} \end{aligned}$$

So $16^{53} \equiv 4 \pmod{7}$, by the transitive property. Thus, when 16^{53} is divided by 7, the remainder is 4. ■

Frozen Digits

I was studying tetrations, or "power towers", and I found a decently well-known fact. The last $k-1$ digits of ${}^k3 = 3^{3^{\cdot^{\cdot^{\cdot^3}}}}$ (k threes) remain constant, for all numbers ${}^a3$ with $a \geq k$ (see here for more). Why is this true? The link shows an ad-hoc proof for the last two digits, but how can we tackle larger cases? For example, how can we prove that the last **10** digits of ${}^T3$ remain constant for all $T \geq 11$?

EXAMPLE 4.9 Find the remainder when 3^{247} is divided by 17.

SOLUTION

Once again, we let the congruence do the job for us. We have

$$3^3 = 27 \equiv 10 \pmod{17}$$

Squaring both sides,

$$\begin{aligned} 3^6 &\equiv 100 \pmod{17} \\ &\equiv -2 \pmod{17} \end{aligned}$$

Raise both sides to the fourth power:

$$\begin{aligned} 3^{24} &\equiv (-2)^4 \pmod{17} \\ &\equiv -1 \pmod{17} \end{aligned}$$

Now apply the division algorithm with 24 as the divisor:

$$\begin{aligned} 3^{247} = 3^{24\cdot 10+7} &= (3^{24})^{10} \cdot 3^6 \cdot 3 \\ &\equiv (-1)^{10} \cdot (-2) \cdot 3 \pmod{17} \\ &\equiv -6 \pmod{17} \end{aligned}$$

Change -6 to its least residue:

$$\equiv 11 \pmod{17}$$

Thus, the remainder is 11. (Once again, appreciate the power of congruences.) ■

5.7 Digital Sum

2009 AMC 10A Problem # 5

What is the sum of the digits of the square of 111111111?

Solution

We see that 111^2 can be written as $111(100+10+1) = 11100+1110+111 = 12321$.

We can apply this strategy to find $111, 111, 111^2$, as seen below.

$$111111111^2 = 111111111(100000000 + 10000000 \cdots + 10 + 1)$$
$$= 11111111100000000 + 1111111110000000 + \cdots + 111111111$$
$$= 12,345,678,987,654,321$$

The digit sum is thus

$$1+2+3+4+5+6+7+8+9+8+7+6+5+4+3+2+1 = 81\boxed{(E)}.$$

■

AMC 1975 Problem #10

The sum of the digits in base ten of $\left(10^{4n^2+8}+1\right)^2$, where n is a positive integer, is

(A) 4	(B) $4n$	(C) $2+2n$	(D) $4n^2$	(E) n^2+n+2

Solution

For any nonnegative integer a we have

$$(10^a+1)^2 = 10^{2a} + 2 \cdot 10^a + 1$$

and the sum of the digits in all cases equals 4.

■

Let n be a natural number. We define the **digit sum** for base $b > 1$ $F_b : \mathbb{N} \to \mathbb{N}$ to be the following:

$$F_b(n) = \sum_{i=0}^{k-1} d_i$$

where $k = \lfloor \log_b n \rfloor + 1$ is the number of digits in the number in base b, and

$$d_i = \frac{n \bmod b^{i+1} - n \bmod b^i}{b^i}$$

is the value of each digit of the number.

For example, in base 10, the digit sum of 84001 is $F_{10}(84001) = 8+4+0+0+1 = 13$.

Mu Alpha Theta National Convention 2002, Number Theory Test, Alpha Division, Problem # 25

25. *What is the sum of the digits of the sum of the digits of the sum of the digits of 4444^{4444}?

A. 25 B. 16 C. 11 D. 7 E. NOTA

Solution

25. **D** Let $S(n)$ be the sum of the digits of n. Thus, we seek $S(S(S(4444^{4444})))$. Since $4444^{4444} < 10000^{5000}$, and 10000^{5000} is 1 followed by $4 \cdot 5000 = 20000$ zeroes,

$$S(4444^{4444}) < \underbrace{S(999\cdots999)}_{20000\ 9s} = 9 * 20000 = 180000,$$

. Since $S(4444^{4444}) < 180000$, $S(S(4444^{4444})) < S(99999) = 45$ because 99999 has the largest sum of digits of numbers less than 180000. Finally, $S(S(S(4444^{4444}))) < S(39) = 12$ because 39 has the largest sum of digits among numbers less than 45. Hence our answer is less than 12. To find the answer, we observe that $S(n) \equiv n \pmod 9$ for all n, (prove this by noting that $10 \equiv 1 \pmod 9$). Hence,

$$S(S(S(4444^{4444}))) \equiv 4444^{4444} \pmod 9 \equiv 7^{4444}.$$

The powers of 7 cycle $7, 4, 1, 7, 4, 1...$ (mod 9) and $4444 \equiv 1 \pmod 3$, so $7^{4444} \equiv 7 \pmod 9$. Since 7 is the only positive number less than 12 which is congruent to 7 mod 9,

$$S(S(S(4444^{4444}))) = 7.$$

■

5.7.1 Digital Sum in Base b

Mu Alpha Theta National Convention, 2001, Number Theory Test, Theta Division, Problem # 13

What is the sum of the digits of the base 9 representation of 2001?

Solution

13. 2001/9 = 222 remainder 3. 3 is the last digit. 222/9 = 24 remainder 6. 6 is the second to last digit. 24/9 = 2 remainder 6. 2 and 6 are the first two digits. 2 + 6 + 6 + 3 = 17.

(see file: Sum of the Digits in Base b notation)

Solution by Stanley Rabinowitz, Far Rockaway, N. Y. Suppose $N = \sum_{k=0}^{n} a_k b^k$. Then

$$a_j = \left[\frac{N}{b^j}\right] - b\left[\frac{N}{b^{j+1}}\right],$$

What is the sum of the digits of the base 9 representation of 2001?

$$a_0 = \left\lfloor\frac{2001}{9^0}\right\rfloor - 9\left\lfloor\frac{2001}{9^1}\right\rfloor$$
$$= 2001 - 9(222)$$
$$= 2001 - 1998$$
$$= 3$$

$$N - (b-1)\sum_{j=1}^{\infty}\left[\frac{N}{b^j}\right].$$

$$2001 - (8)\left(\left\lfloor\frac{2001}{9}\right\rfloor + \left\lfloor\frac{2001}{9^2}\right\rfloor + \left\lfloor\frac{2001}{9^3}\right\rfloor + \left\lfloor\frac{2001}{9^4}\right\rfloor + \cdots\right)$$

$$= 2001 - 8\left(\left\lfloor\frac{2001}{9}\right\rfloor + \left\lfloor\frac{\left\lfloor\frac{2001}{9^1}\right\rfloor}{9}\right\rfloor + \left\lfloor\frac{\left\lfloor\frac{2001}{9^2}\right\rfloor}{9}\right\rfloor + \left\lfloor\frac{\left\lfloor\frac{2001}{9^2}\right\rfloor}{9}\right\rfloor\right.$$

$$= 2001 - 8(222 + 24 + 2) = 17$$

■

5.8 Digital Roots

Let n be a positive integer and let $s(n)$ be the sum of the digits of n. Then $s\big(s(n)\big)$ equals the sum of the digits of the sum of the digits of n.

For example, let $n = 529$. Then $s(529) = 5 + 2 + 9 = 16$ and $s\big(s(529)\big) = s(16) = 7$.

We can continue to iterate on this process, $s\left(s\big(s(\cdots)\big)\right)$. Every starting positive integer n will terminate in a finite number of steps to an integer between 1 and 9. This process will always converge because $s(n) < n$ for all $n \geq 10$ and $s(n) = n$ for all $n \in \{1,2,\ldots,9\}$.

Let $\mathbb{S}(n) = s\left(s\big(s(\cdots)\big)\right)$ where the iteration continues until $s\left(s\big(s(\cdots)\big)\right) \in \{1,2,\ldots,9\}$.

$\mathbb{S}(n)$ is called the ***digital root*** of the positive integer n.

Digital roots have many interesting properties. The following are the mostly commonly cited.

For all positive integers a and b

(1) $\mathbb{S}(a) = a - 9n$ for that unique nonnegative integer n such that $a - 9n \in \{1,2,\ldots,9\}$

(2) $\mathbb{S}(9a) = 9$

(3) $\mathbb{S}(a) = \begin{cases} a \bmod (9) & 9 \nmid a \\ 9 & 9 \mid a \end{cases}$

(4) $\mathbb{S}(a+b) = \mathbb{S}\big(\mathbb{S}(a) + \mathbb{S}(b)\big)$

(5) $\mathbb{S}(a \cdot b) = \mathbb{S}\big(\mathbb{S}(a) \cdot \mathbb{S}(b)\big)$

(6) $\mathbb{S}(a^b) = \mathbb{S}\left(\big(\mathbb{S}(a)\big)^b\right)$.

http://applet-magic.com/DigitSum.htm

(They use the term "digit sum" to refer to "digital root".)

DigitSum(Polynomial(a)) = DigitSum(Polynomial(DigitSum(a))

Example: Let Polynomial(a) = a^2+a. Then Polynomial(11)=121+11=132 and thus DigitSum(Polynomial(11))=6. DigitSum(11)=2 so Polynomial(DigitSum(11))=4+2=6.

Division by single digit numbers other than multiples of 3 is equivalent to multiplication by a specific digit for that divisor. For example, division by 2 is equivalent to multiplication by 5. Thus DigitSum(32/2) = DigitSum(32*5) = DigitSum(160) = 7. which is the same as DigitSum(16). Division by 4 is equivalent to multiplication by 7 so DigitSum(20/4) = DigitSum(20*7) = DigitSum(140) = 5, which is correct.

The rule is DigitSum(a/b) = DigitSum(DigitSum(a)*Equivalent(DigitSum(b))) providing that DigitSum(b) is not a multiple of 3.

We will prove property (1) below. We simply note that property (2) follows from (1) with $n = a - 1$. Property (3) is a consequence of properties (1) and (2) and the definition of the modulus function. Properties (4), (5) and (6) are consequences of modular addition and modular multiplication and property (3).

Proof of Property (1)

Suppose $a = a_r 10^r + a_{r-1}10^{r-1} + \cdots + a_1 10^1 + a_0$ where $a_j \in \{0,1,\ldots,9\}$ for all j and $a_r \neq 0$ and recall that for all positive integers n

$$\begin{aligned} 10^n - 1 &= (10-1)(10^{n-1} + 10^{n-2} + \cdots + 10^1 + 10^0) \\ &= 9 \cdot (10^{n-1} + 10^{n-2} + \cdots + 10^1 + 10^0). \end{aligned}$$

It then follows that

$$\begin{aligned} a &= a_r 10^r + a_{r-1}10^{r-1} + \cdots + a_1 10^1 + a_0 \\ &= (a_r + a_{r-1} + \cdots + a_0) + a_r(10^r - 1) + a_{r-1}(10^{r-1} - 1) + \cdots + a_1(10^1 - 1) \end{aligned}$$

$= (a_r + a_{r-1} + \cdots + a_0) + 9k_1,$ where k_1 is some nonnegative integer

$= b + 9k_1,$ where $b = s(a)$.

If $b = a_r + a_{r-1} + \cdots + a_0 \in \{1,2,\ldots,9\}$ then the iterations stop and $\mathbb{S}(a) = s(a)$. In this case we see that $\mathbb{S}(a)$ has the form

$$\mathbb{S}(a) = s(a) = b = a - 9k_1 \in \{1,2,\ldots,9\}$$

as we were required to show.

If $b = a_r + a_{r-1} + \cdots + a_0 \notin \{1,2,\ldots,9\}$ then we repeat the process starting with the integer $b = s(a)$ instead of a. In this case suppose that

$$b = b_t 10^t + b_{t-1} 10^{t-1} + \cdots + b_1 10^1 + b_0$$

where $b_j \in \{0,1,\ldots,9\}$ for all j and $b_t \neq 0$. Following the same line of reasoning as in the previous iteration we then have

$$\begin{aligned} b &= b_t 10^t + b_{t-1} 10^{t-1} + \cdots + b_1 10^1 + b_0 \\ &= (b_t + b_{t-1} + \cdots + b_0) + 9k_2, \text{ where } k_2 \text{ is some nonnegative integer} \\ &= c + 9k_2, \text{ where } c = s(b) = s\big(s(a)\big). \end{aligned}$$

If $s\big(s(a)\big) = b_t + b_{t-1} + \cdots + b_0 \in \{1,2,\ldots,9\}$ then the iterations stop and $\mathbb{S}(a) = s(b) = s\big(s(a)\big)$. In this case we see that $\mathbb{S}(a)$ has the form

$$\mathbb{S}(a) = s\big(s(a)\big) = c = b - 9k_2 = (a - 9k_1) - 9k_2 = a - 9(k_1 + k_2) \in \{1,2,\ldots,9\}$$

as we were required to show.

If $s\big(s(a)\big) = b_t + b_{t-1} + \cdots + b_0 \notin \{1,2,\ldots,9\}$ then we repeat the process starting integer $c = s(b) = s\big(s(a)\big)$. In this case suppose that

$$c = c_v 10^v + c_{v-1} 10^{v-1} + \cdots + c_1 10^1 + c_0$$

where $c_j \in \{0,1,\ldots,9\}$ for all j and $c_v \neq 0$. As before we find

$$\begin{aligned} c &= c_v 10^v + c_{v-1} 10^{v-1} + \cdots + c_1 10^1 + c_0 \\ &= (c_v + c_{v-1} + \cdots + c_0) + 9k_3, \text{ where } k_3 \text{ is some nonnegative integer} \\ &= d + 9k_3, \text{ where } d = s(c) = s\big(s(b)\big) = s\Big(s\big(s(a)\big)\Big). \end{aligned}$$

If $s\Big(s\big(s(a)\big)\Big) = c_v + c_{v-1} + \cdots + c_0 \in \{1,2,\ldots,9\}$ then the iterations stop and $\mathbb{S}(a) = d = s(c) = s\big(s(b)\big) = s\Big(s\big(s(a)\big)\Big)$. In this case we see that $\mathbb{S}(a)$ has the form

$$\mathbb{S}(a) = s\Big(s\big(s(a)\big)\Big) = c - 9k_3 = a - 9(k_1 + k_2 + k_3) \in \{1,2,\ldots,9\}$$

as we were required to show.

If $s\Big(s\big(s(a)\big)\Big) = c_v + c_{v-1} + \cdots + c_0 \notin \{1,2,\ldots,9\}$ then the process continues. *How do we know that this process will eventually end?*

Notice that $a > s(a)$, that is

$$a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_1 10^1 + a_0 > a_r + a_{r-1} + \cdots + a_1 + a_0$$

unless $a = s(a) = a_0 \in \{1,2,\ldots,9\}$. But $s(a) \in \{1,2,\ldots,9\}$ means the process ends.

Similarly, $s(a) > s\big(s(a)\big)$. That is,

$$s(a) = b = b_t 10^t + b_{t-1}10^{t-1} + \cdots + b_1 10^1 + b_0$$
$$> b_t + b_{t-1} + \cdots + b_0 = s(b) = s\big(s(a)\big)$$

unless $b = s(b) = b_0 \in \{1,2,\ldots,9\}$. But $s(b) \in \{1,2,\ldots,9\}$ means the process ends.
In general,

$$a > s(a) > s\big(s(a)\big) > s\Big(s\big(s(a)\big)\Big) > \cdots$$

as long as the process continues. But a is finite, hence $s\Big(\cdots s\Big(s\big(s(a)\big)\Big)\Big)$ must eventually belong to $\{1,2,\ldots,9\}$ which means the process cannot go on forever.

■

15.2 Digital root

Given a positive integer n, let $\mathbf{d}(n)$ be the sum of the digits of n. If the operation $\mathbf{d}$ is repeated indefinitely, it stabilizes after a finite number of steps and yield a number between 1 and 9, which we call the digital root of n, denoted $\mathbf{D}(n)$. See [Dudeny, *Amusements*, p.157].

Theorem 15.1. **1.** $\mathbf{D}(m+n) = \mathbf{D}(\mathbf{D}(m) + \mathbf{D}(n))$.

2. $\mathbf{D}(mn) = \mathbf{D}(\mathbf{D}(m)\mathbf{D}(n))$.

3. $\mathbf{D}(m^n) = \mathbf{D}(\mathbf{D}(m)^n)$.

4. $\mathbf{D}(\mathbf{D}(n)) = \mathbf{D}(n)$.

5. $\mathbf{D}(n+9) = \mathbf{D}(n)$.

6. $\mathbf{D}(9n) = 9$.

Proof. (5) $\mathbf{D}(n+9) = \mathbf{D}(\mathbf{D}(n)+\mathbf{D}(9)) = \mathbf{D}(\mathbf{D}(n)+9) = \mathbf{D}(n)$ since $\mathbf{D}(n)$ is a single-digit number.
(6) $\mathbf{D}(9n) = \mathbf{D}(9\mathbf{D}(n)) = 9$ since $\mathbf{D}(n)$ has one single digit. □

National Mu Alpha Theta 2002, Number Theory Test, Alpha Division, Problem # 13

13. A digital root is the value of the sum of the digits of a number until only one digit remains. For example, for the number 625, first add 6+2+5 = 13. Now since 13 has 2 digits, add those digits; that is, 1+3=4. So the digital root of 625 is 4. What is the digital root is of 6^6? (Hint: Consider the first 5 terms of the sequence of 6^{th} powers and their digital roots.)
a) 0 b) 1 c) 6 d) 9

Solution

$1^6 = 1 \to 1$
$2^6 = 64 \to 10 \to 1$
$3^6 = 729 \to 18 \to 9$
$4^6 = 4096 \to 19 \to 10 \to 1$
$5^6 = 15625 \to 19 \to 10 \to 1$

Pattern 1, 1, 9, 1, 1, 9

$$\mathbb{S}(a) = \begin{cases} a \bmod(9) & 9 \nmid a \\ 9 & 9 \mid a \end{cases}$$

$$6^1 \bmod(9) = 6$$
$$6^2 \bmod(9) = 0$$

Therefore

$$6^k \bmod(9) = 0 \text{ for all } k \geq 2.$$

Therefore $9|6^6$ which by definition means $\mathbb{S}(6^6) = 9$.

■

Jim Totten's Problems of the Week

(171) *Problem.* One and only one of the following numbers is a perfect square. Which is it? Why? Do <u>not</u> compute the square roots. In fact, do <u>not</u> use calculators or computers at all.

3,669,517,136,205,224
1,898,732,825,398,318
4,715,006,864,295,101
5,901,643,220,186,100
7,538,062,944,751,882
2,512,339,789,576,516

Solution. Let us suppose that the integer a is the square root of the number we wish to identify. Then a can be written as $10b + c$, where b is some natural number and c is a digit between 0 and 9, inclusive. Then

$$a^2 = (10b + c)^2 = 100b^2 + 20bc + c^2 = 10(10b^2 + 2bc) + c^2.$$

Thus, the units digit of a^2 is affected only by the units digit of c^2. Since the units digit of c^2 can only be one of 0, 1, 4, 5, 6, or 9, we have eliminated two of the possibilities.
Now let us write a in the form $9d + e$, where d is a natural number and e is a digit between 0 and 8, inclusive. Then

$$a^2 = (9d + e)^2 = 81d^2 + 18de + e^2 = 9(9d^2 + 2de) + e^2.$$

Thus, on division by 9 the number we are seeking must leave a remainder of e^2 (actually e^2 reduced by some multiple of 9 in order to get a remainder in the proper range from 0 to 8, inclusive). Now e^2, on division by 9, leaves a remainder which is one of 0, 1, 4, or 7. Consequently, a^2 must leave a remainder of 0, 1, 4, or 7 on division

by 9. But we know that the remainder on dividing a number by 9 is the same as the remainder on dividing the sum of its digits by 9. Of the four remaining candidates, the sum of the digits has a remainder in the set $\{0, 1, 4, 7\}$ only for 2,512,339,789,576,516. (It is, in fact, the square of 50,123,246.)

see file “Digital Roots, Rings and Clock Arithmetic”

Thus we obtain the digital root of any positive number N we simply divide by 9 and take the remainder—except that if N is a multiple of 9 we set $\text{d.r.}(N) = 9$ (rather than 0). Hence 'calculating with digital roots (base 10)' is exactly the same as 'working modulo 9'.

Mu Alpha Theta Florida State Convention 2005, Number Theory Test, Problem #24

A perfect number is a positive integer whose positive integral factors (not including itself) add up to that number. For example, 6 is the smallest perfect number because $6 = 1 + 2 + 3$. What is the digital root of the 2nd smallest perfect number?

Solution

Theorem – the digital root of all perfect numbers larger than 6 is 1.

Verfication for this particular case. The 2nd smallest perfect number is 28 and

$$dr(28) = dr(2 + 8) = dr(10) = dr(1 + 0) = 1.$$

■

Mu Alpha Theta Florida State Convention 2005, Number Theory Test, Problem #25

If p is a prime greater than 2005, which of the following cannot be its digital root?

Solution

25. C If the digital root of a number is divisible by 3, so is the original number. No primes greater than 3 can have a digital root of a multiple of 3.

Property 2. *The difference between n and $B(n)$ is a multiple of 9; i.e., $n - B(n) = 9k$ for some non-negative integer k.*

Corollary: *The difference between n and $B(n)$ is a multiple of 3.*

Property 5. *A prime number exceeding 3 cannot have a digital root equal to 3, 6 or 9.*

For, since $n - B(n)$ is a multiple of 3, if $B(n)$ is a multiple of 3, then so must be n; and the only prime number which is a multiple of 3 is 3 itself.

■

5.8.1 Digital Roots in Base b

$$\mathrm{dr}_b(n) = n - (b-1)\left\lfloor \frac{n-1}{b-1} \right\rfloor.$$

Let $s_7(n)$ equal the sum of the digits of the base 7 equivalent of the base 10 number n. For example if $n = n_r 7^r + n_{r-1}7^{r-1} + \cdots + n_1 7^1 + n_0$ where $n_j \in \{0,1,\ldots,6\}$ for all j and $n_r \neq 0$, then $s_7(n) = n_7 + n_{r-1} + \cdots + n_1 + n_0$.

Note we are adding $n_0, n_1, \ldots, n_7$ in base 10.

$$\begin{gathered} a = a_r 7^r + a_{r-1}7^{r-1} + \cdots + a_1 7^1 + a_0 \\ = a_r(7^r - 1) + a_{r-1}(7^{r-1} - 1) + \cdots + a_1(7^1 - 1) + (a_r + a_{r-1} + \cdots + a_0) \\ = 6k_1 + (a_r + a_{r-1} + \cdots + a_0) \\ = 6k_1 + b, \text{ where } b = s_7(a) \end{gathered}$$

Now suppose that

$$b = b_t 7^t + b_{t-1}7^{t-1} + \cdots + b_1 7^1 + b_0.$$

Then

$$\begin{gathered} b = b_t 7^t + b_{t-1}7^{t-1} + \cdots + b_1 7^1 + b_0 \\ = 6k_2 + (b_t + b_{t-1} + \cdots + b_0) \\ = 6k_2 + c, \text{ where } c = s_7(b) = s_7\big(s_7(a)\big) \end{gathered}$$

Now suppose that

$$c = c_v 7^v + c_{v-1}7^{v-1} + \cdots + c_1 7^1 + c_0.$$

Then

$$\begin{gathered} c = c_v 7^v + c_{v-1}7^{v-1} + \cdots + c_1 7^1 + c_0 \\ = 6k_3 + (c_v + c_{v-1} + \cdots + c_0) \\ = 6k_3 + d, \text{ where } d = s_7(c) = s_7\big(s_7(b)\big) = s_7\Big(s_7\big(s_7(a)\big)\Big). \end{gathered}$$

$$a = 6k_1 + b = 6k_1 + 6k_2 + c = 6k_1 + 6k_2 + 6k_3 + d.$$

That is

$$\begin{aligned} a &= 6k_1 + 6k_2 + 6k_3 + s_7\Big(s_7\big(s_7(a)\big)\Big) \\ &= 6(k_1 + k_2 + k_3) + s_7\Big(s_7\big(s_7(a)\big)\Big) \\ &= 6m + s_7\Big(s_7\big(s_7(a)\big)\Big) \end{aligned}$$

$$= 6k_1 + (b_t 7^t + b_{t-1}7^{t-1} + \cdots + b_1 7^1 + b_0)$$

$$= 6k_1 + \left(6k_2 + (b_t + b_{t-1} + \cdots + b_0)\right)$$
$$= 6k_1 + 6k_2 + (b_t + b_{t-1} + \cdots + b_0)$$

$$6k_2 + (b_t + b_{t-1} + \cdots + b_0)$$

$$b = b_t 7^t + b_{t-1} 7^{t-1} + \cdots + b_1 7^1 + b_0 = 6k_2 + (b_t + b_{t-1} + \cdots + b_0)$$

$$= 9k_1 + 9k_2 + c, \text{ with } c = s(b) = s\big(s(a)\big)$$
$$= 9k_1 + 9k_2 + 9k_3 + d, \text{ with } d = s(c) = s\big(s(b)\big) = s\left(s\big(s(a)\big)\right)$$
$$= \cdots = 9k_1 + 9k_2 + \cdots + 9k_m + s\left(s\left(\cdots s\big(s(a)\big)\right)\right)$$
$$= 9n + \mathbb{S}(a)$$

Therefore,

$$\mathbb{S}(a) = a - 9n.$$

$$a \bmod(9) = b \bmod(9)$$

$$s(a) = a_r + a_{r-1} + \cdots + a_0$$

$$7^b - 1 = (7-1)(7^{b-1} + 7^{b-2} + \cdots + 7^1 + 7^0)$$

$$324115_7 = 3 * 7^5 + 2 * 7^4 + 4 * 7^3 + 1 * 7^2 + 1 * 7^1 + 5 * 7^0 = 56656_{10}$$

$$56656\ mod(6) = 4$$

$$\text{dr}(324115_7)$$

$$3 + 2 + 4 + 1 + 1 + 5 = 16_{10}$$

$$3 + 2 + 4 + 1 + 1 + 5 = 22_7$$

$$16_{10} = 2 \cdot 7^1 + 2 \cdot 7^0 = 22_7$$
$$22_7$$
$$2 + 2 = 4$$
$$4_{10} = 4_7$$

$$324115 \bmod(6) = 1$$

$$43612_7$$
$$4 + 3 + 6 + 1 + 2 = 16_{10}$$
$$16_{10} = 22_7$$
$$2 + 2 = 4_{10}$$
$$4_{10} = 4_7$$
$$43612 \bmod(6) = 4$$

$$213_8$$
$$2 + 1 + 3 = 6_{10}$$

$$\mathrm{dr}_b(n) = n - (b-1)\left\lfloor \frac{n-1}{b-1} \right\rfloor .$$

$$324115 - (7-1)\left\lfloor \frac{324115-1}{7-1} \right\rfloor = 324115 - (7-1)(54019)$$

54019

5.9 Missing Digit Puzzle Problems

1. The integer $1287xy6$ is a multiple of 72. Find the number xy. (*Mathematics Teacher*, 1986)

$1287xy6$ is a multiple of 8 and 9

$$1287xy6 \equiv 0 \pmod 9 \quad \textbf{AND} \quad 1287xy6 \equiv 0 \pmod 8$$

Now recall that a number is divisible by 9 if and only if the sum of the digits is a multiple of 9.

That is $(1+2+8+7)+(x+y+6)=2(9)+(x+y+6)\equiv 0 \pmod 9$

$$\Leftrightarrow 2(9) \pmod 9 + (x+y+6) \pmod 9 \equiv 0 \pmod 9$$
$$\Leftrightarrow x+y+6 \equiv 0 \pmod 9$$

If $1287xy6$ is divisible by 8 then it is also divisible by 4. And it is divisible by 4 if and only if the number formed by the last two digits is divisible by 4. That is, if $10y+6\equiv 0 \pmod 4$.

$$10y+6\equiv 0 \pmod 4 \Leftrightarrow 10 \pmod 4 \cdot y + 6 \pmod 4 \equiv 0 \pmod 4$$
$$\Leftrightarrow 2y+2\equiv 0 \pmod 4.$$

But recall that $ca \equiv cb \pmod m$ if and only if $a \equiv b \pmod{m/(c,m)}$. So

$$2y+2\equiv 0 \pmod 4 \Leftrightarrow y+1\equiv 0 \pmod{4/(2,4)}$$
$$\Leftrightarrow y+1\equiv 0 \pmod{4/2}$$
$$\Leftrightarrow y+1\equiv 0 \pmod 2.$$

But this is equivalent to saying that y is odd.

We also know that $1287xy6$ is divisible by 8 if and only if the number formed by the last three digits is divisible by 8. That is, $100x+10y+6\equiv 0 \pmod 8$. But

$$100x+10y+6\equiv 0 \pmod 8$$
$$\Leftrightarrow 4x+2y+6\equiv 0 \pmod 8$$
$$\Leftrightarrow 2x+y+3\equiv 0 \left(\mathrm{mod}\, 8/(8,2)\right)$$
$$\Leftrightarrow 2x+y+3\equiv 0 \pmod{8/2}$$
$$\Leftrightarrow 2x+y+3\equiv 0 \pmod 4.$$

■

Koshy

Supplementary Exercises (p. 243)

1. Because $1287xy6 \equiv 0 \pmod{72}$,

$$1287xy6 \equiv 0 \pmod 8 \quad \text{and} \tag{1}$$

$$1287xy6 \equiv 0 \pmod 9 \tag{2}$$

Congruence (1) implies $y+1\equiv 0 \pmod 2$, so y is odd. Thus, $y=1, 3, 5, 7,$ or 9. The two congruences yield

$$2x+y+3\equiv 0 \pmod 4 \quad \text{and} \tag{3}$$

$$x+y+6\equiv 0 \pmod 9 \tag{4}$$

If $y=1$, then $2x+4\equiv 0 \pmod 4$; that is, $x=0, 2, 4, 6,$ or 8, of which only 2 satisfies (4), so $(2, 1)$ is a solution. If $y=3$, then $2x+6\equiv 0 \pmod 4$ by (3), so $x+1\equiv 0 \pmod 2$. Thus, $x=1, 3, 5, 7,$ or 9, of which only $x=9$ satisfies (4). The corresponding solution is $(9, 3)$. Similarly, we get one more solution, $(5, 7)$. Thus, there are three solutions: $(2, 1)$, $(5, 7)$, and $(9, 3)$.

■

Problem (PUMaC 2009 Number Theory.)

If $17! = 355687ab8096000$, *where* a *and* b *are two missing digits, find* a *and* b.

- 17! is divisible both by 9 and by 11, so:
  - $3+5+\cdots+a+b+\cdots \equiv 0 \pmod 9$, so $a+b \equiv 6 \pmod 9$.
  - $3-5+\cdots+a-b-\cdots \equiv 0 \pmod{11}$, so $a-b \equiv 2 \pmod{11}$.

  This means $a = 4$ and $b = 2$.

(5A081)

1. The six-digit number $\underline{\mathbf{2}}\,\underline{\mathbf{1}}\,\underline{7}\,\underline{\mathbf{X}}\,\underline{8}\,\underline{\mathbf{5}}$, when divided by 9, leaves a remainder of 2. What is the value of the obscured digit, **X**?

Solution

If $\underline{\mathbf{2}}\,\underline{\mathbf{1}}\,\underline{7}\,\underline{\mathbf{X}}\,\underline{8}\,\underline{\mathbf{5}}$ *leaves a remainder of 2 when divided by 9, then* $\underline{\mathbf{2}}\,\underline{\mathbf{1}}\,\underline{7}\,\underline{\mathbf{X}}\,\underline{8}\,\underline{3}$ *must be divisible by 9, and the sum of its digits must also be divisible by 9.*
$2+1+7+X+8+3 = 21+X$, *which is only divisible by 9 if* $X = 6$.

■

(TA044)

4. Find all pairs of integers (M,N) for which the four digit integer MM5N is divisible by 12.

Solution

$50 + N$ must be divisible by $4 \Leftrightarrow 48 + 2 + N$ is divisible by $4 \Leftrightarrow N \in \{2,6\}$
$M + M + 5 + N$ must be divisible by 3
Case $N = 2$

$$2M + 7 = 3k, M \in \{1,4,7\}$$

Case $N = 6$

$$2M + 11 = 3k, M \in \{2,5,8\}$$

So we have the cases

$$(M,N) \in \{(1,2),(4,2),(7,2),(2,6),(5,6),(8,6)\}$$

■

(TC884) The number N_{10} is a multiple of 7. Its base two representation is

$$N_2 = 11101000111011abc101$$

where each of the missing digits a, b, and c must be either 0 or 1. Find the ordered triple (a, b, c) of integers.

Solution

Rewrite N_{10} as an integer in base eight.

$$N_8 = 16473\underline{?}5.$$

In base eight, N_8 is divisible by 7 if and only if the sum of its digits equals $7k$ for some nonnegative integer k. (This theorem is an analog of "casting out nines".)

$$1 + 6 + 4 + 7 + 3 + \underline{?} + 5 = 26 + \underline{?} = 7k$$

where $0 \leq \underline{?} < 8$. It follows that $\underline{?} = 2_8 = 010_2$. That is, $(a, b, c) = (0,1,0)$.

[Note: Need to elaborate on how and why
$11101000111011abc101_2 = 16473\underline{?}5_8$.]

■

Example

Find the missing digit $\boldsymbol{a}$ in the base 5 number $n = (420\boldsymbol{a}1332)_5$ if n is even and divisible by 3.

Solution

For n to be divisible by 2 in an odd numbered base $(b = 5)$ means that the number of odd digits in n must be an even number.

Not considering $\boldsymbol{a}$ there are three odd digits in n $(1, 3$ and $3)$. Therefore $\boldsymbol{a}$ must be odd if n is even (has an even number of odd digits). But the only odd digits in base 5 are 1 and 3. So $\boldsymbol{a}$ must be 1 or 3.

For n to be divisible by 3, $n \bmod(3) = 0$.

$$n \bmod(3)$$

$$= \left(4 \cdot 5^7 + 2 \cdot 5^6 + 0 \cdot 5^5 + (a) \cdot 5^4 + 1 \cdot 5^3 + 3 \cdot 5^2 + 3 \cdot 5^1 + 2 \cdot 5^0\right) \bmod(3)$$
$$= \left(4 \cdot (-1)^7 + 2 \cdot (-1)^6 + 0 \cdot (-1)^5 + (a) \cdot (-1)^4 + 1 \cdot (-1)^3 + 3 \cdot (-1)^2 + 3 \cdot (-1)^1 + 2 \cdot (-1)^0\right) \bmod(3)$$
$$= \left(-4 + 2 + (a) - 1 + 3 - 3 + 2\right) \bmod(3)$$
$$= (a - 1) \bmod(3)$$

This implies that a must be 1 or 4.

Hence for n to be divisible by both 2 and 3, $\boldsymbol{a = 1}$.

■

Mu Alpha Theta, Florida State Convention, 1992-1993, Number Theory Topic Test, Number 1
The mathematics department bought a pack of 72 pencils. The ink on the receipt got smudged and all that could be made out was $\$ \underline{\star} 9.4 \underline{\star}$ (before any sales tax). How much did the department pay per pencil?

Solution

Representing $\$ \underline{\star} 9.4 \underline{\star}$ as the four digit integer $a94b$, we can apply the divisibility rule for 8 to see that $940 + a$ must be divisible by 8. $940 = 117(8) + 4$. So $a = 4$.

By the divisibility rule for 9, we know $b + 9 + 4 + 4 = 17 + b$ must be divisible by 9. So $b = 1$.

Therefore,

$$\frac{\$19.44}{72} = 27¢$$

■

AMC 2019 10B Problem #14
The base-ten representation for $19!$ Is $121{,}6T5{,}100{,}40M, 832, H00$, where T, M, and H denote digits that are not given. What is $T + M + H$?

(A) 3	(B) 8	(C) 12	(D) 14	(E) 17

Solution

■

1999 Mu Alpha Theta National Convention, Number Theory Test, Alpha Division, Tie Breaker #2
If 792 divides the integer $13xy45z$, find the digits x, y, and z.

Solution

First note that $792 = 2^3 \cdot 3^2 \cdot 11$ so we can apply the divisibility tests for $8, 9$ and 11.

(*i*) The divisibility test for 8 tells us that the last three digits must be divisible by 8.

$$450 \bmod 8 = 2 \Longrightarrow 456 \bmod 8 = 0 \Longrightarrow z = 6.$$

(*ii*) The divisibility test for 9 tells us that the sum of the digits must be divisible by 9.

$$(1 + 3 + x + y + 4 + 5 + 6) \bmod 9 = 0 \Longrightarrow x + y \in \{8,17\}$$

(*iii*) The divisibility test for 11 tells us that the alternating sum of the digits must be divisible by 11.

$$(1 - 3 + x - y + 4 - 5 + 6) \bmod 11 = 0 \Longrightarrow (x - y) \bmod 11 = 8$$
$$\Longrightarrow x - y \in \{-3,8\}$$

Solving the generic simultaneous equations $x + y = m$ and $x - y = n$ gives us

$$x = (m + n)/2 \text{ and } y = (m - n)/2.$$

This tells us that m and n have to both be even or both be odd. This just leaves two possibilities: $(m, n) = (8,8)$ or $(m, n) = (17, -3)$.

We can see that $(m, n) = (17, -3) \Longrightarrow (x, y) = (7,10)$ which is impossible because $y \leq 9$.

Finally, $(m, n) = (8,8) \Longrightarrow (x, y) = (8,0)$, which is the only possible pair.

Therefore, $(x, y, z) = (8,0,6)$ and as a check we note that $1380456 = 792 \cdot 1743$ which confirms our answer.

■

British Mathematical Olympiad Round 1, 2002-2003, Problem 1.

Given that

$$34! = 295\,232\,799\,cd9\,604\,140\,847\,618\,609\,643\,5ab\,000\,000,$$

determine the digits a, b, c and d.

Solution

Finding b.

The prime factorization of $34!$ is easily found to be

$$34! = 2^{32} \cdot 3^{15} \cdot 5^7 \cdot 7^4 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31.$$

The 2^{32} and 5^7 prime factors tell us that $34!$ ends with seven 0's. Therefore $b = 0$.

Finding a.

Likewise, the prime factorization of

$$\frac{34!}{10^7} = 29\,523\,279\,9cd\,960\,414\,084\,761\,860\,964\,35a,$$

is

$$\frac{34!}{10^7} = 2^{25} \cdot 3^{15} \cdot 7^4 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31$$

and hence is divisible by 8. Therefore, the three digit number $35a$ must be divisible by 8.

We note that $350 \pmod 8 = 6$, hence $352 \pmod 8 = 0$ and $a = 2$.

Finding c and d.

We also know that $34!$ is divisible by both 9 and 11. Hence

$$\begin{pmatrix} 2+9+5+2+3+2+7+9+9+c+d+9+6+0+4 \\ +1+4+0+8+4+7+6+1+8+6+0+9+6+4+3 \\ +5+2+0+0+0+0+0+0+0 \end{pmatrix} \pmod 9$$
$$= (c+d+141) \pmod 9 = (c+d+6) \pmod 9 = 0$$

and

$$\begin{pmatrix} 2-9+5-2+3-2+7-9+9-c+d-9+6-0+4 \\ -1+4-0+8-4+7-6+1-8+6-0+9-6+4-3 \\ +5-2+0-0+0-0+0-0+0 \end{pmatrix} \pmod{11}$$
$$= (d-c+19) \pmod{11} = (d-c+8) \pmod{11} = 0.$$

Therefore, $(c+d) \in \{3,12\}$ and $(d-c) \in \{-8,3\}$. So, we have four cases to consider.

Solving $c+d=m$ and $d-c=n$ simultaneously, we have

$$c = \frac{m-n}{2} \text{ and } d = \frac{m+n}{2}.$$

Consider the value of (c,d) at each of the four cases

$$(m,n) \in \{(3,-8),(3,3),(12,-8),(12,3)\}.$$

We can eliminate $(3,-8)$ and $(12,3)$ because they return nonintegral values for c and d. We can eliminate $(12,-8)$ because it returns a value for $c > 9$. So $(m,n) = (3,3)$ is the only possible solutions. This returns

$$(c,d) = \left(\frac{3-3}{2}, \frac{3+3}{2}\right) = (0,3).$$

That is, $c=0$ and $d=3$. Therefore, $(a,b,c,d) = (2,0,0,3)$.

Note the answer $2,0,0,3$ is a partial clue that you have the correct answer because it is often the case in math contest problems that the solution is related to the year the test was given (in this case, the year was 2003).

■

5.10 Extra Modular Arithmetic Problems

AMC 1970 Problem #34

The greatest integer that will divide $13{,}511$, $13{,}903$ and $14{,}589$ and leave the same remainder is

(A) 28	(B) 49	(C) 98	
(D) an odd multiple of 7 greater than 49			
(E) an even multiple of 7 greater than 98			

Solution

■

AMC 1971 Problem #12

For each integer $N > 1$, there is a mathematical system in which two or more integers are defined to be congruent if they leave the same non-negative remainder when divided by N. If $69,\ 90$, and 125 are congruent in one such system, then in that same system, 81 is congruent to

(A) 3	(B) 4	(C) 5	(D) 7	(E) 8

Solution

■

Mu Alpha Theta National Convention, 2001, Number Theory Test, Mu Division, Problem # 16

If b is a positive integer and $b \equiv 2 \pmod 3$ and $b \equiv 7 \pmod 3$, what is the remainder when b is divided by 12?

Solution

16. First not that B ≡ -1 (mod 3) and B ≡ -1 (mod 8) => B ≡ -1 (mod 24). Thus B ≡ -1 (mod 12) => B ≡ 11 (mod 12).

■

Mu Alpha Theta National Convention, 2001, Number Theory Test, Mu Division, Problem # 19

If $40a \equiv 1 \pmod 7$, what is $162a$ congruent to $\pmod 7$?

Solution

19. 42a + 3(40a) ≡ 0 + 3(1) (mod 7). Thus 162a ≡ 3 (mod 7).

■

Mu Alpha Theta National Convention, 2001, Number Theory Test, Mu Division, Problem # 24

How many whole numbers are there less than $10{,}000$ which have units and tens digits of 1 when expressed in bases $4, 5$, and 6?

Solution

24. We are hunting for integers, N, such that N ≡ 5 (mod 16), N ≡ 6 (mod 25), and N ≡ 7 (mod 36). From the first of these relations, we know that N ≡ 1 (mod 4), but that contradicts the third relation which shows that N ≡ 3 (mod 4). Thus there are no such integers.

■

Mu Alpha Theta National Convention, 2001, Number Theory Test, Mu Division, Problem # 27

What is the second smallest positive integer x such that $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod 9$, and $x \equiv 5 \pmod{25}$?

Solution

27. Given x ≡ 2 (mod 4), we can say x = 4a –2 for some positive integer, a. Then from the second equation, 4a -2 ≡ 3 (mod 9) => 4a ≡ 5 (mod 9) => a ≡ 8 (mod 9) and thus we can say a = 9b – 1 for some positive integer, b. Thus x = 36b – 6. Finally, from the last equation, 36b – 6 ≡ 5 (mod 25) => 36b ≡ 11 (mod 25) => b ≡ 1 (mod 25). Thus we can say that b = 25c – 24 for some positive integer, c. Thus x = 900c – 870. 930 is the second smallest positive solution.

■

Mu Alpha Theta National Convention, 2001, Number Theory Test, Mu Division, Problem # 37

N is a positive integer less than one hundred. If $3^N \equiv N \pmod{100}$, what is N?

Solution

37. Solving this problem involves a degree of deduction taking several factors into consideration. We can rule out even values of N. We can also note that phi(10) = 4 and phi(100) = 40. This will help limit our search as we know that the units digit of 3^N repeats in a 4-cycle and the last pair of digits repeats in (at most) a 40-cycle. In fact, noting that 3 x 3 x 3 x 3 = 81 = (80 + 1), we can see by binomial expansion that taking 81 to the fifth power produces a number with a units digit of 1 and a tens digit of 0. Thus 3^N repeats its last two digits in a 20-cycle. Now we must simply look for where $3^N \equiv 0$ (mod 20) and adjust N by adding/subtracting multiples of 20. We thus need only check the first 20 positive integers (and only the 10 odd ones of those).

We can rule out most of these by comparing the 4-cycle of units digits. If $N \equiv 1$ (mod 4), then the units digit of 3^N will be 3. If $N \equiv 3$ (mod 4), the units digit will be 7. The only N that need be tested are thus 7 and 13. $3^N \equiv N$ (mod 20) for 7, but not 13. The tens digit of 3^7 is 8, thus 87 is the only solution such that $3^N \equiv N$ (mod 100).

■

Mu Alpha Theta National Convention 2001, Number Theory Test, Theta Division, Problem # 22

If $3x \equiv 4 \pmod 5$ and $5x \equiv 6 \pmod 7$, which of the following could be x ?

(A) 19 (B) 34 (C) 53 (D) 630 (E) NOTA

Solution

22. Given that 3x ≡ 4 (mod 5), we can say that 3x ≡ 4+5 (mod 5), then 3x ≡ 9 (mod 5), and thus x ≡ 3 (mod 5). Likewise we can find that x ≡ 4 (mod 7). From the latter of these relationships, we can say that x = 7y –3 for any positive integer y. Thus we know that 7y -3 ≡ 3 (mod 5) => 7y ≡ 1 (mod 5) ≡ 21 (mod 5). Thus y ≡ 3 (mod 5). We can say that y = 5z –2 for any positive integers z. From the relationship between x and y, we now know that x = 7(5z –2) –3 = 35z – 17. Thus x ≡ -17 (mod 35) ≡ 18 (mod 35). 53 is the only answer which satisfies this relationship.

■

Mu Alpha Theta National Convention 2001, Number Theory Test, Theta Division, Problem # 40

What is the remainder when 337,500,000 is divided by 128 ?

Solution

40. **This problem can be tediously worked out by long division. There is a much simpler way however. Find the prime factorization of the large number.**

$337{,}500{,}000 = (2^5)(3^3)(5^8)$. Divide both this number and 128 by 32. Now take the remaining portion of the large number and find its remainder when divided by 4 (which is 128/32): $(3^3)(5^8) \equiv (-1)^3(1^8) \pmod 4 \equiv -1 \pmod 4 \equiv 3 \pmod 4$. Multiplying both sides back by 32 tells the solver that the original number is congruent to 96 (mod 128).

■

Mu Alpha Theta National Convention 2005, Number Theory Test, Alpha Division, Problem #9
When M is divided by 9 the remainder is 6. When N is divided by 27 the remainder is 9. What is the remainder when the product MN is divided by 27 ?
Solution

$$M = 9k + 6 = 3(3k + 2)$$
$$N = 27k + 9 = 9(3k + 1)$$
$$MN = 27(3k + 2)(3k + 1)$$

Therefore,

$$MN \equiv 0 \bmod(27).$$

■

Mu Alpha Theta National Convention 2005, Number Theory Test, Alpha Division, Problem #29
M and N are positive integers such that $3M + 8N \equiv 5 \pmod{17}$. Find the remainder when $9M + 7N$ is divided by 17.
Solution
In general, if $a \equiv b \pmod m$ then $ac \equiv bc \pmod m$. Applying this result we know that

$$3(3M + 8N) \equiv 3(5) \pmod{17} \Longrightarrow 9M + 24N \equiv 15 \pmod{17}.$$

But we also know that

$$(9M + 24N)(\bmod 17) \equiv (9M + 7N + 17N)(\bmod 17)$$
$$\equiv (9M + 7N)(\bmod 17).$$

Therefore

$$9M + 7N \equiv 15 \pmod{17}.$$

That is, 15 is the remainder when $9M + 7N$ is divided by 17.

■

Mu Alpha Theta National Convention 2005, Number Theory Test, Alpha Division, Problem #28
The remainder when N is divided by 18 is 16. Given that N is a multiple of 28, what integers between 0 and 18 could be the remainder when $N/4$ is divided by 18 ?
Solution
We are given that $N = 28m$ for some integer m and that $N \equiv 16 \pmod{18}$. This tells us that

$$N \equiv 16 \pmod{18} \text{ and } N = 28m \Longrightarrow 28m \equiv 16 \pmod{18}$$
$$\Longrightarrow 7m \equiv 4 \left(\mod\left(\frac{18}{\gcd(4,18)}\right)\right)$$
$$\Longrightarrow 7m \equiv 4 \pmod{9}.$$

The question is to find the remainder r when $N/4$ is divided by 18. That is find $N/4 \pmod{18}$.

$$\frac{N}{4} = \frac{28m}{4} = 7m$$

So, the question is to find $7m \pmod{18}$ given that $7m \equiv 4 \pmod{9}$.

But we know that if $7m \equiv c \pmod{18}$ then $7m \equiv c \pmod{9}$. That is,

$$7m - c = 18k = 9(2k) \Longrightarrow 7m \equiv c \pmod{9}.$$

However, we know that $7m \equiv 4 \pmod{9}$. So the only possible values for c are 4 and any number congruent to $4 \pmod{9}$, such as 13.

It follows that the only integers between 0 and 18 could be the remainder when $N/4$ is divided by 18 are the integers 4 and 13.

■

Mu Alpha Theta Florida State Convention 2005, Number Theory Test, Problem #3

Given that $x \equiv 7 \pmod{360}$, what are the possible nonnegative integer values less than 420 for $x \equiv 7 \pmod{420}$?

Solution

In general, if $a \equiv b \pmod{m}$ and $d|m$, $d > 0$, then $a \equiv b \pmod{d}$. From this property we can see that

$$x \equiv 7 \pmod{360} \Longrightarrow x \equiv 7 \pmod{60}.$$

Now suppose $x \equiv c \pmod{420}$. Then from this same property we have

$$x \equiv c \pmod{420} \Longrightarrow x \equiv c \pmod{60}.$$

So, the only possible nonnegative integer values for c less than 420 are values consistent with the fact that $x \equiv 7 \pmod{60}$.

That is, $c \in \{7,67,127,187,247,307,367\}$.

■

2016 Lehigh University High School Math Contest, Problem #16

How many 3 element subsets of $\{1,2,3,4,5,6,7,8,9,10,11\}$ are there for which the sum of the elements in the subset is a multiple of 3?

Solution

To start you need to remember that by definition of a set (or subset) the order of the elements in the set (or subset) is irrelevant (*i.e.* $\{4,7,10\}$ and $\{7,10,4\}$ are not distinct solutions) and by definition all elements of the set (or subset) must be distinct (*i.e.* $\{5,5,8\}$ is not a solution even though the sum is a multiple of 3).

Let $\{a_1, a_2, a_3\}$ be a subset of $\{1,2,3,4,5,6,7,8,9,10,11\}$. Saying that the sum is a multiple of 3 is the same as requiring that $(a_1 + a_2 + a_3) \bmod(3) \equiv 0 \bmod(3)$.
We can restate the problem as

$$a_1 \bmod(3) + a_2 \bmod(3) + a_3 \bmod(3) \equiv 0 \bmod(3).$$

Now let $b_j = a_j \bmod(3)$, $b_j \in \{0,1,2\}$. Then we can partition the problem into just three cases:

$$\{b_1, b_2, b_3\} | b_1 + b_2 + b_3 = 0$$

$$\{b_1, b_2, b_3\} | b_1 + b_2 + b_3 = 3$$

$$\{b_1, b_2, b_3\} | b_1 + b_2 + b_3 = 6.$$

There is only one subset in the first case, namely $\{0,0,0\} \bmod(3)$. There are two subsets in the second case, $\{1,1,1\} \bmod(3)$ and $\{0,1,2\} \bmod(3)$. And there is just one subset in the third case, namely, $\{2,2,2\} \bmod(3)$.
Now we need to separate the numbers $\{1,2,3,4,5,6,7,8,9,10,11\}$ according to their $\bmod(3)$ value.

$$\begin{aligned} \{3,6,9\} &\ \bmod(3) = 0 \\ \{1,4,7,10\} &\ \bmod(3) = 1 \\ \{2,5,8,11\} &\ \bmod(3) = 2. \end{aligned}$$

In the case $\{0,0,0\} \bmod(3)$ we need to select 3 of the 3 elements in $\{3,6,9\}$ without replacement and where the order of selection is not important to us. This is the definition of *combinations* and equals $\binom{3}{3} = 1$.
In the case $\{1,1,1\} \bmod(3)$ we need to select 3 of the 4 elements in $\{1,4,7,10\}$ without replacement and where the order of selection is not important to us. This is the definition of *combinations* and equals $\binom{4}{3} = 4$.
In the case $\{0,1,2\} \bmod(3)$ we need to select 1 of the 3 elements in $\{3,6,9\}$, select 1 of the four elements in $\{1,4,7,10\}$ and 1 of the four elements in $\{2,5,8,11\}$. There are $\binom{3}{1}\binom{4}{1}\binom{4}{1} = 48$ ways we can do this.
Finally in the case $\{2,2,2\} \bmod(3)$ we need to select 3 of the 4 elements in $\{2,5,8,11\}$ without replacement and where the order of selection is not important to us. This is the definition of *combinations* and equals $\binom{4}{3} = 4$.
In total there are $1 + 4 + 48 + 4 = 57$ ways to select the three numbers from $\{1,2,3,4,5,6,7,8,9,10,11\}$, without replacement and order not important, such that the sum of the three numbers selected is a multiple of 3.

■

2007 Lehigh University High School Math Contest, Problem #17
For how many primes p is $h(p) = p^2 + 3p - 1$ also prime?
Solution

We begin by considering the special cases of $p = 2$ and $p = 3$.

$$h(2) = 9. \quad \text{Composite.}$$
$$h(3) = 17. \ \text{Prime.}$$

We have previous established that for all prime $p > 3$, $p^2 - 1$ is divisible by 24 and hence is a multiple of 3. Therefore,

$$h(p) = p^2 + 3p - 1 = (p^2 - 1) + 3p$$

is a multiple of 3 for all $p > 3$ and hence cannot be prime.

Therefore $h(p) = p^2 + 3p - 1$ is only prime in the single case of the prime $p = 3$.

■

Chapter 6. Factorials

6.1 Sum of Factorials mod k

The general approach is revealed in the following example.

1999 Mu Alpha Theta National Convention, Number Theory Test, Alpha Division, Problem # 6

If $A = \sum_{k=3}^{45} k!$, then what is the remainder when A is divided by 240?

Solution

First note that

$$240 = 2^4 \cdot 3 \cdot 5 \text{ and } 6! = 2^4 \cdot 3^2 \cdot 5 = 240 \cdot 3.$$

It follows that

$$k! = 6! \cdot m_k \text{ for some integer } m_k \text{ for all } k \geq 6$$
$$= 240 \cdot 3 \cdot m_k.$$

For example, $9! = 6! \cdot (9 \cdot 8 \cdot 7)$. Therefore,

$$A = \sum_{k=3}^{45} k! = 3! + 4! + 5! + \sum_{k=6}^{45} k!$$
$$= 3! + 4! + 5! + 240\left(3\sum_{k=6}^{45} m_k\right)$$
$$= 150 + 240\left(3\sum_{k=6}^{45} m_k\right)$$
$$= 150 + 240n \text{ for some integer } n.$$

Hence,

$$A \bmod(240) = \left(\sum_{k=3}^{45} k!\right) \bmod(240) = (150 + 240n) \bmod(240) = 150.$$

■

NATIONAL MU ALPHA THETA CONVENTION 1991

NUMBER THEORY TOPIC TEST

13. Find the remainder when 1! + 2! + 3! + ... + 91! is divided by 15.

A. 3 B. 5 C. 7 D. 9 E. 11

Solution

$1 + 1\cdot 2 + 1\cdot 2\cdot 3 + 1\cdot 2\cdot 3\cdot 4 + 1\cdot 2\cdot 3\,4\cdot 5 + \ldots + 91!$

$1 + 2 + 6 + 24 + 15(8 + \ldots)$

$33 + 15(8 + \ldots)$

$3 + 15(2 + 8 + \ldots)$

$\therefore$ Remainder is 3

■

6.2 Factorial Base Representation of Positive Integers

6.2.1 Definition and Properties

The factorial base representation of the nonnegative integer n (also called the *factoradic* of n) is an expression for n of the form

$$n = a_m \cdot m! + a_{m-1} \cdot (m-1)! + \cdots + a_2 \cdot 2! + a_1 \cdot 1!$$

for some positive integer m with $a_j \in \{0,1, \ldots, j\}$ for each coefficient a_j and $a_m \neq 0$. In this situation, the notation adopted is

$$n = (a_m, a_{m-1}, \ldots, a_1)_!.$$

That is, the coefficient vector $(a_m, a_{m-1}, \ldots, a_1)$ followed by the factorial symbol ! as a subscript.

For example, we could have

$$5 = \mathbf{2}\cdot 2! + \mathbf{1}\cdot 1! \qquad = (\mathbf{2},\mathbf{1})_!$$

$$11 = \mathbf{1}\cdot 3! + \mathbf{2}\cdot 2! + \mathbf{1}\cdot 1! \qquad = (\mathbf{1},\mathbf{2},\mathbf{1})_!$$

$$28 = \mathbf{1}\cdot 4! + \mathbf{0}\cdot 3! + \mathbf{2}\cdot 2! + \mathbf{0}\cdot 1! \qquad = (\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})_!$$

and

$$4700 = \mathbf{6}\cdot 6! + \mathbf{3}\cdot 5! + \mathbf{0}\cdot 4! + \mathbf{3}\cdot 3! + \mathbf{1}\cdot 2! + \mathbf{0}\cdot 1! = (\mathbf{6},\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0})_!.$$

Theorem (Existence and Uniqueness)

There *exists* a *unique* factorial base representation (*i.e. factoradic*) for *every* nonnegative integer n.

A proof by induction of this theorem is straightforward once you establish the following identity as a Lemma.

Lemma

$$\left(1\cdot 1! + 2\cdot 2! + \cdots + (n-1)\cdot(n-1)!\right) + 1 = n!.$$

To understand why this lemma is critical to the theorem, think about the largest number you can generate with the form

$$a_{n-1}\cdot(n-1)! + a_{n-2}\cdot(n-2)! + \cdots + a_2\cdot 2! + a_1\cdot 1!.$$

The largest number occurs when each coefficient a_k is maximized. That is, by taking $a_k = k$. In this case we get

$$(n-1)\cdot(n-1)! + (n-2)\cdot(n-2)! + \cdots + 2\cdot 2! + 1\cdot 1!.$$

This lemma states that the next integer above the largest possible number of the form

$$a_{n-1}\cdot(n-1)! + a_{n-2}\cdot(n-2)! + \cdots + a_2\cdot 2! + a_1\cdot 1!$$

is the integer

$$n! = 1\cdot n! + 0\cdot(n-1)! + 0\cdot(n-2)! + \cdots + 0\cdot 2! + 0\cdot 1!$$

which is the smallest possible number of the form

$$a_n\cdot n! + a_{n-1}\cdot(n-1)! + \cdots + a_2\cdot 2! + a_1\cdot 1!$$

subject to the constraint the leading coefficient $a_n \neq 0$.

You should note that this lemma is the factorial base analogy to how in base 10 the next integer after largest possible integer of the form

$$a_{n-1}\cdot 10^{n-1} + a_{n-2}\cdot 10^{n-2} + \cdots + a_1\cdot 10^1 + a_0 10^0$$

is the smallest possible integer of the form

$$a_n\cdot 10^n + a_{n-1}\cdot 10^{n-1} + \cdots + a_1\cdot 10^1 + a_0 10^0$$

subject to the constraint the leading coefficient $a_n \neq 0$.

For example, the next integer after

$$999 = 9 \cdot 10^2 + 9 \cdot 10^1 + 9 \cdot 10^0$$

is

$$1000 = 1 \cdot 10^3 + 0 \cdot 10^2 + 0 \cdot 10^1 + 0 \cdot 10^0.$$

This lemma can be used repeatedly in an induction argument to show that the factorial base number system does *not repeat* or *skip* any of the positive integers. We will not reproduce all the steps of that argument here but will simply note that the necessary steps can be matched one by one with the steps necessary to show that the base 10 numeration system does not repeat or skip any of the positive integers.

But we will verify that this lemma is true as it can be a useful result in a variety of other situations.

Proof (of Lemma)

$$\begin{aligned}
&\left(1 \cdot 1! + 2 \cdot 2! + \cdots + (n-1) \cdot (n-1)!\right) \\
&\quad = \left(1 \cdot 1! + 2 \cdot 2! + \cdots + (n-1) \cdot (n-1)!\right) + \left(1! + 2! + \cdots + (n-1)!\right) \\
&\qquad\qquad - \left(1! + 2! + \cdots + (n-1)!\right) \\
&\quad = \left(\left(1 \cdot 1! + 1!\right) + \left(2 \cdot 2! + 2!\right) + \cdots + \left((n-1) \cdot (n-1)! + (n-1)!\right)\right) \\
&\qquad\qquad - \left(1! + 2! + \cdots + (n-1)!\right) \\
&\quad = \left(\left(2 \cdot 1!\right) + \left(3 \cdot 2!\right) + \cdots + \left(n \cdot (n-1)!\right)\right) \\
&\qquad\qquad - \left(1! + 2! + \cdots + (n-1)!\right) \\
&\quad = \left(2! + 3! + \cdots + n!\right) - \left(1! + 2! + \cdots + (n-1)!\right) \\
&\quad = n! - 1.
\end{aligned}$$

Therefore,

$$\left(1 \cdot 1! + 2 \cdot 2! + \cdots + (n-1) \cdot (n-1)!\right) + 1 = n!.$$

■

6.2.2 Converting from a Factorial Base to Base 10

Example

Find the base 10 representation of $(3,2,0,6)_!$.

Solution

$$\begin{aligned}
(3,2,0,6)_! &= 3(4!) + 2(3!) + 0(2!) + 1(1!) \\
&= 3(24) + 2(6) + 0(2) + 1(1)
\end{aligned}$$

$$= 72 + 12 + 0 + 1$$
$$= 85.$$

That is, $(3,2,0,6)_! = 85_{10} = 85$.

■

6.2.3 Converting from Base 10 to a Factorial Base: Standard Method

Example

Find the factorial base representation of 1073.

Answer

$$1073 = \mathbf{1}(6!) + \mathbf{2}(5!) + \mathbf{4}(4!) + \mathbf{2}(3!) + \mathbf{2}(2!) + \mathbf{1}(1!) = (\mathbf{1},\mathbf{2},\mathbf{4},\mathbf{2},\mathbf{2},\mathbf{1})_!.$$

Solution

Start by finding the largest integer n for which $n! \leq 1073$. We note that $6! = 720$ but $7! = 5040$. So $n = 6$.

Divide 1073 by $6!$ with remainder.

$$1073 = \mathbf{1} \cdot 6! + 353.$$

Divide the remainder 353 by $5!$ with remainder.

$$353 = \mathbf{2} \cdot 5! + 113.$$

Divide the remainder 113 by $4!$ with remainder.

$$113 = \mathbf{4} \cdot 4! + 17$$

Divide the remainder 17 by $3!$ with remainder.

$$17 = \mathbf{2} \cdot 3! + 5$$

Divide the remainder 5 by $2!$ with remainder.

$$5 = \mathbf{2} \cdot 2! + 1$$

Divide the remainder 1 by $1!$ with remainder.

$$1 = \mathbf{1} \cdot 1!.$$

This shows that

$$\begin{aligned} 1073 &= \mathbf{1} \cdot 6! + 353 \\ &= \mathbf{1} \cdot 6! + \mathbf{2} \cdot 5! + 113 \\ &= \mathbf{1} \cdot 6! + \mathbf{2} \cdot 5! + \mathbf{4} \cdot 4! + 17 \\ &= \mathbf{1} \cdot 6! + \mathbf{2} \cdot 5! + \mathbf{4} \cdot 4! + \mathbf{2} \cdot 3! + 5 \\ &= \mathbf{1} \cdot 6! + \mathbf{2} \cdot 5! + \mathbf{4} \cdot 4! + \mathbf{2} \cdot 3! + \mathbf{2} \cdot 2! + 1 \\ &= \mathbf{1} \cdot 6! + \mathbf{2} \cdot 5! + \mathbf{4} \cdot 4! + \mathbf{2} \cdot 3! + \mathbf{2} \cdot 2! + \mathbf{1} \cdot 1! \\ &= (\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{2}, \mathbf{2}, \mathbf{1})_!. \end{aligned}$$

6.2.4 Converting from Base 10 to a Factorial Base: Bottom Up "Short Cut" Method

The bottom up method for converting from base 10 to a factorial base has some similarities to the bottom up method for converting from base 10 to base b.

Step 1: Solve for a_1

The first step is to divide n by 2 with remainder. That is, express n in the form $n = 2 \cdot d_1 + r_1$ where $r_1 \in \{0,1\}$.

I claim that

$$d_1 = \frac{a_m \cdot m! + a_{m-1} \cdot (m-1)! + \cdots + a_2 \cdot 2!}{2}.$$

To see this, note that each of the terms in the numerator $a_m \cdot m! + a_{m-1} \cdot (m-1)! + \cdots + a_2 \cdot 2!$ are divisible by 2. Therefore d_1 is an integer and we can see that

$$n = 2 \cdot d_1 + a_1$$

where $a_1 \in \{0,1\}$. That is, a_1 equals the remainder when we divide n by 2 with remainder.

Step 2: Solve for a_2

Now divide d_1 by 3 with remainder. That is, express d_1 in the form $d_1 = 3 \cdot d_2 + r_2$ where $r_2 \in \{0,1,2\}$.

I claim that

$$d_2 = \frac{a_m \cdot m! + a_{m-1} \cdot (m-1)! + \cdots + a_3 \cdot 3!}{2 \cdot 3}.$$

To see this, note that each of the terms in the numerator $a_m \cdot m! + a_{m-1} \cdot (m-1)! + \cdots + a_3 \cdot 3!$ are divisible by 2 and 3. Therefore d_2 is an integer and we can see that

$$d_1 = 3 \cdot d_2 + \frac{a_2 \cdot 2!}{2} = 3 \cdot d_2 + a_2$$

where $a_2 \in \{0,1,2\}$. That is, a_2 equals the remainder when we divide d_1 by 3 with remainder.

Step 3: Solve for a_3

Now divide d_2 by 4 with remainder. That is, express d_2 in the form $d_2 = 4 \cdot d_3 + r_3$ where $r_3 \in \{0,1,2,3\}$.

I claim that

$$d_3 = \frac{a_m \cdot m! + a_{m-1} \cdot (m-1)! + \cdots + a_4 \cdot 4!}{2 \cdot 3 \cdot 4}.$$

To see this, note that each of the terms in the numerator $a_m \cdot m! + a_{m-1} \cdot (m-1)! + \cdots + a_4 \cdot 4!$ are divisible by 2, 3 and 4. Therefore d_3 is an integer and we can see that

$$d_2 = 4 \cdot d_3 + \frac{a_3 \cdot 3!}{2 \cdot 3} = 4 \cdot d_3 + a_3$$

where $a_3 \in \{0,1,2,3\}$. That is, a_3 equals the remainder when we divide d_2 by 4 with remainder.

Steps 4,5,… (continue)

We can continue in this same way to find each of the remaining coefficients $a_4, a_5, \ldots$.

Example

We will now illustrate this "bottom up" method for $n = 1073$ and we will note that we get the same set of coefficients $a_1, a_2, \ldots$ as we found using the "standard" approach.

We start by dividing $n = 1073$ by 2 with remainder.

$$n = 2 \cdot d_1 + r_1 = 2(536) + 1 \Longrightarrow a_1 = r_1 = 1.$$

Now divide $d_1 = 536$ by 3 with remainder.

$$d_1 = 3 \cdot d_2 + r_2 = 3(178) + 2 \Longrightarrow a_2 = r_2 = 2.$$

Now divide $d_2 = 178$ by 4 with remainder.

$$d_2 = 4 \cdot d_3 + r_3 = 4(44) + 2 \Longrightarrow a_3 = r_3 = 2.$$

Now divide $d_3 = 44$ by 5 with remainder.

$$d_3 = 5 \cdot d_4 + r_4 = 5(8) + 4 \Longrightarrow a_4 = r_4 = 4.$$

Now divide $d_4 = 8$ by 6 with remainder.

$$d_4 = 6 \cdot d_5 + r_5 = 6(1) + 2 \Longrightarrow a_5 = r_5 = 2.$$

Now divide $d_5 = 1$ by 7 with remainder.

$$d_5 = 7 \cdot d_6 + r_6 = 7(0) + 1 \Longrightarrow a_6 = r_6 = 1.$$

The process stops now because continuing will just verify that $a_7 = a_8 = \cdots = 0$.

So, using the bottom up method we have determined that

$$1073 = (a_6, a_5, a_4, a_3, a_2, a_1)_! = (1,2,4,2,2,1)_!$$

which is the same answer we found using the standard method in the previous section.

■

AMC 1961 Problem #35

The number 695 is to be written with a factorial base of numeration, that is,

$$695 = a_1 + a_2 \cdot 2! + a_3 \cdot 3! + \cdots + a_n \cdot n!$$

where $a_1, a_2, \ldots, a_n$ are integers such that $0 \leq a_k \leq k$, and $n!$ means $n(n-1)(n-2)\cdots 2 \cdot 1$. Find a_4.

(A) 0	(B) 1	(C) 2	(D) 3	(E) 4

Solution

Factorial Base of Numeration

■

Mu Alpha Theta National Convention 2007, Mu Division, Number Theory Test, Problem #24

24) In base-factorial you express a positive integer, b, as $b = a_k a_{k-1} \ldots a_2 a_1$ if $b = a_k \cdot k! + a_{k-1} \cdot (k-1)! + \ldots + a_2 \cdot 2! + a_1 \cdot 1!$ where a_n are integers and $0 \leq a_n < (n+1)!$ for all $1 \leq n \leq k$.
Find 4155 in base-factorial.
A) 498011 B) 537411 C) 523111 D) 543011 E) NOTA

Solution

$$24)\ 4155 = 5 \cdot 6! + 4 \cdot 5! + 3 \cdot 4! + 0 \cdot 3! + 1 \cdot 2! + 1 \cdot 1! \quad 543011\ \mathbf{D}$$

■

6.3 Factorial Base Representation of Rational Numbers

6.3.1 Definitions and Properties

Let $\frac{a}{b}$ be a rational number in reduced form with $0 < \frac{a}{b} < 1$, (*i.e.* in the open unit interval).
The factorial base representation of the rational number $\frac{a}{b}$ is an expression of the form

$$\frac{a}{b} = \frac{d_2}{2!} + \frac{d_3}{3!} + \cdots + \frac{d_m}{m!}$$

for some positive integer m with $d_j \in \{0, 1, \ldots, j-1\}$ for each coefficient d_j.

Terminating and Nonterminating Factorial Base Representations of a Rational Number

Lemma

For all $m \in \{1,2,3,\ldots\}$ we have

$$\frac{1}{m!} = \sum_{i=m}^{\infty} \left(\frac{i}{(i+1)!}\right).$$

Proof

$$\frac{1}{m!} = \frac{1}{m!} + \left(\frac{1}{(m+1)!} + \frac{1}{(m+2)!} + \frac{1}{(m+3)!} + \cdots\right)$$

$$-\left(\frac{1}{(m+1)!} + \frac{1}{(m+2)!} + \frac{1}{(m+3)!} + \cdots\right)$$

$$= \sum_{i=m}^{\infty} \frac{1}{i!} - \sum_{i=m+1}^{\infty} \frac{1}{i!} = \sum_{i=m+1}^{\infty} \frac{1}{(i-1)!} - \sum_{i=m+1}^{\infty} \frac{1}{i!}$$

$$= \sum_{i=m+1}^{\infty} \left(\frac{1}{(i-1)!} - \frac{1}{i!}\right) = \sum_{i=m+1}^{\infty} \left(\frac{i}{i!} - \frac{1}{i!}\right) = \sum_{i=m+1}^{\infty} \left(\frac{i-1}{i!}\right)$$

$$= \sum_{i=m}^{\infty} \left(\frac{i}{(i+1)!}\right).$$

■

For example,

$$\frac{1}{5!} = \frac{5}{6!} + \frac{6}{7!} + \frac{7}{8!} + \frac{8}{9!} + \cdots.$$

The left-hand side of this expression is called the terminating factorial base representation of the rational number $\frac{1}{120} = \frac{1}{5!}$ and the right-hand side is called the nonterminating expression.

For another example, consider the rational number $2/3$.

$$\frac{2}{3} = \frac{1}{2!} + \frac{1}{3!}$$ Terminating Form

$$\frac{2}{3} = \frac{1}{2!} + \frac{0}{3!} + \frac{3}{4!} + \frac{4}{5!} + \frac{5}{6!} + \frac{6}{7!} + \cdots$$ Nonterminating Form

Theorem (Existence and Uniqueness)

There *exists* a *unique*, *terminating form* factorial base representation for *every* rational number in $(0,1)$.

Theorem

If

$$\frac{a}{b} = \frac{d_2}{2!} + \frac{d_3}{3!} + \cdots + \frac{d_m}{m!}$$

is the unique *terminating* form factorial base representation of the rational number $\frac{a}{b}$ then **m will equal the smallest integer such that $m!$ is divisible by b**, the denominator of the rational number $\frac{a}{b}$ in reduced form.

For example …

$m = 3$ for the rational number $\frac{5}{6}$ because $3!$ is divisible by $b = 6$ but $2!$ is not.

$m = 4$ for the rational number $\frac{1}{4}$ because $4!$ is divisible by $b = 4$ but neither $2!$ nor $3!$ are.

$m = 4$ for the rational number $\frac{3}{8}$ because $4!$ is divisible by $b = 8$ but neither $2!$ nor $3!$ are.

$m = 7$ for the rational number $\frac{2}{7}$ because $7!$ is divisible by $b = 7$ but none of $2!, 3!, 4!, 5!, 6!$ are divisible by 7.

6.3.2 Converting from Base 10 to a Factorial Base: Standard (or Greedy) Method

d_2 equals the largest integer number of times that $\frac{1}{2!}$ will go into $\frac{a}{b}$.

d_3 equals the largest integer number of times that $\frac{1}{3!}$ will go into $\frac{a}{b} - \frac{d_2}{2!}$.

d_4 equals the largest integer number of times that $\frac{1}{4!}$ will go into $\frac{a}{b} - \frac{d_2}{2!} - \frac{d_3}{3!}$.

… etc.

Example

Find the factorial base representation of $\frac{5}{8}$.

Answer

$$\frac{5}{8} = \frac{1}{2!} + \frac{0}{3!} + \frac{3}{4!}.$$

Solution

Step 1. Find m.

$m = 4$ for the rational number $\frac{a}{b} = \frac{5}{8}$ because $4!$ is divisible by $b = 8$ but neither $2!$ nor $3!$ are. So we need to find d_2, d_3 and d_4 such that

$$\frac{5}{8} = \frac{d_2}{2!} + \frac{d_3}{3!} + \frac{d_4}{4!}$$

with $d_2 \in \{0,1\}$, $d_3 \in \{0,1,2\}$ and $d_4 \in \{0,1,2,3\}$.

Step 2. Find d_2.

d_2 equals the largest integer number of times that $\frac{1}{2!}$ will go into $\frac{a}{b} = \frac{5}{8}$. That is, d_2 is the largest integer such that

$$\frac{d_2}{2!} \leq \frac{5}{8}.$$

A straightforward way to find this is to divide $5 \cdot 2!$ by 8 with remainder. Now

$$5 \cdot 2! = d_2 \cdot 8 + r_2 = 1 \cdot 8 + 2$$

So $\boldsymbol{d_2 = 1}$ and $r_2 = 2$. But we can also read off $\frac{a}{b} - \frac{d_2}{2!}$ from this calculation. It follows from the result

$$a \cdot 2! = d_2 \cdot b + r_2$$

that

$$\frac{a}{b} - \frac{d_2}{2!} = \frac{r_2}{2! \cdot b} = \frac{2}{2! \cdot 8} = \frac{1}{8}.$$

Note: As we follow through with the next few steps it will become obvious that this result generalizes to

$$\frac{a}{b}-\frac{d_2}{2!}-\frac{d_3}{3!}-\cdots-\frac{d_k}{k!}=\frac{r_k}{k!\cdot b}.$$

Step 3. Find d_3.

d_3 equals the largest integer number of times that $\frac{1}{3!}$ will go into $\frac{a}{b}-\frac{d_2}{2!}=\frac{r_2}{2!\cdot 8}=\frac{1}{8}$. That is, d_3 is the largest integer such that

$$\frac{d_3}{3!}\leq\frac{1}{8}.$$

Proceeding as in the previous step we will divide $1\cdot 3!$ by 8 with remainder.

$$1\cdot 3!=d_3\cdot 8+r_3=0\cdot 8+6$$

So $\boldsymbol{d_3=0}$ and $r_3=6$. We can read off $\frac{a}{b}-\frac{d_2}{2!}-\frac{d_3}{3!}$ from this calculation. It follows from the result

$$1\cdot 3!=d_3\cdot 8+r_3$$

that

$$r_3=1\cdot 3!-d_3\cdot 8$$

$$\frac{r_3}{3!\cdot 8}=\frac{1}{8}-\frac{d_3}{3!}=\left(\frac{a}{b}-\frac{d_2}{2!}\right)-\frac{d_3}{3!}.$$

Step 4. Find d_4.

d_4 equals the largest integer number of times that $\frac{1}{4!}$ will go into

$$\frac{a}{b}-\frac{d_2}{2!}-\frac{d_3}{3!}=\frac{r_3}{3!\cdot 8}=\frac{6}{3!\cdot 8}=\frac{1}{8}.$$

That is, d_4 is the largest integer such that $\frac{d_4}{4!}\leq\frac{1}{8}$.

Continuing in the same manner we will divide $1 \cdot 4!$ by 8 with remainder.

$$1 \cdot 4! = d_4 \cdot 8 + r_4 = 3 \cdot 8 + 0$$

So $\boldsymbol{d_4 = 3}$ and $r_4 = 0$.

The process stops now because we have a remainder of 0. Note that the process stopped with d_4 (*i.e.* $m = 4$) as was predicted.

$$\frac{5}{8} = \frac{d_2}{2!} + \frac{d_3}{3!} + \frac{d_4}{4!} = \frac{1}{2!} + \frac{0}{3!} + \frac{3}{4!}$$

and as a check we note that

$$\frac{1}{2!} + \frac{0}{3!} + \frac{3}{4!} = \frac{1}{2} + \frac{1}{4} = \frac{5}{8}.$$

■

6.3.3 Converting from Base 10 to a Factorial Base: Bottom Up "Short Cut" Method

$$\frac{a}{b} = \frac{d_2}{2!} + \frac{d_3}{3!} + \cdots + \frac{d_m}{m!}$$

Step 1: Solve for $\boldsymbol{d_m}$

We start by multiplying both sides of the defining equation given above by $m!$.

$$\frac{a}{b}m! = \left(\frac{d_2}{2!}m! + \frac{d_3}{3!}m! + \cdots + \frac{d_{m-1}}{(m-1)!}m!\right) + d_m$$

$$= m\left(\frac{d_2}{2!}(m-1)! + \frac{d_3}{3!}(m-1)! + \cdots + \frac{d_{m-1}}{(m-1)!}(m-1)!\right) + d_m$$

$$= mq_1 + d_m$$

Recall that m equals the smallest integer such that $m!$ is divisible by b. It follows that

$$\frac{a}{b}m!$$

is an integer. We can see that

$$q_1 = \frac{d_2}{2!}(m-1)! + \frac{d_3}{3!}(m-1)! + \cdots + \frac{d_{m-1}}{(m-1)!}(m-1)!$$

is an integer. So it follows from the relationship

$$\frac{a}{b}m! = mq_1 + d_m$$

That d_m is the remainder and q_1 is the integer quotient when we divide the integer $\frac{a}{b} \cdot m!$ by m with remainder.

Step 2: Solve for d_{m-1}

Now subtract $\frac{d_m}{m!}$ from $\frac{a}{b}$ and repeat the process.

$$\frac{a}{b} - \frac{d_m}{m!} = \frac{d_2}{2!} + \frac{d_3}{3!} + \cdots + \frac{d_{m-1}}{(m-1)!}$$

Now if we multiply both sides by $(m-1)!$ we find

$$\left(\frac{a}{b} - \frac{d_m}{m!}\right)(m-1)! = \left(\frac{d_2}{2!} + \frac{d_3}{3!} + \cdots + \frac{d_{m-1}}{(m-1)!}\right)(m-1)!$$

$$= \left(\frac{d_2}{2!}(m-1)! + \frac{d_3}{3!}(m-1)! + \cdots + \frac{d_{m-2}}{(m-2)!}(m-1)!\right) + d_{m-1}$$

$$= (m-1)\left(\frac{d_2}{2!}(m-2)! + \frac{d_3}{3!}(m-2)! + \cdots + \frac{d_{m-2}}{(m-2)!}(m-2)!\right) + d_{m-1}$$

$$= (m-1)q_2 + d_{m-1}$$

Following the reasoning as in the previous step we can see that d_{m-1} is the remainder and q_2 is the integer quotient when we divide the integer $\left(\frac{a}{b} - \frac{d_m}{m!}\right)(m-1)!$ by $m-1$ with remainder.

But we don't need to recalculate

$$\left(\frac{a}{b} - \frac{d_m}{m!}\right)(m-1)!$$

because

$$\left(\frac{a}{b}-\frac{d_m}{m!}\right)(m-1)!=\left(\frac{d_2}{2!}+\frac{d_3}{3!}+\cdots+\frac{d_{m-1}}{(m-1)!}\right)(m-1)!$$

$$=\frac{d_2}{2!}(m-1)!+\frac{d_3}{3!}(m-1)!+\cdots+\frac{d_{m-1}}{(m-1)!}(m-1)!=q_1.$$

That is, $q_1=(m-1)q_2+d_{m-1}$.

Hence to find d_{m-1} we simply need to read off the remainder when we divide the previous quotient q_1 by $(m-1)$ with remainder.

The process continues in the same way. We will find $q_2=(m-2)q_3+d_{m-2}$ and so we can find d_{m-2} by reading off the remainder when we divide q_2 by $(m-2)$ with remainder.

… etc.

Example

We will again find the factorial base representation of $\frac{5}{8}$ but this time we will use the "bottom up" process.

Solution

Step 1. Find m.

$m=4$ for the rational number $\frac{a}{b}=\frac{5}{8}$ because $4!$ is divisible by $b=8$ but neither $2!$ nor $3!$ are.
So we need to find d_2, d_3 and d_4 such that

$$\frac{5}{8}=\frac{d_2}{2!}+\frac{d_3}{3!}+\frac{d_4}{4!}$$

with $d_2\in\{0,1\}$, $d_3\in\{0,1,2\}$ and $d_4\in\{0,1,2,3\}$.

Step 2. Find d_4.

We have shown that $d_m=d_4$ is the remainder when we divide $\frac{5}{8}\cdot 4!$ by 4 with remainder.

$$\frac{5}{8} \cdot 4! = 4q_1 + r_1 = 4(3) + 3.$$

Therefore $\boldsymbol{d_4 = r_1 = 3}$ and $q_1 = 3$.

Step 3. Find d_3.

We have shown that $d_{m-1} = d_3$ is the remainder when we divide the previous quotient q_1 by 3 with remainder.

$$q_1 = 3 = 3q_2 + r_2 = 3(1) + 0.$$

Therefore $\boldsymbol{d_3 = r_2 = 0}$ and $q_2 = 1$.

Step 3. Find d_2.

We have shown that d_2 is the remainder when we divide the previous quotient q_2 by 2 with remainder.

$$q_2 = 1 = 2q_3 + r_3 = 2(0) + 1.$$

Therefore $\boldsymbol{d_2 = r_3 = 1}$ and $q_2 = 0$.

So we have verified that

$$\frac{5}{8} = \frac{d_2}{2!} + \frac{d_3}{3!} + \frac{d_4}{4!} = \frac{1}{2!} + \frac{0}{3!} + \frac{3}{4!}$$

using the "bottom up" method.

■

(5D974)

4. There are unique integers $a_2, a_3, a_4, a_5, a_6, a_7$ such that

$$\frac{5}{7} = \frac{a_2}{2!} + \frac{a_3}{3!} + \frac{a_4}{4!} + \frac{a_5}{5!} + \frac{a_6}{6!} + \frac{a_7}{7!},$$

where $0 \le a_i < i$ for $i = 2, 3, \ldots, 7$. Find $a_2 + a_3 + a_4 + a_5 + a_6 + a_7$.

Solution

One Approach: $\frac{5}{7}-\frac{1}{2}=\frac{3}{14}$, $a_2=1$. $\frac{3}{14}-\frac{1}{6}=\frac{1}{21}$, $a_3=1$. $\frac{1}{21}-\frac{1}{24}=\frac{1}{168}$, $a_4=1$.

$\frac{1}{168}-\frac{1}{120}<0$, $a_5=0$, $\frac{1}{168}-\frac{4}{720}=\frac{1}{2520}$, $a_6=4$. $\frac{1}{2520}=\frac{2}{5040}$, $a_7=2$.

$a_2+a_3+a_4+a_5+a_6+a_7=1+1+1+0+4+2=9$.

Second Approach. Multiply each side of the equation by $7!$ to get $3600-a_7=7\cdot6\cdot5\cdot4\cdot3a_2+7\cdot6\cdot5\cdot4a_3+7\cdot6\cdot5a_4+7\cdot6a_5+7a_6$. The right side is divisible by 7, and since $3600=514\cdot7+2$, it must be the case that $a_7=2$. Now divide each side of this equation by 7 and write it as $514-a_6=6\cdot5\cdot4\cdot3a_2+6\cdot5\cdot4a_3+6\cdot5a_4+6a_5$. The right side is divisible by 6, and $514=85\cdot6+4$, so $a_6=4$. Divide each side by 6, and write it as $85-a_5=5\cdot4\cdot3a_2+5\cdot4a_3+5a_4$, and we get $a_5=0$. Divide by 5: $17-a_4=4\cdot3a_2+4a_3$ to get $a_4=1$. Divide by 4 to get $4-a_3=3a_2$, to get $a_3=1$, and $a_2=1$.

■

AMC 1999 Problem #25

There are unique integers $a_2, a_3, a_4, a_5, a_6, a_7$ such that

$$\frac{5}{7}=\frac{a_2}{2!}+\frac{a_3}{3!}+\frac{a_4}{4!}+\frac{a_5}{5!}+\frac{a_6}{6!}+\frac{a_7}{7!},$$

whose $0\le a_i<i$ for $i=2,3,\ldots,7$. Find $a_2+a_3+a_4+a_5+a_6+a_7$.

(A) 8	(B) 9	(C) 10	(D) 11	(E) 12

Solution

Multiply out the 7! to get

$$5\cdot6!=(3\cdot4\cdots7)a_2+(4\cdots7)a_3+(5\cdot6\cdot7)a_4+42a_5+7a_6+a_7.$$

By Wilson's Theorem (or by straightforward division), $a_7+7(a_6+6a_5+\cdots)\equiv5\cdot6!\equiv-5\equiv2\pmod 7$, so $a_7=2$. Then we move a_7 to the left and divide through by 7 to obtain

$$\frac{5\cdot6!-2}{7}=514=360a_2+120a_3+30a_4+6a_5+a_6.$$

We then repeat this procedure $\pmod 6$, from which it follows that $a_6\equiv514\equiv4\pmod 6$, and so forth. Continuing, we find the unique solution to be $(a_2,a_3,a_4,a_5,a_6,a_7)=(1,1,1,0,4,2)$ (uniqueness is assured by the Division Theorem). The answer is $9\implies(\mathrm{B})$.

■

https://oeis.org/wiki/Factorial_numeral_system

The factoradic representation of a rational number $\frac{a}{b}$ (considered in reduced form) in the open unit interval, i.e. $0 < \frac{a}{b} < 1$, is defined as[3]

$$\frac{a}{b} := \sum_{i=1}^{N} \frac{d_i}{(i+1)!}, \quad 0 \le d_i \le i,$$

where d_i, $0 \le d_i \le i$, is the "factoradic digit" for place-value $\frac{1}{(i+1)!}$, and N is the number of "factoradic digits" after the "factoradic point" (N is the smallest integer such that $(N+1)!$ is divisible by the denominator of $\frac{a}{b}$, considered in reduced form).

Note that d_i can't be equal to $i+1$ since

$$\frac{i+1}{(i+1)!} = \frac{1}{i!}.$$

By using only the terminating form for rationals (see factoradic representation of real numbers for the non-terminating form), we get a unique factoradic representation for any rational number by adding the integer part to the fractional part (i.e. within the open unit interval).

You can go backwards instead. Take a non-negative rational p/q. Let $k!$ be the smallest factorial that is divisible by q. then $k!p/q$ is an integer. Define a_k to be the remainder of this number after division by k. Subtract a_k and divide by k. Define a_{k-1} to be the remainder of the result after division by $k-1$ ... Eventually you only need to divide by 1, at that point just take a_1 to be equal to the integer that remains. Uniqueness comes from the uniqueness of the Euclidean division. – user545963 Apr 3, 2018 at 17:42

6.4 Highest Power of p that divides $n!$

Let p be any prime and n any positive integer. If $p^f | n$ and $p^{f+1} \nmid n$, we say that p^f *exactly divides* n and write $p^f \| n$.

Legendre's Theorem

If n is a positive integer and p is a prime, then $p^e \| n!$, where

$$e = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^r} \right\rfloor$$

and r is determined by n by the inequality $p^r \le n < p^{r+1}$.

Alternatively,

If p is prime and if

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

with $a_r \neq 0$ and $0 \leq a_i < p$ for each i, and if $p^e \| n!$, then

$$e = \frac{n - (a_0 + a_1 + \cdots + a_r)}{p - 1}.$$

The second theorem sounds especially remarkable for $p = 2$:

The greatest power of 2 dividing $n!$ is 2^{n-r} where r is the number of 1s in the binary expansion of n.

Also see article "Factoring Factorials"

The number theory texts giving a proof of formula (1) which are listed in the bibliography are [1], [2], [3], [8], [12], [13], [14]. The following exercise can be solved using the formula.

Exercise 1. What are the last 49 digits of 200!? (Finding the last 50 is tougher!)

The computation of g_p can be shortened by using the relation $[x/m] = [[x]/m]$ for x a real number and m a positive integer. Substituting $x = n/p^j$ and $m = p$ we obtain, for $1 \leqslant j \leqslant k - 1$,

$$\left[\frac{n}{p^{j+1}} \right] = \left[\frac{\left[\frac{n}{p^j} \right]}{p} \right].$$

This is especially useful for large values of n. For example, we compute g_{11} for 2000!.

This is especially useful for large values of n. For example, we compute g_{11} for 2000!.

$$g_{11} = \underbrace{\left[\frac{2000}{11} \right]}_{181} + \underbrace{\left[\frac{181}{11} \right]}_{16} + \underbrace{\left[\frac{16}{11} \right]}_{1} = 198. \qquad (*)$$

Alternate Method

Take a close look at computation (*). The work is quite similar to that done in calculating the digits of the base 11 representation of 2000. (To perform the latter calculation, we take the remainder rather than the quotient after each division in (*).) This suggests that there may be a close relationship between the base p representation of an integer n and the computation of g_p. This was shown by the French mathematician Adrien Legendre (1752–1833) [11], who found an alternative method of obtaining the exponent g_p. To derive Legendre's method, first write out the base p representation of the positive integer n. Suppose this is given by

$$n = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0,$$

where $p^k \leqslant n$, $p^{k+1} > n$ and $0 \leqslant m_i \leqslant p - 1$, each i $(0 \leqslant i \leqslant k)$. Then, for $1 \leqslant r \leqslant k$,

$$\frac{n}{p^r} = \frac{m_k p^k + m_{k-1} p^{k-1} + \cdots + m_r p^r}{p^r} + \frac{m_{r-1} p^{r-1} + \cdots + m_1 p + m_0}{p^r}.$$

Since

$$m_{r-1} p^{r-1} + \cdots + m_1 p + m_0 \leqslant (p-1)(p^{r-1} + \cdots + p + 1) = (p-1) \cdot \frac{p^r - 1}{p - 1}$$

$$= p^r - 1 < p^r,$$

we see that

$$\left[\frac{n}{p^r} \right] = m_k p^{k-r} + m_{k-1} p^{k-r-1} + \cdots + m_r.$$

Thus

$$\left[\frac{n}{p} \right] = m_k p^{k-1} + m_{k-1} p^{k-2} + \cdots + m_3 p^2 + m_2 p + m_1$$

$$\left[\frac{n}{p^2} \right] = m_k p^{k-2} + m_{k-1} p^{k-3} + \cdots + m_3 p + m_2$$

$$\left[\frac{n}{p^3} \right] = m_k p^{k-3} + m_{k-1} p^{k-4} + \cdots + m_3$$

$$\vdots$$

$$\left[\frac{n}{p^{k-1}} \right] = m_k p + m_{k-1}$$

$$\left[\frac{n}{p^k} \right] = m_k.$$

Adding these and using formula (1), we obtain

$$\begin{aligned} g_p &= m_k(1 + p + \cdots + p^{k-1}) + m_{k-1}(1 + p + \cdots + p^{k-2}) + \cdots \\ &\quad + m_3(1 + p + p^2) + m_2(1 + p) + m_1 \\ &= m_k \cdot \frac{p^k - 1}{p - 1} + m_{k-1} \cdot \frac{p^{k-1} - 1}{p - 1} + \cdots \\ &\quad + m_3 \cdot \frac{p^3 - 1}{p - 1} + m_2 \cdot \frac{p^2 - 1}{p - 1} + m_1 \cdot \frac{p - 1}{p - 1} \\ &= \frac{\left((m_k p^k + m_{k-1} p^{k-1} + \cdots + m_3 p^3 + m_2 p^2 + m_1 p + m_0)\right.}{\left.- (m_k + m_{k-1} + \cdots + m_3 + m_2 + m_1 + m_0)\right)} \\ &\quad \frac{}{p - 1} \\ &= \frac{n - s_p}{p - 1}, \end{aligned}$$

where $s_p = m_k + \cdots + m_0$ is the sum of the digits of n to the base p.

Using the formula

$$g_p = \frac{n - s_p}{p - 1}, \tag{2}$$

we obtain the prime factorization of 20! as follows:

p	Base p representation of 20	s_p	$\frac{20 - s_p}{p - 1} = g_p$
2	10100_2	2	$20 - 2 = 18$
3	202_3	4	$\frac{20 - 4}{3 - 1} = 8$
5	40_5	4	$\frac{20 - 4}{5 - 1} = 4$
7	26_7	8	$\frac{20 - 8}{7 - 1} = 2$
11	19_{11}	10	$\frac{20 - 10}{11 - 1} = 1$
13	17_{13}	8	$\frac{20 - 8}{13 - 1} = 1$
17	13_{17}	4	$\frac{20 - 4}{17 - 1} = 1$
19	11_{19}	2	$\frac{20 - 2}{19 - 1} = 1$

This gives us $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11^1 \cdot 13^1 \cdot 17^1 \cdot 19^1$.

The references listed in the bibliography giving formula (2) are [2], [3], [12], [13]. Formula (2) can be used to solve the following exercises.

Exercise 2. Show that the exponent of the greatest power of p dividing $(p^k - 1)!$ is

$$\frac{p^k - (p-1)k - 1}{p - 1}.$$

Exercise 3. Find an integer $n \geqslant 1$ such that the exponent of the greatest power of 3 dividing $n!$ is 50. (Hint: Since s_3 is at least 1, begin by considering the equation $(n - 1)/2 = 50$.)

As a special case of formula (2), take $p = 2$. Then $p - 1 = 1$ and so $g_2 = n - s_2$, or $n = g_2 + s_2$. That is, any integer n is the sum of the greatest power of 2 dividing $n!$ and the sum of its digits to the base 2. (See [9].) For example, the base 2 representation of 17 is 10001_2. Hence $s_2 = 1 + 0 + 0 + 0 + 1 = 2$. As we already showed, $g_2 = 15$ for 17!. Thus $g_2 + s_2 = 15 + 2 = 17$. Notice that, in general, the equation $g_2 = n - s_2$ implies that the exponent of the greatest power of 2 dividing $(2^k + 1)!$ is $2^k - 1$.

We have remarked that formula (1) with shortcut (*) is easily computed with a calculator. Formula (2), on the other hand, requires a conversion to base p, which takes time. Which is faster? In order to find out, I timed myself using both methods on the prime factorizations of 20!, 50! and 100!. In each case the former method took about half as long as the latter to yield the prime factorization.

Number Theory

Naoki Sato <sato@artofproblemsolving.com>

The number of factors of the prime p in $\binom{m}{k}$ is

$$\gamma = \sum_{s=1}^{r} \left(\left\lfloor \frac{m}{p^s} \right\rfloor - \left\lfloor \frac{k}{p^s} \right\rfloor - \left\lfloor \frac{m-k}{p^s} \right\rfloor \right)$$

where r is the largest integer such that $p^s \leq k$ and $p^s \leq m-k$.

1999 Mu Alpha Theta National Convention, Number Theory Test, Alpha Division, Problem #22

Suppose m is an integer such that $m = \binom{151}{9} = \frac{151!}{142!\,9!}$. Find the largest prime divisor of m.

Solution

$n | \binom{n}{k}$ whenever $\gcd(k,n) = 1$. Note this is a sufficient condition but not a necessary one. For example, $10 | \binom{10}{4} = 210$ but $\gcd(10,4) \neq 1$.

It is a classical result that $p | \binom{p}{k}$ for all k whenever p is prime.

In the above problem we simply need to note that 151 is prime. Therefore, the largest prime divisor of $\binom{151}{9}$ is 151.

https://math.stackexchange.com/questions/545962/when-is-binomnk-divisible-by-n

■

Example

Let $n = 28$ and let $p = 3$. Then

$$e = \left\lfloor \frac{28}{3} \right\rfloor + \left\lfloor \frac{28}{9} \right\rfloor + \left\lfloor \frac{28}{27} \right\rfloor = 9 + 3 + 1 = 13$$

and hence by Theorem 2.29,

$$p^{13} \| 28!$$

Pg. 65

By Theorem 2.28,

$$\left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{n}{p^{k-1}} \right\rfloor}{p} \right\rfloor$$

so, we can simplify this algorithm a bit to

$$e = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor}{p} \right\rfloor + \cdots$$

In particular,

$$e = \left\lfloor \frac{28}{3} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{28}{3} \right\rfloor}{3} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{\left\lfloor \frac{28}{3} \right\rfloor}{3} \right\rfloor}{3} \right\rfloor = 9 + \left\lfloor \frac{9}{3} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{9}{3} \right\rfloor}{3} \right\rfloor = 9 + 3 + 1.$$

The preceding computation of the exponent of 3 in the canonical representation of $28!$ bears a marked resemblance to the calculation of the digits in the positional representation of 28 to base 3. That this resemblance is more than superficial is shown by the following theorem.

Pg. 66, Theorem 2.30

If p is prime and if

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

with $a_r \neq 0$ and $0 \leq a_i < p$ for each i, and if $p^e \| n!$, then

$$e = \frac{n - (a_0 + a_1 + \cdots + a_r)}{p - 1}.$$

Example

Note that $28_{10} = 1001_3$. Therefore, using the formula of Theorem 2.30, we again obtain

$$e = \frac{28 - (1 + 0 + 0 + 1)}{3 - 1} = 13$$

as the exponent of 3 such that $3^e \| 28!$

Theorem

There are

$$\left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{5^2} \right\rfloor + \left\lfloor \frac{n}{5^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{5^k} \right\rfloor$$

zeros are there at the end of $n!$ where k is that integer such that $5^k \leq n < 5^{k+1}$.

Example

How many zeros are there at the end of $1000!$?

Solution

There are $\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{25} \right\rfloor + \left\lfloor \frac{1000}{125} \right\rfloor + \left\lfloor \frac{1000}{625} \right\rfloor = 249$ zeros at the end of $1000!$

■

The following problem is an interesting twist on the problem of counting the number of zeros at the end of $n!$.

Exercise (Source: 2005 Lehigh University High School Math Contest, Problem #25)

How many 0's occur at the end of the decimal expansion of $100^{100} - 100!$?

Solution

$100!$ has

$$\left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor + \left\lfloor \frac{100}{5^3} \right\rfloor + \cdots = 20 + 4 + 0 + \cdots = 24$$

terminal zeros. In contrast, $100^{100} = 10^{200}$ has 200 terminal zeros.

It follows that

$$100^{100} - 100! = 1 \cdot 10^{200} + \cdots + c_{24}10^{24} + c_{23}10^{23} + \cdots + c_1 10^1 + c_0 10^0$$

$$= - \begin{array}{r} 1 \cdot 10^{200} + 0 \cdot 10^{199} + \cdots + 0 \cdot 10^r + \cdots + 0 \cdot 10^{24} + 0 \cdot 10^{23} + \cdots + 0 \cdot 10^1 + 0 \cdot 10^0 \\ a_r \cdot 10^r + \cdots + a_{24} \cdot 10^{24} + 0 \cdot 10^{23} + \cdots + 0 \cdot 10^1 + 0 \cdot 10^0 \end{array}$$

for some nonzero base 10 digits a_r and a_{24}. Written in this form we can see that $c_{24} = 10 - a_{24} \neq 0$ while $c_{23} = c_{22} = \cdots = c_1 = c_0 = 0$.

That is $100^{100} - 100!$ has the same number of terminal zeros as $100!$, namely 24.

■

Exercise

Pg. 68, Ex. 9

Find the exponent e such that $3^e \| 91!$

Solution

■

Exercise

Pg. 68, Ex. 10

Prove that 3 does not divide the binomial coefficient $\binom{91}{10}$.

Solution

■

Exercise

Pg. 68, Ex. 11

Find the highest power of 10 that divides $91!$

Solution

■

Exercise

14. Let n be a positive integer. Show that the power of the prime p occurring in the prime-power factorization of $n!$ is

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots.$$

Solution

■

Exercise

15. Use Exercise 14 to find the prime-power factorization of $20!$.

Solution

The largest prime in $20!$ is 19. So

$$20! = 2^{a_2}3^{a_3}5^{a_5}7^{a_7}11^{a_{11}}13^{a_{13}}17^{a_{17}}19^{a_{19}}$$

where

$$a_p = \left[\frac{20}{p}\right] + \left[\frac{20}{p^2}\right] + \left[\frac{20}{p^3}\right] + \cdots.$$

■

Exercise

16. How many zeros are there at the end of $1000!$ in decimal notation? How many in base eight notation?

$$a_5 = \left[\frac{1000}{5}\right] + \left[\frac{1000}{25}\right] + \left[\frac{1000}{125}\right] + \left[\frac{1000}{625}\right]$$

Solution

■

Source: MSHSML 4T046

6. Find the largest integer n for which 7^n will divide 600! (That's 600 factorial.)

Solution

The factors
$1 \cdot 2 \cdots [7] \cdots 2[7] \cdots 594 \cdot [85 \cdot 7] \cdots$
contribute 85 7's.

The factors
$1 \cdot 2 \cdots [1 \cdot 49] \cdots [12 \cdot 49] \cdots$
contribute an additional
12 7's.

The factor $[7^3]$ contri
butes 1 more 7,

$85 + 12 + 1 = 98$

■

(3T815)

Meet 3, 1981-82 Team Event

5. By definition, $n! = n(n-1)(n-2) \cdots (2)(1)$; thus, $5! = 120$, $6! = 720$, etc.

What is the highest power of 3 that will divide $100!$?

Solution

$$\left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{9} \right\rfloor + \left\lfloor \frac{100}{27} \right\rfloor + \left\lfloor \frac{100}{81} \right\rfloor = 33 + 11 + 3 + 1 = 48.$$

■

6.5 Highest Power of p that divides $n!$ in Base b

6.6 Number of Terminal Zeroes in $n!$ Base 10

(4C002)

2. If written out as an integer, the number 50! would terminate in a series of zeroes. How many?

Solution

There are more than 25 factors of 2, plenty to pair with available 5's. Count 5's.
$50! = 1\cdot 2\cdots \underline{5}\cdot 6\cdots 9\,(2\cdot\underline{5})\,11\cdots(3\cdot\underline{5})\cdot 16\cdots(4\cdot\underline{5})\cdots(\underline{5}\cdot\underline{5})\cdots(6\cdot\underline{5})\cdots\cdots(9\cdot\underline{5})\cdots(2\cdot\underline{5}\cdot\underline{5})$
There are twelve factors of 5, hence twelve 0's.

■

Mu Alpha Theta National Convention 2007, Mu Division, Number Theory Test, Problem #12

12) Find the number of zeros at the end of $(2007!)^2$.

A) 499 B) 500 C) 999 D) 1,000 E) NOTA

Solution

12) The number of zeros in 2007! is found by dividing 2007 by powers of 5:
$\lfloor 2007/5\rfloor = 401, \lfloor 2007/25\rfloor = 80, \lfloor 2007/125\rfloor = 16, \lfloor 2007/625\rfloor = 3;\ 401+80+16+3 = 500.$
When raising a number to a power, we multiply the power by the number of zeros to get the total number of zeros: $500\cdot 2 = 1000$ **D**

■

6.7 Number of Terminal Zeroes in $n!$ Base b

https://math.stackexchange.com/questions/1563986/factorials-in-different-base

Suppose that $b = p_1^{k_1}p_2^{k_2}\cdots p_t^{k_t}$.

Let

$$m_i = \frac{1}{k_i}\left(\left\lfloor\frac{n}{p_i}\right\rfloor + \left\lfloor\frac{n}{(p_i)^2}\right\rfloor + \left\lfloor\frac{n}{(p_i)^3}\right\rfloor + \cdots\right).$$

Then the number of trailing zeros of $n!$ in base b will be

$$\min_i\left(\lfloor m_i\rfloor\right).$$

(not yet positive about this but I'm starting to believe it)

How do I find the number of trailing zeroes of N factorial in Base B?

If B is prime, search for the exponent of B in the prime factorization of $N!$,

$$\exp_B = \left\lfloor \frac{n}{B} \right\rfloor + \left\lfloor \frac{n}{B^2} \right\rfloor + \cdots$$

(keep adding terms until you obtain zero, i.e., until $B^k > n$). $\exp_B$ is the number of trailing zeroes.

If B is not prime, but is the product of prime factors to the first power, choose the greater of them (say p) and perform the above calculation for it. $\exp_p$ will be the number we're searching for.

If there are repeated prime factors, be more careful. For example, if $B = 12 = 2^2 \cdot 3$, calculate $\exp_2$ and $\exp_3$, and then compare $\lfloor \exp_2 /2 \rfloor$ with $\exp_3$. The least of them will work. For example, if $n = 8$, $\exp_2 = 7$ and $\exp_3 = 2$, hence $\lfloor \exp_2 /2 \rfloor = 3 > \exp_3$, but if $n = 9$, $\exp_2 = 7$, and $\exp_3 = 4$, then the relation is reverted.

This doesn't mean we need to calculate every exponent, for example if $B = 60 = 2^2 \cdot 3 \cdot 5$, $\exp_3$ will be ever less than $\exp_5$, therefore there is no need to calculate $\exp_3$. On the other hand, $\exp_5$ is always less or equal to $\exp_2 /2$, and hence the only exponent we need is $\exp_5$.

For 10 we check the largest prime factor powers(powers of 5) of 10. So in any base we should find the number of largest prime factor exponent of 10(in that base). For example in base 26, it's 13.

(unsure about this)

(TD864) When written in base three, a positive integer p has two terminal zeroes. When written in base four or five, the integer p has one terminal zero. In how many positive integral bases greater than one, other than those already mentioned, must the representation of p have at least one terminal zero?
Solution

a base b

If $p_{10} = c_r \cdot b^r + c_{r-1}b^{r-1} + \cdots + c_1 b^1 + c_0$ where b is an integer greater than or equal to 2 and $c_j \in \{0,1,2, \ldots, b-1\}$ for each $j = 0,1, \ldots, r$, then we write $p_{10} = a_b$ where

$$a_b = \left(\underline{c_r}\ \underline{c_{r-1}} \cdots \underline{c_1}\ \underline{c_0}\right).$$

For example, we write

$$8931_{10} = 35016_7.$$

because

$$8931_{10} = 8931 = \underline{3} \cdot 7^4 + \underline{5} \cdot 7^3 + \underline{0} \cdot 7^2 + \underline{1} \cdot 7^1 + \underline{6} \cdot 7^0.$$

Terminal Zeroes in Base b

Suppose $p_{10} = \left(\underline{c_r}\ \underline{c_{r-1}} \cdots \underline{c_k}\ \underbrace{00 \cdots 00}_{k \text{ zeroes}}\right)_b$ with $r > k$. That is suppose

$$p_{10} = c_r \cdot b^r + c_{r-1}b^{r-1} + \cdots + c_k b^k + \underbrace{0 \cdot b^{k-1} + \cdots + 0 \cdot b^1 + 0}_{k \text{ zeroes}}.$$

In this case we can factor out b^k.

$$\begin{aligned} p_{10} &= c_r \cdot b^r + c_{r-1}b^{r-1} + \cdots + c_k b^k \\ &= b^k(c_r \cdot b^{r-k} + c_{r-1}b^{r-1-k} + \cdots + c_k). \end{aligned}$$

This shows that

$$\boxed{p_{10} = \left(\underline{c_r}\ \underline{c_{r-1}} \cdots \underline{c_k}\ \underbrace{00 \cdots 00}_{k \text{ zeroes}}\right)_b \iff b^k | p_{10}.}$$

Recall that $b^k | p_{10}$ means that b^k divides p_{10} or equivalently b^k is a factor of p_{10}. We need this result to solve this problem.

In this problem we are given the information that the base 3 representation of p (base 10) has (at least) 2 terminal zeroes and when p is represented in base four or five, the integer p has (at least) one terminal zero.

From our above result this tells us that

$$\begin{aligned} &\underline{\text{Base } 3} \quad p = \star \cdots \star\, 00 \implies 3^2 | p \\ &\underline{\text{Base } 4} \quad p = \star \cdots \star\star\, 0 \implies 4^1 | p \\ &\underline{\text{Base } 5} \quad p = \star \cdots \star\star\, 0 \implies 5^1 | p. \end{aligned}$$

From here it follows that

$$p = 3^2 \cdot 4^1 \cdot 5^1 \cdot \boldsymbol{m} = 3^2 \cdot 2^2 \cdot 5^1 \cdot \boldsymbol{m}$$

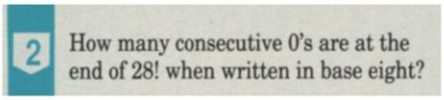
where $\boldsymbol{m}$ is an arbitrary integer.

Now we come back to the original question. For what positive integral bases greater than one, other than bases 3, 4 and 5, *must* the representation of p have at least **one** terminal zero? What about base 6? Can we be sure that $6^1 | p$? We can see that it does because

$$p = 3^2 \cdot 2^2 \cdot 5^1 \cdot \boldsymbol{m} = \boldsymbol{6^1} \cdot 3^1 \cdot 2^1 \cdot 5^1 \cdot \boldsymbol{m}.$$

It is clear that every base number b of the form $b = 2^{r_1}3^{r_2}5^{r_3}$ with $r_1 \in \{0,1,2\}$, $r_2 \in \{0,1,2\}$, and $r_3 \in \{0,1\}$ will divide $p = 3^2 \cdot 2^2 \cdot 5^1 \cdot \boldsymbol{m}$.
This leads to the enumeration problem where there are 3 choices for r_1, 3 choices for r_2 and 2 choices for r_3. Combined this leads to a total of $3 \times 3 \times 2 = 18$ base numbers – *except* that this includes $b = 1,3,4,5$ which we were told to not include in the final count.
Hence there are $18 - 4 = 14$ additional base numbers where p expressed in that base *must* have at least one terminal zero.

■



December 1992

2 Find the highest power of 2 that divides 28!

$28-2^2$ $18-2^1$ $8-2^3$
$26-2^1$ $16-2^4$ $6-2^1$
$24-2^3$ $14-2^1$ $4-2^2$
$22-2^1$ $12-2^2$ $2-2^1$
$20-2^2$ $10-2^1$

Thus 2^{25} is the highest power of 2 that divides 28! Since $8^8 = (2^3)^8 = 2^{24}$, 8 divides 28! eight times and so 8 zeros result at the end of 28! (base eight).

AMC 1965 Problem #33
If the number $15!$, that is, $15 \cdot 14 \cdot 13 \cdots 1$, ends with k zeros when given to the base 12 and ends with h zeros when give to the base 10, then $k + h$ equals:

(A) 5	(B) 6	(C) 7	(D) 8	(E) 9

Solution

■

AMC 1970 Problem #23
The number $10!$ (10 is written in base 10), when written in the base 12 system, ends with exactly k zeros. The value of k is

(A) 1	(B) 2	(C) 3	(D) 4	(E) 5

Solution

■

1999 Mu Alpha Theta National Convention, Number Theory Test, Alpha Division, Problem #26
How many zeros are at the end of $(22!)^2$ when it's written in base 4?
Solution
Suppose $m_{10} = n_b$. That is, the base 10 m equals the base b integer n. Then the number of zeros at the end of n_b equals the largest positive integer k such that $b^k | m_{10}$.
So, in this problem we are looking for the largest k such that $4^k | (22!)^2$.
From Legendre's Theorem we know that if n is a positive integer and p is a prime, then $p^e \| n!$, where

$$e = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^r} \right\rfloor$$

and r is determined by n by the inequality $p^r \leq n < p^{r+1}$.

This problem comes with two "twists". First the base 10 number of interest is $(22!)^2$ instead of just $22!$. (*i.e.* Legendre's Theorem does not *directly* apply.)

The second "twist" we want to find the highest power of 4 that divides our number of interest and 4 is not a prime number. (*i.e.* we have a second reason why Legendre's Theorem does not *directly* apply.)
However, if $p^k \| n$ for some prime p, then $(p^2)^k \| n^2$. Applying this result to our problem, if $2^k \| 22!$ then $4^k \| (22!)^2$.

But Legendre's Theorem applies directly to finding the value of k such that $2^k \| 22!$. From Legendre's Theorem we see that

$$k = \left\lfloor \frac{22}{2} \right\rfloor + \left\lfloor \frac{22}{4} \right\rfloor + \left\lfloor \frac{22}{8} \right\rfloor + \left\lfloor \frac{22}{16} \right\rfloor = 11 + 5 + 2 + 1 = 19.$$

Therefore, the largest k such that $4^k \| (22!)^2$ must be 19.

■

Note: We could have also used the result:

If p is prime and if

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

with $a_r \neq 0$ and $0 \leq a_i < p$ for each i, and if $p^e \| n!$, then

$$e = \frac{n - (a_0 + a_1 + \cdots + a_r)}{p - 1}.$$

■

6.8 Sum of Factorials Mod n

(Koshy, page 242)

Find the remainder when

20. $1! + 2! + \cdots + 100!$ is divided by 11.
21. $1! + 2! + \cdots + 300!$ is divided by 13.

EXAMPLE 4.4 Find the remainder when $1! + 2! + \cdots + 100!$ is divided by 15.

SOLUTION

Notice that when $k \geq 5$, $k! \equiv 0 \pmod{15}$ (why?). Therefore,

$$\begin{aligned} 1! + 2! + \cdots + 100! &\equiv 1! + 2! + 3! + 4! + 0 + \cdots + 0 \pmod{15} \\ &\equiv 1 + 2 + 6 + 24 \pmod{15} \\ &\equiv 1 + 2 + 0 \pmod{15} \\ &\equiv 3 \pmod{15} \end{aligned}$$

Thus, when the given sum is divided by 15, the remainder is 3. ■

6.9 Extra Factorial Problems

Mu Alpha Theta National Convention 2007, Mu Division, Number Theory Test, Problem #10

10) Find the largest positive integer, n, such that $n!$ is NOT congruent to $0 \pmod{200}$.
A) 10 B) 50 C) 100 D) 200 E) NOTA

Solution

10) $200 = 2^3 \cdot 5^2$ In order for $n!$ to not be congruent to $0 \pmod{200}$, then it cannot contain all of the factors of 200. $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$ which is congruent to $0 \pmod{200}$ and $9! = 2^7 \cdot 3^4 \cdot 5 \cdot 7$ which is not congruent. Thus the largest value is 9 **E**

■

AMC 1965

33. If the number 15!, that is, $15 \cdot 14 \cdot 13 \cdots 1$, ends with k zeros when given to the base 12 and ends with h zeros when given to the base 10, then $k + h$ equals:

(A) 5 (B) 6 (C) 7 (D) 8 (E) 9

Solution

■

Chapter 7. Linear Congruence Equations

Develop more before launching into systems

Theorem

If $a, b, c_1, c_2, \ldots, c_n \in \mathbb{Z}$ and if $c_1, c_2, \ldots, c_n$ are pairwise relatively prime, then

$$a \equiv b \bmod (c_1 \cdot c_2 \cdots c_n) \iff \begin{array}{c} a \equiv b \bmod c_1 \\ a \equiv b \bmod c_2 \\ \vdots \\ a \equiv b \bmod c_{n-1} \\ a \equiv b \bmod c_n \end{array}$$

15 Find the smallest number that when divided by each of the integers 2, 3, 4, 5, 6, 7, 8, 9, and 10 will give a remainder that is 1 less than the divisor.

January 1989

Let x be the number. Then

$$x \bmod(2) = 1 \Longrightarrow (x+1) \bmod(2) = 0$$
$$x \bmod(3) = 2 \Longrightarrow (x+1) \bmod(3) = 0$$
$$x \bmod(4) = 3 \Longrightarrow (x+1) \bmod(4) = 0$$
$$x \bmod(5) = 4 \Longrightarrow (x+1) \bmod(5) = 0$$
$$x \bmod(6) = 5 \Longrightarrow (x+1) \bmod(6) = 0$$
$$x \bmod(7) = 6 \Longrightarrow (x+1) \bmod(7) = 0$$
$$x \bmod(8) = 7 \Longrightarrow (x+1) \bmod(8) = 0$$
$$x \bmod(9) = 8 \Longrightarrow (x+1) \bmod(9) = 0$$
$$x \bmod(10) = 9 \Longrightarrow (x+1) \bmod(10) = 0$$

$\Longrightarrow$

$x + 1$ is divisible by 2,3,4,5,6,7,8,9 and 10.

The LCM(2,3,4,5,6,7,8,9,10) is the smallest integer divisible by all these numbers.

$$x + 1 = \text{LCM}(2,3,4,5,6,7,8,9,10)$$
$$x = \text{LCM}(2,3,4,5,6,7,8,9,10) - 1$$
$$x = 2520 - 1 = 2519.$$

2.2 Linear congruences in one variable

Theorem 2.7 (Solutions of linear congruences in one variable)**.** *Let $a, b \in \mathbf{Z}$ and $m \in \mathbf{N}$, and consider the congruence*

$$ax \equiv b \bmod m. \tag{2.1}$$

Let $d = (a, m)$.

(i) *(Existence of a solution) The congruence (2.1) has a solution $x \in \mathbf{Z}$ if and only if $d \mid b$.*

(ii) *(Number of solutions) Suppose $d \mid b$. Then $ax \equiv b \bmod m$ has exactly d pairwise incongruent solutions x modulo m. The solutions are of the form $x = x_0 + km/d$, $k = 0, 1, \ldots, d-1$, where x_0 is a particular solution.*

(iii) *(Construction of a solution) Suppose $d \mid b$. Then a particular solution can be constructed as follows: Apply the Euclidean algorithm to compute $d = (a, m)$, and, working backwards, obtain a representation of d as a linear combination of a and m. Multiply the resulting equation through with (b/d). The new equation can be interpreted as a congruence of the desired type, (2.1), and reading off the coefficient of a gives a particular solution.*

Corollary 2.8. *Let $a \in \mathbf{Z}$ and $m \in \mathbf{N}$. If $(a, m) = 1$, the congruence*

$$ax \equiv 1 \bmod m \tag{2.2}$$

has a unique solution x modulo m; if $(a, m) \neq 1$, the congruence has no solution.

Definition 2.9 (Modular inverses)**.** *A solution x to the congruence (2.2), if it exists, is called a **modular inverse of** a (with respect to the modulus m) and denoted by $\overline{a}$.*

Remark. Note that $\overline{a}$ is not uniquely defined. The definition depends implicitly on the modulus m. In addition, for a given modulus m, $\overline{a}$ is only *unique modulo* m; i.e., any $x \in \mathbf{Z}$ with $x \equiv \overline{a} \bmod m$ is also a a modular inverse of m.

7.1 Chinese Remainder Theorem

Theorem 2.10 (Chinese Remainder Theorem)**.** *Let $a_1, \ldots, a_r \in \mathbf{Z}$ and let $m_1, m_2, \ldots, m_r \in \mathbf{N}$ be given such that $(m_i, m_j) = 1$ for $i \neq j$. Then the system*

$$x \equiv a_i \bmod m_i \qquad (i = 1, \ldots, r) \tag{2.3}$$

has a unique solution x modulo $m_1 \cdots m_r$.

Corollary 2.11 (Structure of residue systems modulo $m_1 \cdots m_r$)**.** *Let $m_1, \ldots, m_r \in \mathbf{N}$ with $(m_i, m_j) = 1$ for $i \neq j$ be given and let $m = m_1 \cdots m_r$. There exists a 1-1 correspondence between complete systems of residues modulo m and r-tupels of complete systems of residues modulo $m_1, \ldots, m_r$. More precisely, if, for each i, a_i runs through a complete system of residues modulo m_i, then the corresponding solution x to the simultaneous congruence (2.3) runs through a complete system of residues modulo m.*

Theorem

Let $a_1, a_2 \ldots, a_r \in \mathbb{Z}$ (set of integers) and let $m_1, m_2, \ldots, m_r \in \mathbb{N}$ (set of positive integers) with $(m_i, m_j) = 1$ for $i \neq j$ be given. Let $M = m_1 \cdot m_2 \cdots m_r$. Let $M_i = M/m_i$. Then the single congruence equation

$$\left(\sum_{i=1}^{r} M_i\right) x \equiv \sum_{i=1}^{r} M_i a_i \pmod{M}$$

has the same unique solution $(\bmod M)$ as the system of equations

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}. \end{aligned}$$

Systems of Linear Congruences

A general system of simultaneous linear congruences

$$\begin{aligned} a_1x &\equiv b_1 \pmod{n_1} \\ a_2x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_rx &\equiv b_r \pmod{n_r} \end{aligned}$$

can be simplified to the form

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_r \pmod{m_r} \end{aligned}$$

by dividing each congruence through by (a_i,n_i), then multiplying by the inverse mod $m_i = \frac{n_i}{(a_i,n_i)}$ of the coefficient $\frac{a_i}{(a_i,n_i)}$. The simplified system may or may not be solvable, but in any case, it must have the same set of solutions as the original system.

Theorem 1. *If $(a, m) = 1$, then the congruence $ax \equiv b \pmod{m}$ phas exactly one solution modulo m.*

Theorem 2. *Consider the congruence $ax \equiv b \pmod{m}$.*

1. *The congruence has a solution if and only if $(a, m) \mid b$.*
2. *If u_0 is any particular solution, then a complete set of solutions is:*

$$u_0, u_0 + \frac{m}{g}, u_0 + \frac{2m}{g}, \ldots, u_0 + \frac{(g-1)m}{g}$$

where $g = (a, m)$. Thus there are g solutions.

3. *A particular solution u_0 can be obtained by solving the congruence*

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$$

This is possible since $\left(\frac{a}{g}, \frac{m}{g}\right) = 1$. (See last theorem.)

Generalization to non-coprime moduli [edit]

The Chinese remainder theorem can be generalized to non-coprime moduli. Let m, n, a, b be any integers, let $g = \gcd(m, n)$, and consider the system of congruences:

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n},$$

If $a \equiv b \pmod{g}$, then this system of equations has a unique solution modulo $\operatorname{lcm}(m, n) = mn/g$. Otherwise, it has no solutions.

If we use Bézout's identity to write $g = um + vn$, then the solution is

$$x = \frac{avn + bum}{g}.$$

This defines an integer, as g divides both m and n. Otherwise, the proof is very similar to that for coprime moduli.

https://forthright48.com/chinese-remainder-theorem-part-2-non-coprime-moduli/

To prove this, we begin by observing a general principle: *if a and b are relatively prime, then two simultaneous congruences of the form*

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b} \tag{7}$$

are precisely equivalent to one congruence to the modulus ab. For the first

Example Illustrating the Chinese Remainder Theorem

Find the least nonnegative solution of the system of linear congruences

$$x \equiv 1 \bmod 2$$
$$x \equiv 2 \bmod 3$$
$$x \equiv 1 \bmod 5$$
$$x \equiv 5 \bmod 7.$$

Answer: 131.

Proof:

By the Chinese remainder theorem, provided the moduli ($m_1 = 2, m_2 = 3, m_3 = 5$, and $m_4 = 7$) are pairwise relatively prime, there will be a unique solution x' (modulo $M = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$) of the form

$$x' = b_1 M_1 x_1 + b_2 M_2 x_2 + b_3 M_3 x_3 + b_4 M_4 x_4$$

where $b_1 = \mathbf{1}, b_2 = \mathbf{2}, b_3 = \mathbf{1}$, and $b_4 = \mathbf{5}$, $M_i = M/m_i$ and x_i is the unique solution to $M_i x \equiv 1 \bmod m_i$.

Clearly, the moduli 2,3,5 and 7 are pairwise relatively prime so we can proceed to find x' via the CRT (Chinese remainder theorem).

First, we need to find the $M_i = M/m_i$.

$$M_1 = 210/2 = 105$$
$$M_2 = 210/3 = 70$$
$$M_3 = 210/5 = 42$$
$$M_4 = 210/7 = 30.$$

The next step is find the x_i, the solutions to the linear congruences $M_i x \equiv 1 \bmod m_i$. That is, solve

$$105\ x_1 \equiv 1 \bmod 2$$
$$70\ x_2 \equiv 1 \bmod 3$$
$$42\ x_3 \equiv 1 \bmod 5$$
$$30\ x_4 \equiv 1 \bmod 7.$$

(Remember that part of the proof of the CRT was to show that the x_i will exist and will be unique modulo m_i.)

We have already learned how we can work back up through the Euclidean algorithm or by using Blankinship's algorithm to solve the general linear congruence $ax \equiv b \bmod m$ (Section 2.2).

However, for moduli this small it is probably easier to find the solutions by brute force.

We know that the unique solution (modulo 2) to

$$105\ x_1 \equiv \mathbf{1} \bmod 2$$

must be 0 or 1. So simply check both possibilities and see which one works!

We see that

$$105\ (0) \equiv 0 \bmod 2$$

but

$$105\ (\mathbf{1}) \equiv \mathbf{1} \bmod 2.$$

So $x_1 = \mathbf{1}$.

We know that the unique solution (modulo 3) to

$$70\ x_2 \equiv \mathbf{1} \bmod 3$$

must be $0, 1$ or 2. So simply check all three possibilities and see which one works!

We see that

$$70\ (0) \equiv 0 \bmod 3$$
$$70\ (\mathbf{1}) \equiv \mathbf{1} \bmod 3$$
$$70\ (2) \equiv 2 \bmod 3.$$

So $x_2 = \mathbf{1}$.

We know that the unique solution (modulo 5) to

$$42\ x_3 \equiv \mathbf{1} \bmod 5$$

must be $0, 1,2,3$ or 4. So simply check all five possibilities and see which one works!

We see that

$$42\ (0) \equiv 0 \bmod 5$$
$$42\ (1) \equiv 2 \bmod 5$$
$$42\ (2) \equiv 4 \bmod 5$$
$$42\ (\mathbf{3}) \equiv \mathbf{1} \bmod 5$$
$$42\ (4) \equiv 3 \bmod 5.$$

So $x_3 = \mathbf{3}$.

Finally, we know that the unique solution (modulo 7) to

$$30\ x_4 \equiv \mathbf{1} \bmod 7$$

must be $0, 1,2,3,4,5,6$ or 7. So simply check all seven possibilities and see which one works!

We see that

$$30\ (0) \equiv 0 \bmod 7$$
$$30\ (1) \equiv 2 \bmod 7$$
$$30\ (2) \equiv 4 \bmod 7$$
$$30\ (3) \equiv 6 \bmod 7$$
$$30\ (\mathbf{4}) \equiv \mathbf{1} \bmod 7$$
$$30\ (5) \equiv 3 \bmod 7$$
$$30\ (6) \equiv 5 \bmod 7$$

So $x_4 = \mathbf{4}$.

Therefore the desired unique solution modulo $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ is

$$\begin{aligned} x' &= b_1 M_1 x_1 + b_2 M_2 x_2 + b_3 M_3 x_3 + b_4 M_4 x_4 \\ &= (1 \cdot 105 \cdot 1) + (2 \cdot 70 \cdot 1) + (1 \cdot 42 \cdot 3) + (5 \cdot 30 \cdot 4) \\ &= 971. \end{aligned}$$

However, we can find a smaller nonnegative solution! We see that

$$971 = 4 \cdot 210 + 131.$$

Therefore, $131 \equiv 971 \bmod 210$. We also note that $0 \leq 131 < 210$ which tells us that 131 is the least nonnegative solution.

■

TA054

What is the smallest integer such that division by n leaves a remainder of $n-1$ for $n = 2, 3, \ldots, 10$; that is, division by $n = 2$ leaves a remainder of 1, division by $n = 3$ leaves a remainder of 2, etc., through $n = 10$?

1T943

Find the smallest positive integer k having the properties
(a) it is divisible by 13
(b) it has a remainder of 1 when divided by any of the numbers 2, 3, . . . ,12.

1A104

A certain positive integer is three greater than a multiple of 5, five greater than a multiple of 8, and eight greater than a multiple of 13. Determine the value of the least such integer.

Solution

Let x be the integer we are looking for. Then

x is three greater than a multiple of $5 \Leftrightarrow x \equiv 3 \bmod(5)$ (1)

x is five greater than a multiple of $8 \Leftrightarrow x \equiv 5 \bmod(8)$ (2)

x is eight greater than a multiple of $13 \Leftrightarrow x \equiv 8 \bmod(13)$. (3)

By the Chinese Remainder Theorem the value of x is unique $\bmod(5 \cdot 8 \cdot 13) = \bmod(520)$.

Chinese Remainder Theorem: Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$. That is, there is a unique solution $0 \le x < m$, and all other solutions are congruent modulo m to this solution.

From (Eq. 1) we know that x is three greater than a multiple of $5 \Leftrightarrow x = 5k + 3$ for some integer k. Consider both sides of (Eq. 1) $\bmod(8)$.

$$x \bmod(8) = (5k + 3) \bmod(8).$$

But from (Eq. 2) we also know that

$$x \equiv 5 \bmod(8).$$

Therefore

$$x \bmod(8) = (5k + 3) \bmod(8) = 5 \bmod(8)$$

or

$$(5k + 3) \equiv 5 \bmod(8)$$

which implies

$$5k \equiv 5 - 3 = 2 \bmod(8).$$

What does the statement $5k \equiv 2 \bmod(8)$ really mean? Because we are working $\bmod(8)$ we must have $k \in \{0,1,2,3,4,5,6,7\}$. So we are looking for that value of $k \in \{0,1,2,3,4,5,6,7\}$ such that $5k$ has a remainder of 2 when divided by 8. We can see by inspection that $k = 2$ satisfies this requirement because $5k = 5(2) = 10$ has a remainder of 2 when divided by 8.

But if we were working $\bmod(488)$ then $k \in \{0,1,2,3, \ldots, 486, 487\}$ and it may take you forever to find k "by inspection". We need a systematic approach.

7.2 Euler's Systematic Reduction Method

Find k such that $5k \equiv 2 \bmod(8)$ using Euler's Systematic Reduction Method.

$$\begin{gathered} 5k \equiv 2 \bmod(8) \\ \Leftrightarrow 5k = 8a + 2 \text{ for some integer } a \\ \Leftrightarrow 5k \bmod(5) = (8a + 2) \bmod(5) \\ \Leftrightarrow 0 \equiv (3a + 2) \bmod(5) \\ \Leftrightarrow 3a + 2 = 5b \text{ for some integer } b \\ \Leftrightarrow (3a + 2) \bmod(3) = 5b \bmod(3) \\ \Leftrightarrow 3a \bmod(3) + 2 \bmod(3) = 5b \bmod(3) \\ \Leftrightarrow 2 \bmod(3) = 5b \bmod(3) \end{gathered}$$

$$\Leftrightarrow 2 \equiv 2b \bmod(3)$$
$$\Leftrightarrow 2b = 3c + 2 \text{ for some integer } c$$
$$\Leftrightarrow 2b \bmod(2) = (3c + 2) \bmod(2)$$
$$\Leftrightarrow 0 \equiv c \bmod(2).$$

So, we have systematically reduced the problem of finding $k \in \{0,1,2,3,4,5,6,7\}$ such that $5k \equiv 2 \bmod(8)$ to the easier problem of find $c \in \{0,1\}$ such that $c \equiv 0 \bmod(2)$. Now we can immediately see that $c = 0$ satisfies $c \equiv 0 \bmod(2)$.

Now work your way back up the if and only if (*i.e.* $\Leftrightarrow$) statements

$$c = 0$$
$$2b = 3c + 2 \Leftrightarrow 2b = 2 \Leftrightarrow b = 1$$
$$3a + 2 = 5b \Leftrightarrow 3a + 2 = 5 \Leftrightarrow 3a = 3 \Leftrightarrow a = 1$$
$$5k = 8a + 2 \Leftrightarrow 5k = 8 + 2 \Leftrightarrow 5k = 10 \Leftrightarrow k = 2.$$

So $k = 2$, which is the same answer we got "by inspection". More specifically,

$$5k \equiv 2 \bmod(8) \Leftrightarrow k \equiv 2 \bmod(8).$$

That is, $k \in \{2,10,18,26,34,42,50,58,66,74, \dots\}$.

Now consider both sides of (Eq. 1) $\bmod(13)$.

$$x \bmod(13) = (5k + 3) \bmod(13).$$

But from (Eq. 3) we also know that

$$x \equiv 8 \bmod(13).$$

Therefore

$$x \bmod(13) = (5k + 3) \bmod(13) = 8 \bmod(13)$$

or

$$(5k + 3) \equiv 8 \bmod(13)$$

which implies

$$5k \equiv 8 - 3 = 5 \bmod(13).$$

Now we want to find that value of $k \in \{0,1,2,3,4, \dots ,11,12\}$ such that $5k$ has a remainder of 5 when divided by 13. We can see by inspection that $k = 1$ satisfies this requirement because $5k = 5(1) = 5$ has a remainder of 5 when divided by 13.

$$5k \equiv 5 \bmod(13) \Leftrightarrow k \equiv 1 \bmod(13).$$

That is, $k \in \{1,14,27,40,53,66,79,92,105, \dots\}$.

The smallest positive value of k that is in both lists is $k = 66$. Therefore,

$$x = 5k + 3 = 5(66) + 3 = 333 \bmod(520).$$

■

(TA054)

4. What is the smallest integer such that division by n leaves a remainder of $n-1$ for $n = 2, 3, \ldots, 10$; that is, division by $n = 2$ leaves a remainder of 1, division by $n = 3$ leaves a remainder of 2, etc., through $n = 10$?

Solution

Let the number be M. Then

(for instance) $M = 3k+2$; $M+1 = 3(k+1)$

$\therefore$ M+1 has 3 for a divisor; and

so on for $n = 2, 4, 5, \ldots, 10$.

$M+1 = \text{lcm}\{2, 3, 4, \ldots, 10\}$

$M+1 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$

$M = 2519$

■

7.3 Extra Linear Congruence Problems

Mu Alpha Theta National Convention, 2001, Number Theory Test, Mu Division, Problem # 9
What is the smallest positive prime number that leaves a remainder of one when divided by both 3 and 11?

Solution

9. There is a simple theorem in modular arithmetic that says that when we are looking for a set of number s with the same congruence in two different mods, then we are looking for the set of numbers that has that same congruence in the LCM of the two previous mods. The LCM of 3 and 11 is 33. We are looking for the smallest prime with a congruence of 1 (mod 33). A quick search reveals 67 as the answer.

$$3|(x-1) \text{ and } 11|(x-1) \Rightarrow 33|(x-1)$$
$$(x-1) \in \{33,66,99,\ldots\}$$
$$x \in \{34,67,100,\ldots\}$$

Smallest prime value of x is 67.

■

Mu Alpha Theta National Convention 2007, Mu Division, Number Theory Test, Problem #29

29) Given that x is a positive integer less than 100, find the sum of all possible values of x such that $28x \equiv 2 \pmod{54}$.

A) 58 B) 96 C) 144 D) 170 E) NOTA

Solution

29) $28x \equiv 2 \pmod{54}$ is the same thing as saying: find an integer solution to $28x + 54y = 2$, a linear Diophantine equation. This is equivalent to $14x + 27y = 1$. Using the Euclidian algorithm, an initial solution is $x_0 = 2$ and $y_0 = -1$. All possible solutions are in the form $x = 2 + 27t$ and $y = -1 - 14t$. The integer values of x less than 100 are 2, 29, 56, and 83. **D**

■

Chapter 8. Fibonacci Numbers

8.1 Definition

The Fibonacci sequence $F_1, F_2, F_3, \ldots$ is defined by the recurrence relation $F_{n+1} = F_n + F_{n-1}$.

F_1 and F_2 need to be specified in order to initiate the recurrence. The standard set of initial values are $F_1 = 1$ and $F_2 = 1$. But for some problems it is sufficient to state that $F_1 = a$ and $F_2 = b$ without assigning particular values to a and b.

In the standard model with $F_1 = 1$ and $F_2 = 1$, the first five numbers in the sequence are

	$F_1 = 1$	$F_2 = 1$	$F_3 = 2$	$F_4 = 3$	$F_5 = 5$

In some textbooks the Fibonacci sequence starts at F_0 instead of F_1. Notice that taking the initial values $F_0 = 0$ and $F_1 = 1$ with the recurrence $F_{n+1} = F_n + F_{n-1}$ leads to the same value for F_n, $n = 1,2,3, \ldots$ as the "standard" model. That is, with this alternative definition we get

$F_0 = 0$	$F_1 = 1$	$F_2 = 1$	$F_3 = 2$	$F_4 = 3$	$F_5 = 5$

8.2 $\gcd(F_i, F_j)$

Mu Alpha Theta National Convention 2005, Number Theory Test, Alpha Division, Problem #14
The Fibonacci sequence is defined such that the first two numbers in the sequence are both 1 and each successive number is the sum of the two previous numbers in the sequence. The first 5 numbers in the sequence are $1,1,2,3,$ and 5. What is the greatest common divisor of the 23rd and 24th numbers in the Fibonacci sequence?

Solution

The two important results to remember are

(i) $F_{n+1} = F_n + F_{n-1}$

(ii) $\gcd(a, b) = \gcd(a + b, b)$.

Repeatedly using these two results we can see why $\gcd(F_n, F_{n-1}) = 1$ for all n.

$$\gcd(F_{24}, F_{23}) = \gcd(F_{23} + F_{22}, F_{23}) = \gcd(F_{22}, F_{23})$$
$$\gcd(F_{23}, F_{22}) = \gcd(F_{22} + F_{21}, F_{22}) = \gcd(F_{21}, F_{22})$$
$$\gcd(F_{22}, F_{21}) = \gcd(F_{21} + F_{20}, F_{21}) = \gcd(F_{20}, F_{21})$$
$$\vdots$$
$$\gcd(F_2, F_1) = \gcd(1,1) = 1.$$

■

Theorem

$$\gcd(f_m, f_n) = f_{\gcd(m,n)}$$
$$m|n \Leftrightarrow f_m|f_n$$

Proof

Use the identity $\varphi_{m+n} = \varphi_{m-1}\varphi_n + \varphi_m\varphi_{n+1}$. Based on this, we can prove $k \mid n \Longrightarrow \varphi_k \mid \varphi_n$ by induction on n/k. For the converse and the claim concerning the gcd, verify that $a = bq + r$ implies $(\varphi_a, \varphi_b) = (\varphi_b, \varphi_r)$. An alternative method: Show that for every m, the indices of the Fibonacci numbers divisible by m are just the multiples of the index of the smallest Fibonacci number with this property.

8.3 Fibonacci Numbers Mod m

Let $F_{n+1} = F_n + F_{n-1}$ and let $F_1 = a$ and let $F_2 = b$. Let $h_{n,m} = F_n \bmod(m)$. Then

$$F_{n+1} \bmod(m) = (F_n + F_{n-1}) \bmod(m) = (F_n \bmod(m) + F_{n-1} \bmod(m)) \bmod(m).$$

That is,

$$h_{n+1,m} = \left(h_{n,m} + h_{n-1,m}\right) \bmod(m).$$

■

The sequence $h_{1,m}, h_{2,m}, h_{3,m}, \ldots$ is periodic.

In mathematics, a **periodic sequence** (sometimes called a **cycle**[*citation needed*]) is a sequence for which the same terms are repeated over and over:

$a_1, a_2, \ldots, a_p, \ a_1, a_2, \ldots, a_p, \ a_1, a_2, \ldots, a_p, \ldots$[*citation needed*]

The number p of repeated terms is called the **period** (period).[1]

A **(purely) periodic** sequence (with **period *p***), or a ***p*-periodic sequence**, is a sequence a_1, a_2, a_3, ... satisfying One size fits all

$a_{n+p} = a_n$

[2] for all values of n.[1][3][4][5][6] If a sequence is regarded as a function whose domain is the set of natural numbers, then a periodic sequence is simply a special type of periodic function.[*citation needed*] The smallest p for which a periodic sequence is p-periodic is called its **least period**[1][7] or **exact period**.[7][*verification needed*]

A periodic sequence is one that repeats itself. The period, p, of a periodic sequence is the number of terms in each repetition.

In number theory, the nth **Pisano period**, written as $\pi(n)$, is the period with which the sequence of Fibonacci numbers taken modulo n repeats. Pisano periods are named after Leonardo Pisano, better known as Fibonacci. The existence of periodic functions in Fibonacci numbers was noted by Joseph Louis Lagrange in 1774.[1][2]

So the study of Pisano periods may be further reduced to that of Pisano periods of primes. In this regard, two primes are anomalous. The prime 2 has an odd Pisano period, and the prime 5 has period that is relatively much larger than the Pisano period of any other prime. The periods of powers of these primes are as follows:

- If $n = 2^k$, then $\pi(n) = 3 \cdot 2^{k-1} = \frac{3 \cdot 2^k}{2} = \frac{3n}{2}$.
- if $n = 5^k$, then $\pi(n) = 20 \cdot 5^{k-1} = \frac{20 \cdot 5^k}{5} = 4n$.

From these it follows that if $n = 2 \cdot 5^k$ then $\pi(n) = 6n$.

Lemma 6.3.9: The Fibonacci sequence (mod m) is periodic.

Proof (from [28])

Modulo m a term will be equivalent to some value from 0 to $m - 1$, or one of m possible values

Therefore, when adding two terms (mod m) we can have m^2 possible outcomes.

Since this is a finite number of outcomes, we can guarantee that at some point the pairs will repeat and the sequence will start over again.

■

■

https://sites.math.rutgers.edu/~zeilberg/essays683/renault

http://webspace.ship.edu/msrenault/fibonacci/fib.htm

3. **Corollary 2**. If m has prime factorization $m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$, then $\pi(m) = [\pi(p_1^{e_1}), \pi(p_2^{e_2}), \ldots, \pi(p_n^{e_n})]$.
4. Given a prime p, let t be the largest integer such that $\pi(p^t) = \pi(p)$. Then $\pi(p^e) = p^{e-t}\pi(p)$ for all $e \geq t$.
   - For example, $\pi(3^1) = 8$, but $\pi(3^2) = 24$. Thus for the prime 3, $t = 1$ and we have the formula $\pi(3^e) = 3^{e-1} \cdot 8$. Similarly, we find that $\pi(7) = 16$, but $\pi(7^2) \neq 16$. Thus, $\pi(7^e) = 7^{e-1} \cdot 16$.

Definition The *period* of the Fibonacci sequence modulo a positive integer j is the smallest positive integer m such that $F_m \equiv 0 \pmod{j}$ and $F_{m+1} \equiv 1 \pmod{j}$.

Let $F_{n+1} = F_n + F_{n-1}$ and let $F_1 = F_2 = 1$. Find $F_{324} \bmod(4)$.

Solution

Let $b_{n,m} = F_n \bmod(m)$. It follows from the Fibonacci recurrence that

$$F_{n+1} \bmod(m) = (F_n + F_{n-1}) \bmod(m)$$

$$= (F_n \bmod(m) + F_{n-1} \bmod(m)) \bmod(m)$$

That is,

$$b_{n+1,m} = \left(b_{n,m} + b_{n-1,m}\right) \bmod(m)$$

■

Mu Alpha Theta National Convention 2001, Number Theory Test, Alpha Division, Problem # 39

Let $F_{n+1} = F_n + F_{n-1}$ and let $F_1 = F_2 = 1$. Find the smallest positive integer m such that $F_{n+m} \equiv F_n \pmod{7}$ for all integers n.

(A) 8 (B) 12 (C) 16 (D) 24 (E) NOTA

Solution

39. The Fibonacci numbers will always be cyclical in any mod because a term is defined by its predecessors and there are a limited number of possible combinations for a pair of predecessors which would then produce the same cyclical pattern each time that pair occurs. The trick is just to write down the modular residues of the Fibonacci numbers (mod 7) until the cycle is found: 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, etc. The 1st pair of terms (1, 1) reappeared as the 17^{th} pair. The cycle is thus a 16-cycle, thus m = 16.

■

8.4 Fibonacci Number Identities

https://www.cut-the-knot.org/arithmetic/algebra/FibonacciGCD.shtml

(see file "Fibonacci HW #2")

$$f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$$

$$f_1 = 1, f_2 = 1, f_3 = 2, \ldots$$

$$f_{n+m} = f_{n-1}f_m + f_n f_{m+1}.$$

Any two consecutive Fibonacci numbers are coprime.

8.5 Extra Problems for Fibonacci Numbers

AMC 1992 Problem #18

The increasing sequence of positive integers $a_1, a_2, a_3, \ldots$ has the property that

$$a_{n+2} = a_n + a_{n+1} \text{ for all } n \geq 1.$$

If $a_7 = 120$, then a_8 is

(A) 128	(B) 168	(C) 193	(D) 194	(E) 210

Solution

18. **(D)** If $a_1 = a$ and $a_2 = b$ then $(a_3,\ a_4,\ a_5,\ a_6,\ a_7,\ a_8) =$

$$(a+b,\ a+2b,\ 2a+3b,\ 3a+5b,\ 5a+8b,\ 8a+13b).$$

Therefore $5a+8b = a_7 = 120$. Since $5a = 8(15-b)$ and 8 is relatively prime to 5, a must be a multiple of 8. Similarly, b must be a multiple of 5. Let $a = 8j$ and $b = 5k$ to obtain $40j + 40k = 120$, which has two solutions in positive integers, $(j, k) = (1, 2)$ and $(2, 1)$. When $(j, k) = 2, 1)$, $(a, b) = (16, 5)$, which is impossible since the sequence is increasing, so $(j, k) = (1, 2)$ and $(a, b) = (8, 10)$. Consequently, $a_8 = 8a + 13b = 194$.

Note. This sequence begins with the eight terms

$$8, 10, 18, 28, 46, 74, 120, 194.$$

$$a_3 = a_1 + a_2$$
$$a_4 = a_2 + a_3 = a_2 + a_1 + a_2 = a_1 + 2a_2$$

$$a_5 = a_3 + a_4 = (a_1 + a_2) + (a_1 + 2a_2) = 2a_1 + 3a_2$$
$$a_6 = a_4 + a_5 = 3a_1 + 5a_2$$
$$a_7 = a_5 + a_6 = 5a_1 + 8a_2$$
$$a_8 = 8a_1 + 13a_2$$

$$5a_1 + 8a_2 = 120, \ \ 1 \le a_1 < a_2$$

$$a_1 + a_2 + \frac{3a_2}{5} = 24$$

$$\frac{6a_2}{5} = p$$
$$a_2 + \frac{a_2}{5} = p$$
$$a_2 = 5p$$

$$120 = 5a_1 + 8a_2 = 5a_1 + 40p$$

$$5a_1 = 120 - 40p$$
$$a_1 = 24 - 8p, a_2 = 5p$$

The only positive solutions for both a_1 and a_2 happen when $p = 1$ and $p = 2$

$$a_1 = 16, a_2 = 5$$
$$a_1 = 8, a_2 = 10.$$

But $a_1 < a_2$ so $a_1 = 8$ and $a_2 = 10$.
Therefore,

$$a_8 = 8a_1 + 13a_2 = 8(8) + 13(10) = 64 + 130 = 194.$$

■

Mu Alpha Theta National Convention 2001, Number Theory Test, Alpha Division, Problem # 39

Let $F_{n+1} = F_n + F_{n-1}$ and let $F_1 = F_2 = 1$. Find the smallest positive integer m such that $F_{n+m} \equiv F_n \pmod 7$ for all integers n.

(A) 8 (B) 12 (C) 16 (D) 24 (E) NOTA

Solution

39. The Fibonacci numbers will always be cyclical in any mod because a term is defined by its predecessors and there are a limited number of possible combinations for a pair of predecessors which would then produce the same cyclical pattern each time that pair occurs. The trick is just to write down the modular residues of the Fibonacci numbers (mod 7) until the cycle is found: 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, etc. The 1st pair of terms (1, 1) reappeared as the 17^{th} pair. The cycle is thus a 16-cycle, thus m = 16.

■

Mu Alpha Theta National Convention, 2001, Number Theory Test, Mu Division, Problem # 10
How many of the first 400 Fibonacci numbers are multiples of 3? (Let the first two Fibonacci numbers both be 1.)
Solution

10. Rewriting the Fibonacci numbers in (mod 3) reveals a pattern which repeats in cycles of 4 with only one of the numbers in that cycle being congruent to 0 (mod 3). Thus exactly 100 of the first 400 Fibonacci's are multiples of 3.

■

2008 Mu Alpha Theta National Convention **Open Number Theory**

27. How many of the first 120 elements of the Fibonacci sequence starting with 1,1,... are divisible by 4?

A. 10 B. 20 C. 30 D. 40 E. NOTA

Solution

27. **B**. Writing out the first few terms of that sequence mod4 gives 1,1,2,3,1,0,1,1,... which means it has a period of 6 and is divisible by 4 once in each period, so 20 times in the first 120.

I am still hoping to find a set of results about the Fibonacci sequence modulo m.

■

Fibonacci Series Modulo m
Author(s): D. D. Wall

THEOREM 1. *$f_n \pmod m$ forms a simply periodic series. That is, the series is periodic and repeats by returning to its starting values.*

THEOREM 2. *If m has the prime factorization $m = \prod p_i^{e_i}$ and if h_i denotes the length of the period of $f_n \pmod{p_i^{e_i}}$, then $h = \text{lcm}\ [h_i]$, the least common multiple of the h_i.*

Mu Alpha Theta National Convention 2007, Alpha Division, Number Theory Test, Problem #16

16. The Fibonacci Numbers F(n), where n is a natural number, are defined as F(1) = 1, F(2) = 1, and for n > 2, defined recursively by F(n) = F(n – 1) + F(n – 2). Let x be the sum of the ten smallest Fibonacci numbers. What is the remainder when x is divided by 3?

Solution

16. **(B)**. The ten smallest Fibonacci numbers are 1, 1, 2, 3, 5, 8, 13, 21, 34, and 59. The sum of these is 143, which has a remainder of 2 upon division by 3. As an alternative to adding up these numbers, we could use the fact that the sum of the first n Fibonacci numbers is F(n + 2) – 1. Since in this problem n = 10, we have F(12) – 1 = 144 – 1 = 143, producing the same result.

■

Chapter 9. Pythagorean Triples

If x, y, and z are positive integers such that $x^2 + y^2 = z^2$ then we call the triple (x, y, z) a **Pythagorean Triple**.

Pg. 60, Definition (Primitive Pythagorean Triples)
If x, y, and z are relatively prime positive integers such that $x^2 + y^2 = z^2$ then we call the triple (x, y, z) a **Primitive Pythagorean Triple**.

Note: Recall that x, y, z are relatively prime provided $(x, y, z) = 1$.

Pg. 60, Theorem 2.26 (Pythagorean Triples)
The integers x, y, and z with x even form a primitive *Pythagorean triple* if and only if there exists integers s and t, with $s < t$, with $(s, t) = 1$ and with one of s and t even and the other odd, such that $x = 2st, y = t^2 - s^2$, and $z = t^2 + s^2$.

Theorem 2.1.1. *Every primitive Pythagorean triple (a, b, c) with b even is given by the formula $(u^2 - v^2, 2uv, u^2 + v^2)$ with u and v relatively prime natural numbers of different parity and $u > v$.*

■

every Pythagorean triple has the property that one of the legs is divisible by 3.

Problem 1 (Homework) *Prove that in every Pythagorean triple (a, b, c) at least one of the numbers a, b, c is divisible by 5.*

All the conjectures formulated above are true for all primitive Pythagorean triples. The reader is invited to prove them all.

Exactly one of x, y is divisible by 3.
Exactly one of x, y is divisible by 4.
Exactly one of x, y, z is divisible by 5.
The largest number that always divides xyz is 60.
z is odd

All prime factors of z are primes of the form $4n + 1$. Therefore, z is of the form $4n + 1$.

9.1 Longest Leg and Hypotenuse Differ By Exactly One

https://en.wikipedia.org/wiki/Pythagorean_triple

There exist infinitely many Pythagorean triples in which the hypotenuse and the longest leg differ by exactly one. Such triples are necessarily primitive and have the form $(2n + 1, 2n^2 + 2n, 2n^2 + 2n + 1)$. This results from Euclid's formula by remarking that the condition implies that the triple is primitive and must verify $(m^2 + n^2) - 2mn = 1$. This implies $(m - n)^2 = 1$, and thus $m = n + 1$. The above form of the triples results thus of substituting m for $n + 1$ in Euclid's formula.

There exist infinitely many Pythagorean triples in which the hypothenuse and the longest leg differ by exactly two. They are all primitive and are obtained by putting $n = 1$ in Euclid's formula.

More generally, for every integer $k > 0$, there exist infinitely many primitive Pythagorean triples in which the hypothenuse and the odd leg differ by $2k^2$. They are obtained by putting $n = k$ in Euclid's formula.

9.2 Legs Differ By Exactly One

Before we find a *general parametrization* of all primitive Pythagorean triples let us look also at the case $b = a+1$. The equation becomes $a^2+a^2+2a+1 = c^2$ or $2c^2-(2a+1)^2 = 1$. We will see in the last section of this Chapter that this equation leads to the so called Pell's equation. We know that there are at least two particular solutions for this equation: $c = 5$, $a = 4$ and $c = 29$, $a = 20$. One can check that the following recurrence gives an infinite sequence of solutions:

$$a_{n+1} = 3a_n + 2c_n + 1, \text{ and } c_{n+1} = 4a_n + 3c_n + 2, \ c_0 = 1, \ a_0 = 0, \ n \in \mathbb{N}.$$

The fact that these formulae generate Pythagorean triples of the form $(a, a + 1, c)$, reduces to a simple algebra calculation and an induction argument. The first ten such triples that are generated this way are: $(3, 4, 5)$, $(20, 21, 29)$, $(119, 120, 169)$, $(696, 697, 985)$, $(4059, 4060, 5741)$, $(23660, 23661, 33461)$, $(137903, 137904, 195025)$, $(803760, 803761, 1136689)$, $(4684659, 4684660, 6625109)$ and $(27304196, 27304197, 38613965)$. Is this method generating all of such triples? We will show that this is indeed the case.

9.3 How do I find all primitive Pythagorean triples with one given number?

Let the given number be denoted by b.

We invoke the property that all primitive Pythagorean triple can be expressed in the form

$$(m^2 - n^2, 2mn, m^2 + n^2)$$

with integers $m > n > 0$ where exactly one of m and n is odd and where $\gcd(m, n) = 1$.

Case 1. b is even.

It must be that $b = 2mn$ because $2mn$ is the only even number in a primitive Pythagorean triple.

So, we need to find integers m and n (subject to the above restrictions) such that $b = 2mn$.

Case 2. b is odd and $b = m^2 - n^2$.

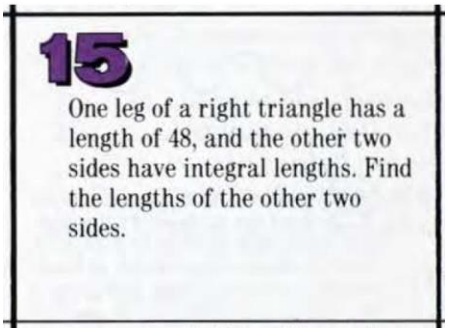
In this case, $b = m^2 - n^2 = (m - n)(m + n)$.

So, we need to find integers m and n (subject to the above restrictions) such that $b = (m - n)(m + n)$.

Case 3. b is odd and $b = m^2 + n^2$.

In this case, $b = m^2 + n^2$.

Mathematics Teacher, May 1986



15

One leg of a right triangle has a length of 48, and the other two sides have integral lengths. Find the lengths of the other two sides.

(15) Let c represent the length of the hypotenuse, and let 48 and a represent the lengths of the legs of the given triangle. Then

$$(48)^2 = c^2 - a^2,$$

or

$$(48)^2 = (c + a)(c - a).$$

If we divide $(48)^2$ into two positive factors in all possible ways, set $c + a$ equal to the larger factor, set $c - a$ equal to the smaller factor, and then solve the resulting pairs of simultaneous equations, the required solutions will be included among them.

Since $(48)^2 = 2^8 \cdot 3^2$, the 27 terms of the product

$$(1 + 2 + 2^2 + 2^3 + \cdots + 2^8) \cdot (1 + 3 + 3^2)$$

give all its factors. Only even factors may be chosen for $c + a$ and $c - a$, since, if one were odd, the other would have to be even. The sum of $c + a$ and $c - a$, that is, $2c$, would then have to be the sum of an odd and an even number, but this is impossible. We are thus reduced to ten possibilities:

$$c + a = 2^7 \cdot 3^2;\ 2^7 \cdot 3;\ 2^7;\ 2^6 \cdot 3^2;\ 2^6 \cdot 3;\ 2^6;\ 2^5 \cdot 3^2;\ 2^5 \cdot 3;\ 2^4 \cdot 3^2;\ 2^3 \cdot 3^2$$

$$c - a = 2;\ 2 \cdot 3;\ 2 \cdot 3^2;\ 2^2;\ 2^2 \cdot 3;\ 2^2 \cdot 3^2;\ 2^3;\ 2^3 \cdot 3;\ 2^4;\ 2^5$$

The solutions of these taken in pairs are

$(c, a) = (577, 575), (195, 189), (73, 55), (290, 286), (102, 90), (50, 14), (148, 140), (60, 36), (80, 64),$ and $(52, 20)$.

(Source: Beiler, Albert H. *Recreations in the Theory of Numbers.* New York: Dover Publications, 1964.)

Mu Alpha Theta 1996 National Convention, Open Division, Number Theory, Problem 13 (adapted)

Let (a, b, c) be a Pythagorean triple such that a, b and c are positive integers with $a < b < c$ and $a^2 + b^2 = c^2$. If $b = 1996$, find a and c.

Solution

$$b^2 = c^2 - a^2 = (c - a)(c + a).$$

We note that the sum of these two factors is even. That is $(c - a) + (c + a) = 2c$. Also the difference of these two factors is even. That is $(c + a) - (c - a) = 2a$.

Therefore, either $(c - a)$ and $(c + a)$ are both odd or both even. But we are given that their product $(c - a)(c + a) = b^2 = 1996^2$ is an even number. Therefore $(c - a)$ and $(c + a)$ must both be even numbers.

We note that $1996^2 = 2^4 \cdot 499^2$ with 499 a prime number. Therefore,

$$(c - a, c + a) = \left\{(2, 2^3 499^2), (2^2, 2^2 499^2), (2^3, 2^1 499^2), (2^1 499^1, 2^3 499^1)\right\}$$

in order that $b^2 = (c - a)(c + a) = 1996^2$. We ruled out the two possibilities $(2^2 499^1, 2^2 499^1)$ and $(2^3 499^1, 2^1 499^1)$ because $c + a > c - a$. We also ruled out all possibilities where either $(c - a)$ or $(c + a)$ is an odd number.

Now suppose we take $c - a = d$ and $c + a = e$. Solving for a and c we find

$$a = \frac{e - d}{2} \text{ and } c = \frac{e + d}{2}.$$

Now notice that when we solve for a in each of the first three cases listed above for $(c - a, c + a) = (d, e)$, we find that $a > b = 1996$.

In particular,

$$a = \frac{2^3 499^2 - 2^1}{2} > 1996 = b$$

$$a = \frac{2^2 499^2 - 2^2}{2} > 1996 = b$$

$$a = \frac{2^1 499^2 - 2^3}{2} > 1996 = b.$$

By elimination we have that

$$(c-a, c+a) = (2^1 499^1, 2^3 499^1).$$

Solving for a and c we find

$$a = \frac{2^3 499^1 - 2^1 499^1}{2} = 1497$$

and

$$c = \frac{2^3 499^1 + 2^1 499^1}{2} = 2495.$$

So, the Pythagorean triple in this problem is $(a, b, c) = (1497, 1996, 2495)$. As a check we note that

$$1497^2 + 1996^2 = 2241009 + 3984016 = 6225025 = 2495^2.$$

■

(3A934)

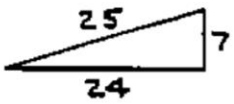
4. Find two distinct pairs of positive integers (a,b) and (c,d), $(c,d) \neq (b,a)$, so that each pair is a solution to $x^2 + y^2 = 625$.

Solution

Recognizing $625 = 25^2$ and recalling that $3^2 + 4^2 = 5^2$, we easily obtain

$25^2 = (5^2)^2 = 5^2(3^2 + 4^2) = 15^2 + 20^2$

If you recall that 7, 24, 25 is a Pythagorean triple, a second solution is obvious. Otherwise, obtain it from



$25^2 = (3^2 + 4^2)^2 = 3^4 + 2 \cdot 3^2 \cdot 4^2 + 4^4$

$= 3^4 - 2 \cdot 3^2 \cdot 4^2 + 4^4 + 4 \cdot 3^2 \cdot 4^2$

$= (3^2 - 4^2)^2 + (2 \cdot 3 \cdot 4)^2 = 7^2 + 24^2$

■

(TT932)

2. Find two distinct pairs of positive integers (a,b) and (c,d), $(c,d) \neq (b,a)$, so that each pair is a solution to $x^2 + y^2 = 169^2$.

Solution

Recall that $5^2 + 12^2 = 13^2 = 169$.

$$(169)^2 = (5^2 + 12^2)^2 = (5^2)^2 + 2 \cdot 5^2 \cdot 12^2 + (12^2)^2$$
$$= (5^2)^2 - 2 \cdot 5^2 \cdot 12^2 + (12^2)^2 + 4 \cdot 5^2 \cdot 12^2$$
$$= (12^2 - 5^2)^2 + (2 \cdot 5 \cdot 12)^2 = 119^2 + 120^2$$

and

$$169^2 = 13^2(5^2 + 12^2) = (13 \cdot 5)^2 + (13 \cdot 12)^2$$

■

(TI9312)

12. Let p, q, and r be a Pythagorean triple with $p < q < r$. Find, in terms of p, q, and r, two distinct pairs of positive integers (a,b) and (c,d), $(c,d) \neq (b,a)$, so that each pair is a solution to $x^2 + y^2 = r^4$.

Solution

$$r^4 = r^2(p^2 + q^2) = (pr)^2 + (qr)^2$$

and

$$r^4 = (q^2 - p^2)^2 + (2pq)^2$$

(This generalizes Event 3A #4 and Tourn. Team Event #2)

■

9.4 Congruent Number Problem

see file "The Congruent Number Problem" Resonance

A positive integer n is called a *congruent number* if there exists a right-angled triangle whose sides are rational numbers and whose area is the given number n.

PROPOSITION A number n is congruent if and only if there exists a rational number a such that $a^2 + n$ and $a^2 - n$ are both squares of rational numbers.

9.5 Extra Pythagorean Triple Problems

(TA163) There is one three-digit integer $\underline{A}\,\underline{B}\,\underline{C}$ with the following property: remove the first digit to form the one-digit number $\underline{A}$ and the two-digit number $\underline{B}\,\underline{C}$. Then $\left(\underline{B}\,\underline{C}\right)^2 - \underline{A}^2$ is a perfect square. Form the two-digit number $\underline{B}\,\underline{C}$ and the one-digit number $\underline{C}$. Both of these numbers are perfect squares. Determine the number $\underline{A}\,\underline{B}\,\underline{C}$.

Solution

$\underline{A}$ and $\underline{BC}$ are part of a Pythagorean Triple since $\left(\underline{BC}\right)^2 - \underline{A}^2$ is a perfect square. There are only a few possibilities that will work. They are 5-12-13, 6-8-10, 7-24-25, 8-15-17, and 9-40-41. These form the numbers 513, 610, 810, 725, 817, and 941. The only one that satisfies the second criterion is 810 with 81 and 0.

■

(1T146) In *Figure 6*, segments $\overline{PQ}$ and $\overline{RS}$ intersect at T. All seven line segments in the figure have integer side lengths. If $PS = 37$, determine exactly the largest possible length $\overline{PQ}$.

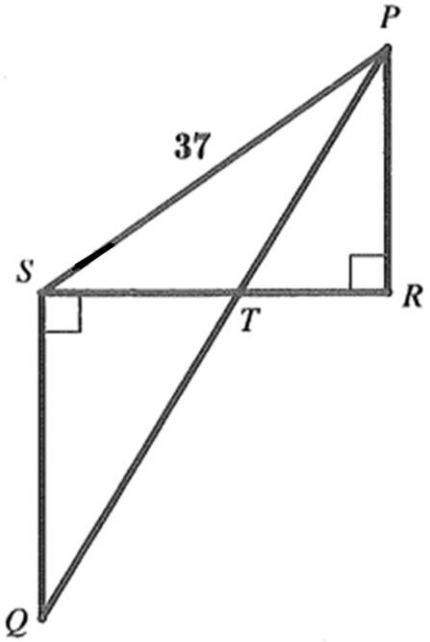


Figure 6

Solution

The only Pythagorean triple with hypotenuse 37 is 12/35/37. The figure may not be to scale; i.e., we don't know whether SR > PR or vice versa. If PR = 35, then △PRT causes us to seek Pythagorean triples with one leg of length 35 and the other leg RT < 12 and as short as possible (so that $\overline{PQ}$ will be as long as possible). Unfortunately, such a triple would have to be of the form x/35/36, and does not exist. So PR =12 and SR = 35. Now in △PRT, we need triples with one leg of length 12, and the other leg RT < 35 and as short as possible. Hopefully 5/12/13 comes to mind, so that RT = 5, ST = 30, and PT = 13. Finally, in △STQ, we seek the triple with short leg 30 and longest possible hypotenuse: 30/72/78 ⇒ PT + TQ = $\boxed{91}$.

■

(1T104) Hexagon *HEXGON* can be dissected into right triangles, as shown in *Figure 4*. The nine line segments in the diagram all have different integer lengths, and $\overline{GO}$ has the shortest length of these all those segments. Calculate the <u>smallest</u> possible value for the perimeter of *HEXAGON*.

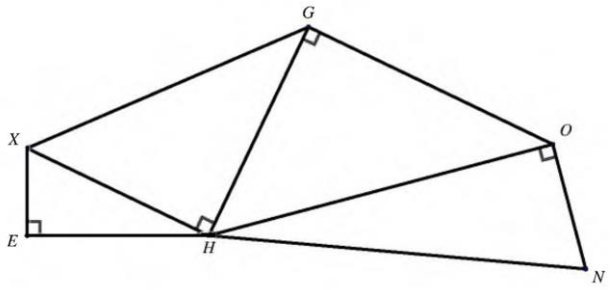
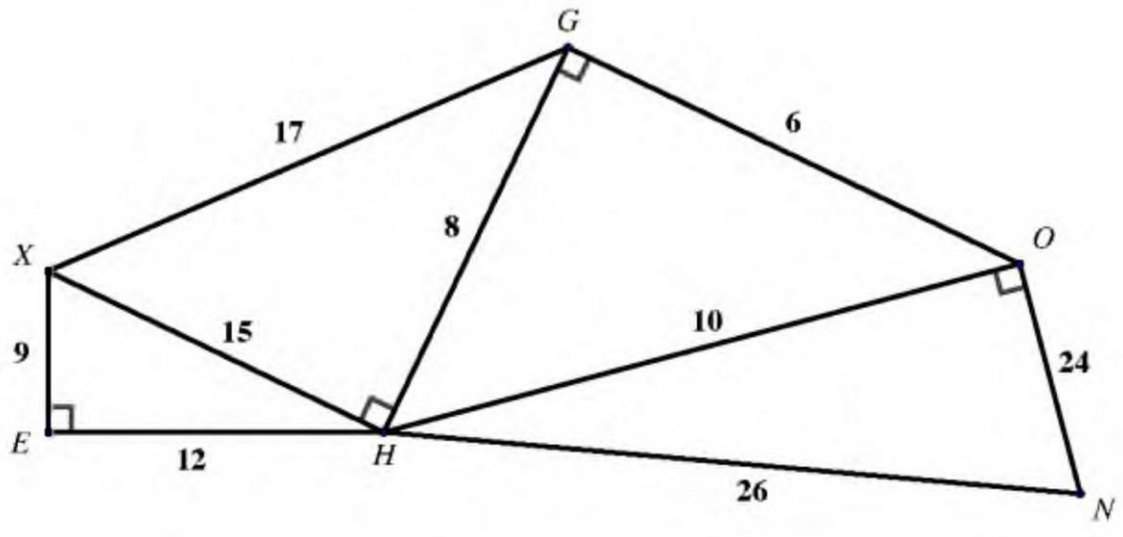


Figure 4

<u>Solution</u>

The smallest Pythagorean triples are (3, 4, 5), (5, 12, 13), (6, 8, 10), (7, 24, 25), (8, 15, 17), . . . Begin by choosing the smallest value in each triple as the length of $\overline{GO}$. GO = 3 fails because GH = 4, and △XGH cannot be another 3-4-5 triangle. GO = 5 works, but then HO = 13, forcing ON = 84 and HN = 85, which will make for a very large hexagon perimeter. The key will be to make hypotenuse HO as small as possible so that △HON uses a "small" Pythagorean triple. This is accomplished by setting GO = 6 and labeling the diagram as shown. The perimeter of the resulting hexagon is $\boxed{94}$.



Source: National Mathematics Magazine, Vol. 15, No. 3 (Dec., 1940), pp. 145-153
5525 hypotenuse of 22 Pythagorean triangles

No. 350. Proposed by *D. L. MacKay*, Evander Childs High School, New York.

Show that 5525 is the hypotenuse of twenty-two integral right triangles. Find them.

Solution by *G. W. Wishard*, Norwood, Ohio.

We need two well-known propositions from the theory of numbers:

(a) The sides of every integral right triangle are given by the formulas:

$$a=2kxy, \qquad b=k(x^2-y^2), \qquad c=k(x^2+y^2),$$

where x and y have no common factor, one of them is even, and $x>y$.

(b) A product $P=LM$ can be represented as a sum of two squares if each factor can, viz.

$$(1) \qquad (r^2+s^2)(u^2+v^2)=(ru+sv)^2+(rv-su)^2.$$

Conversely every representation of P as a sum of two squares can be obtained from representations for L and M by use of (1).*

Now $5525=5^2\cdot 13\cdot 17=k(x^2+y^2)$, $5=2^2+1^2$, $5^2=3^2+4^2$,

$$13=2^2+3^2, \quad 17=4^2+1^2,$$

whence various factorizations of 5525 and repeated application of (1) give the required twenty-two sets as follows:

*See, for example, Carmichæl, *Diophantine Analysis*, pp. 10, 24, ff.

k	x^2+y^2	x		a	b	k	x^2+y^2	x	y	a	b
1105	5	2	1	4420	3315	13	425	16	13	5408	1131
425	13	3	2	5100	2125			19	8	3952	3861
325	17	4	1	2600	4875	5	1105	32	9	2880	4715
221	25	4	3	5304	1547			31	12	3720	4085
85	65	8	1	1360	5355			33	4	1320	5365
		7	4	4760	2805			24	23	5520	235
65	85	9	2	2340	5005	1	5525	74	7	1036	5427
		7	6	5460	845			73	14	2044	5133
25	221	11	10	5500	525			71	22	3124	4557
		14	5	3500	4275			62	41	5084	2163
17	325	17	6	3468	4301						
		18	1	612	5491						

Also solved by *C. C. Chaudoir, Edwin Comfort, Dewey C. Duncan, Frank H. Mehrhoff, C. W. Trigg,* and the *Proposer.*

6 Continued fractions

6.1 Definitions and notations

Definition 6.1 (Continued fractions). *A finite or infinite expression of the form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}, \tag{6.1}$$

where the a_i are real numbers, with $a_1, a_2, \dots > 0$, is called a ***continued fraction*** *(c.f.). The numbers a_i are called the* ***partial quotients*** *of the c.f.*

The continued fraction (6.1) *is called* ***simple*** *if the partial quotients a_i are all integers. It is called* ***finite*** *if it terminates, i.e., if it is of the form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots + \cfrac{1}{a_n}}}, \tag{6.2}$$

and ***infinite*** *otherwise.*

Notation (Bracket notation for continued fractions). *The continued fractions* (6.1) *and* (6.2) *are denoted by $[a_0, a_1, a_2, \dots]$ and $[a_0, a_1, a_2, \dots, a_n]$, respectively. In particular,*

$$[a_0] = a_0, \quad [a_0, a_1] = a_0 + \frac{1}{a_1}, \quad [a_0, a_1, a_2] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \quad \dots$$

Remarks. (i) Note that the first term, a_0, is allowed to be negative or 0, but all subsequent terms a_i must be positive. This requirement ensures that there are no zero denominators and that any finite c.f. (6.2), and all of its convergents, are well-defined.

(ii) In the sequel we will focus on the case of simple c.f.'s, i.e., c.f.'s where all partial quotients are integers.

Definition 6.2 (Convergents). *The **convergents** of a (finite or infinite) c.f.* $[a_0, a_1, a_2, \dots]$ *are defined as*

$$C_0 = [a_0],\ C_1 = [a_0, a_1],\ C_2 = [a_0, a_1, a_2], \dots$$

If the c.f. is simple, its convergents C_i *represent rational numbers, denoted by*

$$C_i = \frac{p_i}{q_i},$$

where p_i/q_i *is in reduced form.*

To simplify a finite continued fraction (as in the example below) start at the bottom and work up.

$$5 - \cfrac{1}{4 - \cfrac{1}{3 - \cfrac{1}{2 - \cfrac{1}{1}}}} = 5 - \cfrac{1}{4 - \cfrac{1}{3 - \cfrac{1}{1}}} = 5 - \cfrac{1}{4 - \cfrac{1}{2}} = 5 - \cfrac{1}{\cfrac{7}{2}} = 5 - \frac{2}{7} = \frac{33}{7}.$$

To simplify an infinite continued fraction, identified as x in the example below, look for a way to rewrite a "smaller" part of the fraction in terms of the same x. Then solve for x.

$$x = \cfrac{3}{2 + \cfrac{3}{2 + \cfrac{3}{2 + \ddots}}} = \cfrac{3}{2 + \left(\cfrac{\mathbf{3}}{\mathbf{2} + \cfrac{\mathbf{3}}{\mathbf{2} + \ddots}} \right)} = \frac{3}{2 + \boldsymbol{x}}$$

That is,

$$x = \frac{3}{2 + x} \Longrightarrow x(2 + x) = 3 \Longrightarrow x^2 + 2x - 3 = 0 \Longrightarrow (x + 3)(x - 1) = 0.$$

So, $x = -3$ and $x = 1$. But $x = -3$ is an extraneous solution (a false solution that satisfies the final step of the derivation but does not satisfy the original problem) so it does not count as a solution. (i.e. toss out $x = -3$ because x is clearly positive)

So,

$$x = \cfrac{3}{2 + \cfrac{3}{2 + \cfrac{3}{2 + \ddots}}} = 1.$$

10.1 Expand a number into continued fraction form

Example 30.

The fraction $\frac{37}{13}$ can be written in the form $2+\dfrac{1}{x+\dfrac{1}{y+\dfrac{1}{z}}}$ where x, y and z are positive integers. Find the values of (x, y, z).

Solution

Step 1. Express $37/13$ in the form $q + r/13$ where q and r are positive integers and $r < 13$ (*i.e.* integer quotient with remainder form). A result called the **remainder theorem** says that there will always be a q and r as described above.

$$\frac{37}{13} = 2 + \frac{11}{13}.$$

Step 2. Rewrite the fraction $r/13$ as $1/(13/r)$.

$$\frac{11}{13} = \frac{1}{\frac{13}{11}}$$

Step 3. It follows by our requirement that $r < 13$ that $13/r > 1$. So we can carry out Step 1 on $13/r$.

$$\frac{13}{11} = 1 + \frac{2}{11}.$$

Summarizing our work up to this point we have

$$\frac{37}{13} = 2 + \frac{11}{13} = 2 + \frac{1}{\frac{13}{11}} = 2 + \frac{1}{1 + \frac{2}{11}}.$$

Step 4. Continue in this pattern.

$$\frac{2}{11} = \frac{1}{\frac{11}{2}} = \frac{1}{5 + \frac{1}{2}}.$$

$$\frac{37}{13} = 2 + \frac{1}{1 + \left(\frac{2}{11}\right)} = 2 + \frac{1}{1 + \left(\frac{1}{5 + \frac{1}{2}}\right)} = 2 + \frac{1}{1 + \frac{1}{5 + \frac{1}{2}}}.$$

Final step. Compare and identify (x, y, z).

$$\frac{37}{13} = 2 + \frac{1}{x + \frac{1}{y + \frac{1}{z}}} = 2 + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{5} + \frac{1}{\mathbf{2}}}}$$

So $(x, y, z) = (1,5,2)$. Note that the **process stops** when we reach a **remainder of 1**.

■

Example 31.

The fraction $\frac{18}{11}$ can be written in the form $2 - \frac{1}{x + \frac{1}{y - \frac{1}{z}}}$ where x, y and z are positive integers. Find the values of (x, y, z).

Solution

The new twist is the presence of minus $(-)$ signs in the above form. Similar to our first step in the last example we now need to $18/11$ in the form $q - r/11$ where q and r are positive integers and $r < 11$ (*i.e.* integer quotient with remainder form). The **remainder theorem** mentioned above also guarantees that this is always possible.

$$\frac{18}{11} = 2 - \frac{3}{11}.$$

Step 2. Continue as in Example 1.

$$\frac{18}{11} = 2 - \frac{3}{11} = 2 - \frac{1}{\frac{11}{3}} = 2 - \frac{1}{3 + \frac{2}{3}} = 2 - \frac{1}{3 + \frac{1}{\frac{3}{2}}} = 2 - \frac{1}{3 + \frac{1}{2 - \frac{1}{2}}}.$$

So $(x, y, z) = (3,2,2)$.

■

10.2 Summary Result

In general, if we want a plus $(+)$ sign we can construct

$$\frac{a}{b} = q + \frac{r}{b} \text{ for some integers } a.\, b, q \text{ and } r$$

with $r < b < a$.

And if we want a minus $(-)$ sign we can construct

$$\frac{a}{b} = q - \frac{r}{b} \text{ for some (different) integers } a, b, q \text{ and } r$$

with $r < b < a$.

10.3 Extra Continued Fraction Problems

(1T124) The fraction $\frac{37}{13}$ can be written in the form

$$2 + \frac{1}{x + \frac{1}{y + \frac{1}{z}}},$$

where x, y, and z are positive integers. Find the values of (x, y, z).
[Original source: *Australian M.C.*, 1981]
Solution
The problem is asking you to express $37/13$ in ***finite simple continued fraction*** form.

Step 1. Express $37/13$ in the form $q + r/13$ where q and r are positive integers and $r < 13$ (*i.e.* integer quotient with remainder form). A result called the **remainder theorem** says that there will always be a q and r as described above.

$$\frac{37}{13} = 2 + \frac{11}{13}.$$

Step 2. Rewrite the fraction $r/13$ as $1/(13/r)$.

$$\frac{11}{13} = \frac{1}{\frac{13}{11}}$$

Step 3. It follows by our requirement that $r < 13$ that $13/r > 1$. So, we can carry out Step 1 on $13/r$.

$$\frac{13}{11} = 1 + \frac{2}{11}.$$

Summarizing our work up to this point we have

$$\frac{37}{13} = 2 + \frac{11}{13} = 2 + \frac{1}{\frac{13}{11}} = 2 + \frac{1}{1 + \frac{2}{11}}.$$

Step 4. Continue in this pattern.

$$\frac{2}{11} = \frac{1}{\frac{11}{2}} = \frac{1}{5 + \frac{1}{2}}.$$

$$\frac{37}{13} = 2 + \frac{1}{1 + \left(\frac{2}{11}\right)} = 2 + \frac{1}{1 + \left(\frac{1}{5 + \frac{1}{2}}\right)} = 2 + \frac{1}{1 + \frac{1}{5 + \frac{1}{2}}}.$$

Final step. Compare and identify (x, y, z).

$$\frac{37}{13} = 2 + \frac{1}{x + \frac{1}{y + \frac{1}{z}}} = 2 + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{5} + \frac{1}{\mathbf{2}}}}$$

So $(x, y, z) = (\mathbf{1}, \mathbf{5}, \mathbf{2})$. Note that the **process stops** when we reach a **remainder of 1**.

[An alternative approach.]

$$2 + \frac{1}{x + \frac{1}{y + \frac{1}{z}}} = \frac{37}{13}$$

$$\Rightarrow \frac{1}{x + \frac{1}{y + \frac{1}{z}}} = \frac{37}{13} - 2 = \frac{11}{13}$$

$$\Rightarrow x + \frac{1}{y + \frac{1}{z}} = \frac{13}{11}$$

$$\Rightarrow x+\frac{1}{y+\frac{1}{z}}=1+\frac{2}{11}\Rightarrow x=\mathbf{1},\quad \frac{1}{y+\frac{1}{z}}=\frac{2}{11}$$

$$\Rightarrow y+\frac{1}{z}=\frac{11}{2}=5+\frac{1}{2}\Rightarrow y=\mathbf{5},\quad \frac{1}{z}=\frac{1}{2}\Rightarrow z=\mathbf{2}.$$

■

(TA922)

Solve for x: $\quad 1-\dfrac{1}{2-\dfrac{1}{3-\dfrac{1}{4-x}}}=\dfrac{1}{3}.$

Solution

Approach 1. Expand $\frac{1}{3}$ into finite simple continued fraction form.

$$\frac{1}{3}=1-\frac{2}{3}=1-\frac{1}{\frac{3}{2}}=1-\frac{1}{2-\frac{1}{2}}=1-\frac{1}{2-\frac{1}{3-\frac{1}{1}}}.$$

Matching the given expression with this form

$$1-\frac{1}{2-\frac{1}{3-\frac{1}{\mathbf{4-x}}}}=1-\frac{1}{2-\frac{1}{3-\frac{1}{\mathbf{1}}}}$$

we see that $4-x=1$ which means that $x=3$.

Approach 2. (Their approach: Go inside out.)

First note that $\dfrac{1}{3-\dfrac{1}{4-x}} = \dfrac{4-x}{12-3x-1}$

Then $\dfrac{1}{2-\dfrac{4-x}{11-3x}} = \dfrac{11-3x}{22-6x-(4-x)}$

The given equation thus takes the form

$1-\dfrac{11-3x}{18-5x} = \dfrac{1}{3}$ or $\dfrac{2}{3} = \dfrac{11-3x}{18-5x}$

$36-10x = 33-9x$ so $3 = x$.

■

(1A132) The expression

$$5-\frac{1}{4-\dfrac{1}{3-\dfrac{1}{2-\dfrac{1}{1}}}}$$

can be simplified and written as a single rational number. Determine exactly that rational number.

Solution

Working from the inside and going out is your best approach.

$$5-\frac{1}{4-\dfrac{1}{3-\dfrac{1}{2-\dfrac{1}{1}}}} = 5-\frac{1}{4-\dfrac{1}{3-\dfrac{1}{1}}} = 5-\frac{1}{4-\dfrac{1}{2}} = 5-\frac{1}{(7/2)} = 5-\frac{2}{7} = \frac{33}{7}.$$

If the problem had been to find x such

$$5-\frac{1}{4-\dfrac{1}{3-\dfrac{1}{2-x}}} = \frac{33}{7}$$

then working from outside and going in is the best approach (in my opinion, at least).

■

(TT892)

2. The fraction $\frac{37}{13}$ can be written in the form $2 + \cfrac{1}{x + \cfrac{1}{y + \frac{1}{z}}}$ where x, y, and z are positive integers. Find (x,y,z).

Solution

$$\frac{37}{13} = 2 + \frac{11}{13} = 2 + \frac{1}{\frac{13}{11}} = 2 + \cfrac{1}{1 + \frac{2}{11}}$$

$$= 2 + \cfrac{1}{1 + \frac{1}{11/2}} = 2 + \cfrac{1}{1 + \cfrac{1}{5 + \frac{1}{2}}}$$

x, y, z

■

(TA164) Let $n = 200$. If

$$x = \cfrac{1}{n + \cfrac{n-1}{n-2 + \cfrac{n-3}{n-4 + \cfrac{n-5}{\ddots}}}}$$

$$\cfrac{}{(n-n+2) + (n-n+1)}$$

the continued fraction until $n - k = 1$, determine exactly the value of x.

Solution

The last three values in this fraction are $\frac{3}{2+1} = 1$. *If we work our way up the fraction, we obtain* $\cfrac{5}{4 + \frac{3}{2+1}} = 1$. *This pattern continues and we notice* $\cfrac{n-1}{n-2 + \cfrac{n-3}{n-4 + \frac{n-5}{\ddots}}} = 1$. *This means* $x = \frac{1}{n+1} = \frac{1}{201}$.

■

(1T046)

Give a numeric value for the continued fraction

$$\cfrac{3}{2+\cfrac{3}{2+\cfrac{3}{2+\ddots}}}$$

Solution

To simplify an infinite continued fraction that we will label as x, look for a way to rewrite a "smaller" part of the fraction in terms of the same x. Then solve for x.

$$x = \cfrac{3}{2+\cfrac{3}{2+\cfrac{3}{2+\ddots}}} = \cfrac{3}{2+\left(\cfrac{3}{2+\cfrac{3}{2+\ddots}}\right)} = \frac{3}{2+x}$$

That is,

$$x = \frac{3}{2+x} \Rightarrow x(2+x) = 3 \Rightarrow x^2 + 2x - 3 = 0 \Rightarrow (x+3)(x-1) = 0.$$

So, $x = -3$ and $x = 1$. But $x = -3$ is an extraneous solution (a false solution that satisfies the final step of the derivation but does not satisfy the original problem) so it does not count as a solution. (i.e. toss out $x = -3$ because x is clearly positive)

So,

$$x = \cfrac{3}{2+\cfrac{3}{2+\cfrac{3}{2+\ddots}}} = 1.$$

■

(1T034)

4. Give a numeric value for the continued fraction $\cfrac{6}{1+\cfrac{6}{1+\cfrac{6}{1+\cfrac{6}{1+\ddots}}}}$

Solution

Let the given expression be x. Then

$$x = \frac{6}{1+x} \;; \qquad x^2 + x - 6 = 0$$

$$(x-2)(x+3) = 0 \;; \qquad x = 2 \text{ or } x = -3$$

But clearly $x > 0$, so $x = 2$.

■

Chapter 11. Representations as a Difference or Sum of Two Squares

2.3 Representations as sums of two squares

The first result that we need is the fact that we can solve a quadratic congruency modulo a prime only in the trivial way:

Theorem 2.3.1. *Let p be a prime number. Then the quadratic equation $x^2 \equiv 1$ (mod p) has only "two" solutions: $x \equiv \pm 1$ (mod p).*

Theorem 2.3.3. *Consider a prime number p. The equation $x^2 \equiv -1$ (mod p) has solutions if and only if $p = 2$ or $p \equiv 1$ (mod 4).*

If p is an odd prime, then the congruence

$$x^2 \equiv -1 \pmod{p}$$

has the solutions

$$x \equiv \pm \left\lfloor \frac{p-1}{2} \right\rfloor ! \pmod{p}$$

if $p \equiv 1 \pmod 4$ and has no solution if $p \equiv 3 \pmod 4$.

If p is an odd prime, $p|(a^2 + b^2)$, and $(a, b) = 1$, the $p \equiv 1 \pmod 4$.

Theorem 2.3.4. (Fermat) *Let p be a prime such that $p \equiv 1$ (mod 4) or $p = 2$. Then there is a representation of p as sum of two perfect squares: $p = x^2 + y^2$ with $x, y \in \mathbb{N}$ and $x < y$. This representation is unique.*

Lemma 2.13 *If p is a prime number and $p \equiv 1 \pmod 4$, then there exist positive integers a and b such that $a^2 + b^2 = p$.*

Lemma 2.14 *Let q be a prime factor of $a^2 + b^2$. If $q \equiv 3 \pmod 4$ then $q|a$ and $q|b$.*

Theorem 2.15 *Fermat. Write the canonical factorization of n in the form*

$$n = 2^{\alpha} \prod_{p \equiv 1(4)} p^{\beta} \prod_{q \equiv 3(4)} q^{\gamma}.$$

Then n can be expressed as a sum of two squares of integers if and only if all the exponents γ are even.

2008 Lehigh University High School Math Contest, Problem #29

29. How many integers between 1 and 1000 cannot be expressed as the difference of squares of integers?

Solution

29. 250. [20,14] It is all numbers of the form $4k + 2$ from 2 to 998. To see this, first note that if $n = x^2 - y^2 = (x - y)(x + y)$, then n is the product of two even numbers or of two odd numbers, and hence n cannot be of the form $4k + 2$. On the other hand, $2k + 1 = (k + 1)^2 - k^2$ and $4(m + 1) = (m + 2)^2 - m^2$.

■

This question comes from Saylor course MA111 which took the question from the 2011 Mathcounts national competition.

How many positive integers less than 2011 cannot be expressed as the difference of the squares of two positive integers?

Solution

Only numbers of the form $4k + 2$ *cannot* be expressed as difference of two squares.

1

Because $a^2 \equiv 0$ or $1 \pmod 4$ for all integers a, it follows that

$$a^2 - b^2 \equiv 0, 1, 3 \pmod 4$$

So, if $n \equiv 2 \pmod 4$, we cannot find a and b such that $n = a^2 - b^2$.
Now, for $n \equiv 1$ or $3 \pmod 4$, then we have the following identity,

$$n = (\frac{n+1}{2})^2 - (\frac{n-1}{2})^2$$

And if $n \equiv 0 \pmod 4$, then we have

$$n = (\frac{n}{4} + 1)^2 - (\frac{n}{4} - 1)^2$$

So, the given solution is wrong somehow. They should have counted the integers of the form $4k + 2$ along with the integers 1 and 4, as they want difference of squares of "positive" integers, which is not satisfied with 1 and 4 in the given identities and also no two perfect squares of positive integers differ by 1 or 4 which can be easily checked by the increasing sequence of squares $1, 4, 9, \ldots$.
But the answer is 505 anyway!

https://math.stackexchange.com/questions/934124/how-many-ways-are-there-to-write-675-as-a-difference-of-two-squares

How many ways are there to write the number 675 as a difference of two squares?

Suppose we have to solve $a^2 - b^2 = n$.

Write $n = pq$ where p and q have the same parity ($p \equiv q \mod 2$) and assume $p \geq q$.

Clearly:

$$\left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 = pq = n$$

Now, show that if p and q don't have the same parity, then $a + b = p$ and $a - b = q$ cannot be solved in integers.

More information: In the case of $675 = 25 \times 27 = pq$, we want p and q to be both odd. But all divisors of 675 are odd. 675 has 12 divisors (why?). now only half of them will have $p \geq q$. So 675 can be written as a difference of two squares in 6 different ways.

Now let's explicitly list these 6 ways using our observation. Notice:

$$675 = 675 \cdot 1 = 135 \cdot 5 = 27 \cdot 25 = 75 \cdot 9 = 225 \cdot 3 = 45 \cdot 15 = p \cdot q.$$

The corresponding solutions using $a = \frac{p+q}{2}, b = \frac{p-q}{2}$ are:

$$675 = 338^2 - 337^2.$$

$$675 = 70^2 - 65^2.$$

$$675 = 26^2 - 1^2.$$

$$675 = 42^2 - 33^2.$$

$$675 = 114^2 - 111^2.$$

$$675 = 30^2 - 15^2.$$

Chapter 12. Decimals, Repeating Decimals

Theorem 1
Every repeating decimal can be expressed in the form a/b where a and b are integers.

■

Theorem 2

A fraction a/b, where a and b are relatively prime integers, is terminating ⇔ the prime factorization of b only contains 2's and/or 5's.

■

A **pure repeating decimal** is a repeating decimal in which all the digits are periodic, *i.e.* the perodicity starts at the decimal point.

For any pure repeating decimal, $0.\overline{d_1 \dots d_P} = \frac{R}{10^P - 1}$, where $R = d_1 \dots d_P$ is the repetend and P is the period.

PROOF. A repeating decimal is a convergent geometric series. $0.\overline{d_1 \dots d_P}$ is a convergent geometric series whose first term is $0.d_1 \dots d_P$ and whose term ratio is 10^{-P}. The sum is therefore

$$\frac{0.d_1 \dots d_P}{1 - 10^{-P}} = \frac{\frac{R}{10^{-P}}}{1 - 10^{-P}} = \frac{R}{10^P - 1}. \square$$

For example, the pure repeating decimal

$$0.23232323 \cdots = 0.\overline{23} = \frac{23}{99}$$

and also

$$0.432143214321 \cdots = 0.\overline{4321} = \frac{4321}{9999}.$$

In this first example, $0.23232323 \cdots$ the repetend R is 23 and the period is 2. The formula

$$0.\overline{d_1 d_2 \cdots d_P} = \frac{d_1 d_2 \cdots d_p}{10^p - 1}$$

is valid even if R is not the *shortest* possible period. For example, instead of thinking of $0.23232323\cdots$ as a pure repeating decimal with repetend 23 and period 2 we can view this number as a pure repeating decimal with repetend 2323 and period 4. That is,

$$0.\overline{23} = 0.\overline{2323}.$$

From the above result this would imply that

$$\frac{23}{99} \stackrel{?}{=} \frac{2323}{9999}.$$

Verifying this particular by cross multiplication and simplification reveals why this will always be the case.

$$\begin{aligned} 9999 \cdot 23 &\stackrel{?}{=} 99 \cdot 2323 \\ (10000-1) \cdot 23 &\stackrel{?}{=} (100-1) \cdot 2323 \\ 230000 - 23 &\stackrel{?}{=} 232300 - 2323 \\ 230000 - 23 &\stackrel{?}{=} 232300 - 2300 - 23 \\ 230000 - 23 &\stackrel{\checkmark}{=} 230000 - 23. \end{aligned}$$

For $1/q$ with a prime denominator other than 2 or 5, all cycles n/q have the same length. Conway, J. H. and Guy, R. K. ``Fractions Cycle into Decimals.'' In *The Book of Numbers.* New York: Springer-Verlag, pp. 157-163 and 166-171, 1996.

December, 1999, MT Calendar, Problem 13

Express $0.\overline{1} + 0.\overline{12} + 0.\overline{123}$ as a repeating decimal.

Solution

$$\begin{aligned} 0.\overline{1} + 0.\overline{12} + 0.\overline{123} &= \frac{1}{9} + \frac{12}{99} + \frac{123}{999} \\ &= \frac{111111}{999999} + \frac{121212}{999999} + \frac{123123}{999999} \end{aligned}$$

$$= \frac{355446}{999999}$$

$$= 0.\overline{355446}\,.$$

Notice that the least common multiple of the three period lengths of $1,2$ and 3 is 6. This is why it is necessary to the common denominator to have six 9's.

■

(1A954)

Find $1.25757575\ldots = 1.25\overline{75}$. Express your answer as the quotient of relatively prime integers.

Solution

Let $x = 1.25757575\ldots = 1.25\overline{75}$. Then

$$100x = 125.\overline{75}$$

and

$$10{,}000x = 12575.\overline{75}.$$

Therefore,

$$10{,}000x - 100x = 12575 - 125$$

$$9900x = 12450$$

$$x = \frac{12450}{9900} = \frac{2 \cdot 3 \cdot 5^2 \cdot 83}{2^2 \cdot 3^2 \cdot 5^2 \cdot 11} = \frac{83}{66}.$$

■

(TA094)

For certain digits A and B, the quantity $x = (0.\overline{3A})(0.B25)$ is a **non-repeating** decimal. Compute the sum of all possible values of x.

Solution

Theorem

A fraction a/b, where a and b are relatively prime integers, is terminating $\Leftrightarrow$ the prime factorization of b only contains 2's and/or 5's.

$0.3\overline{A} = \frac{30+A}{99} = \frac{30+A}{3\cdot 3\cdot 11}$, *while* $0.B25 = \frac{100B+25}{1000} = \frac{4B+1}{40}$. *For their product to be non-repeating, we need all factors of 3 and 11 to be removed from the denominator.*

Consider the possibilities: $30+A \in \{30,31,32,33,34,35,36,37,38,39\}$

$4B+1 \in \{1,5,9,13,17,21,25,29,33,37\}$

If $30 + A = 30, 36,$ *or* 39, *each contributes at least one factor of 3, so* $4B + 1 = 33$ *will cancel the rest of the undesirable factors. If* $30 + A = 33$, *then we only need* $4B + 1$ *to contribute a single factor of 3, so* $4B + 1 = 9, 21,$ *or* 33.

$$\left(\frac{30}{99}+\frac{36}{99}+\frac{39}{99}\right)\left(\frac{33}{40}\right)+\left(\frac{33}{99}\right)\left(\frac{9}{40}+\frac{21}{40}+\frac{33}{40}\right)=\left(\frac{105}{3\cdot 40}\right)+\left(\frac{63}{3\cdot 40}\right)=\frac{168}{120}=\frac{7}{5}.$$

■

Example 32.

Convert $0.38\overline{427} = 0.38427427427\cdots$ into a rational number.

Solution

Let $s = 0.38\overline{427} = 0.38427427427\ldots$

Then,

$$100000s = 38427.427427427\ldots$$
$$100s = 38.427427427\ldots$$

and

$$100000s - 100s = 38427 - 38$$
$$99900s = 38389$$

So,

$$s = 0.38\overline{427} = \frac{38389}{99900}..$$

■

12.1 Basimals

Numbers of the form $(0.a_1a_2a_3\cdots)_{10} = \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \cdots$ with $a_j \in \{0,1,2,3,\ldots,9\}$ are called decimals.

Analogously, we define the term ***basimals*** for non-base 10 numbers of this form. That is, a basimal is a number of the form $(0.a_1a_2a_3\cdots)_k = \frac{a_1}{k} + \frac{a_2}{k^2} + \frac{a_3}{k^3} + \cdots$ with $a_j \in \{0,1,2,\ldots,k-1\}$.

■

12.1.1 Converting Basimals

Example 33.
Convert the basimal number 0.234_6 to a fraction in base 10.

Solution
We have

$$0.234_6 = \frac{2}{6^1} + \frac{3}{6^2} + \frac{4}{6^3}.$$

So,

$$0.234_6 = \frac{2}{6^1} + \frac{3}{6^2} + \frac{4}{6^3} = \frac{2(6^2) + 3(6) + 4}{6^3} = \frac{72 + 18 + 4}{216} = \frac{94}{216}.$$

■

12.1.2 Converting a Repeating Basimal Number

Example 34.
Convert $0.\overline{234}_6$ to a fraction in base 10.

Solution

Let $x = \overline{234}_6$. Then $1000_6 \cdot x = (1000_6) \cdot \left(\overline{234}_6\right) = 234.\overline{234}_6$

Therefore,

$$1000_6 \cdot x - x = 234.\overline{234}_6 - 0.\overline{234}_6 = 234_6.$$

$$(1000_6 - 1_6)x = 234_6$$

$$(555_6)x = 234_6$$

$$x = \frac{234_6}{555_6}.$$

Now separately convert 234_6 and 555_6 to base 10.

$$234_6 = 2 \cdot 6^2 + 3 \cdot 6^1 + 4 \cdot 6^0 = 72 + 18 + 4 = 94_{10}$$

$$555_6 = 5 \cdot 6^2 + 5 \cdot 6^1 \cdot 5 \cdot 6^0 = 5(6^2 + 6^1 + 6^0) = 6^3 - 1 = 216 - 1 = 215_{10}$$

Note:

$$s = 6^2 + 6^1 + 6^0$$
$$6s = 6^3 + 6^2 + 6^1$$
$$\therefore \quad 5s = 6^3 - 6^0 = 6^3 - 1$$

Therefore,

$$0.\overline{234}_6 = \frac{234_6}{555_6} = \frac{94_{10}}{215_{10}}.$$

■

Example 35.

Convert $0.\overline{31}_5$ to a fraction in base 10.

Solution

Let $x = 0.\overline{31}_5$. Then $100_5 \cdot x = 100_5 \cdot \overline{31}_5 = 31.\overline{31}_5$. Therefore

$$100_5 x - x = 31.\overline{31}_5 - 0.\overline{31}_5 = 31_5$$

$$(100_5 - 1_5)x = 31_5$$

$$44_5 \cdot x = 31_5$$

$$x = \frac{31_5}{44_5} = \frac{3(5^1) + 1(5^0)}{4(5^1) + 4(5^0)} = \frac{16_{10}}{24_{10}} = \frac{16}{24} = \frac{2}{3}.$$

■

AMC 1966, Problem #39

In base R_1 the expanded fraction F_1 becomes $0.373737\cdots$, and the expanded fraction F_2 becomes $0.737373\cdots$. In base R_2 fraction F_1, when expanded, becomes $0.252525\cdots$, while fraction F_2 becomes $0.525252\cdots$. The sum of R_1 and R_2 each written in the base ten, is:

(A) 24	(B) 22	(C) 21	(D) 20	(E) 19

Solution

■

12.1.3 Converting a Decimal to a Basimal Number

Example 36.

Convert $\frac{3}{5} = .6$ to a basimal in base 7.

Solution

In analogy to how we can express an integer in base 10 to an integer in base 7 we ask what is the largest fraction $\frac{k}{7}$, $k = 0,1,2,3,4,5,6$ that is less than or equal to $\frac{3}{5}$.

$$\frac{4}{7} \approx 0.57 < \frac{3}{5} = .6 < \frac{5}{7} \approx .71$$

So, the first digit must be 4.

Now repeat this process by finding the largest fraction $\frac{k}{7^2}$, $k = 0,1,2, \ldots ,6$ that is less than or equal to $\frac{3}{5} - \frac{4}{7} = \frac{1}{35} \approx 0.029$. We note that

$$\frac{1}{49} \approx 0.020 < \frac{1}{35} \approx 0.028 < \frac{2}{49} \approx 0.041.$$

So, the second digit must be 1.

This is already getting tedious! Fortunately, there is a very simple short cut procedure.

12.1.4 Introducing a Short Cut Approach

(1) Multiple the base ten decimal by the base you want to convert to. In this case, the base is 7.

$$0.6 \cdot 7 = 4.2.$$

The units digit is the first digit in the basimal representation in base 7.

$$0.4$$

(2) Multiple just the decimal part of the above product (*i.e.* the 0.2 from the product 4.2) by 7.

$$0.2 \cdot 7 = 1.4$$

The units digit in this product is the second digit in the basimal representation in base 7.

$$0.41$$

(3) Repeat

$$0.6 \cdot 7 = 4.2 \Longrightarrow 0.4$$
$$0.2 \cdot 7 = 1.4 \Longrightarrow 0.41$$
$$0.4 \cdot 7 = 2.8 \Longrightarrow 0.412$$
$$0.8 \cdot 7 = 5.6 \Longrightarrow 0.4125$$
$$\vdots$$

We can see that this basimal will continuously repeat the pattern 4125 after this. That is,

$$0.6_{10} = 0.\overline{4125}_7 .$$

■

Check!

$$x = 0.\overline{4125}_7$$
$$10000_7 \cdot x = 4125.\overline{4125}_7$$

$$10000_7 \cdot x - x = 4125_7$$
$$6666_7 \cdot x = 4125_7$$

$$x = \frac{4125_7}{6666_7} = \frac{4 \cdot 7^3 + 1 \cdot 7^2 + 2 \cdot 7^1 + 5 \cdot 7^0}{6 \cdot 7^3 + 6 \cdot 7^2 + 6 \cdot 7^1 + 6 \cdot 7^0} = \frac{1440}{2400} = 0.6$$

■

(3D134) Convert the base-ten fraction $\frac{13}{16}$ into a base-eight equivalent that does not involve a quotient (fraction bar).

Solution

Since place values to the right of the radix ("basimal") point in base-eight are based on powers of 8, we might start by expressing $\frac{13}{16}$ *with a denominator that is a power of 8:* $\frac{52}{64}$. *Now we proceed through the base-eight place values in order: there are six eighths* $\left(\frac{48}{64}\right)$ *in* $\frac{52}{64}$, *with four sixty-fourths remaining. That equates to the decimal* 0.64_8.

■

(3T136) Find the number base n such that $\left(\frac{5}{24}\right)_{10} = (0.113)_n$.

Solution

$\frac{5}{24}=0.113_n \Rightarrow \frac{1}{n}+\frac{1}{n^2}+\frac{3}{n^3}=\frac{5}{24}$. *Multiply both sides by the LCD* $\left(24n^3\right)$ *to obtain* $24n^2+24n+72=5n^3$, *which rearranges to form* $5n^3-24n^2-24n-72=0$. *Combine the Rational Roots Theorem with the fact that n must be a whole number to obtain the factors of* 72 *as choices*: 1, 2, 3, 4, 6, 8, 9, 12, *etc. The first three of these aren't possible, since we are given a basimal with* 3 *as a digit. Use synthetic division to evaluate the polynomial for other values, revealing that n =* $\boxed{6}$.

■

AMC 2019 10A Problem #18

For some positive integer k, the repeating base-k representation of the (base-ten) fraction $\frac{7}{51}$ is $0.\overline{23}_k = (0.232323\ldots)_k$. What is k?

(A) 13	(B) 14	(C) 15	(D) 16	(E) 17

Solution

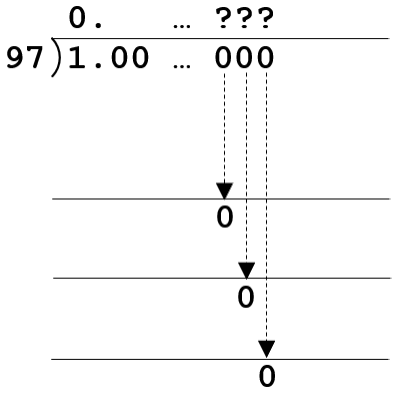
■

12.2 Repetends

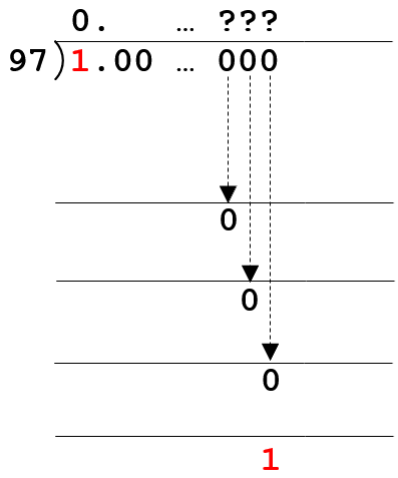
Example 37.
When expanded as a decimal, the fraction $1/97$ has a ***repetend*** (the repeating part of the decimal) of 96 digits that start right after the decimal point. Find the last three digits CBA of the repetend.

Solution
We need to reverse engineer the standard long-division algorithm.

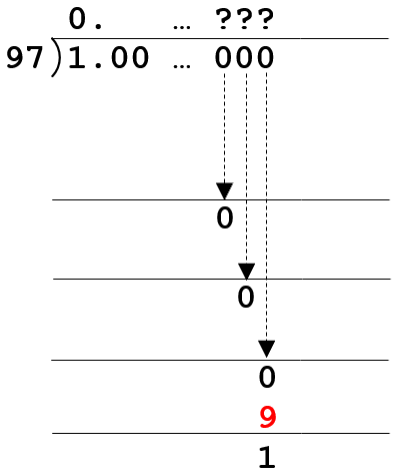
We want to determine the last three digits in the repetend so draw a three step long-division grid with the three "dropped" 0's in place.



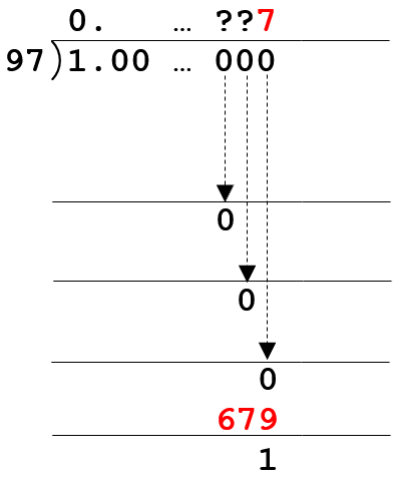
The quotient will restart its repeating pattern when the remainder is the same as the dividend. That is, when the remainder equals 1.



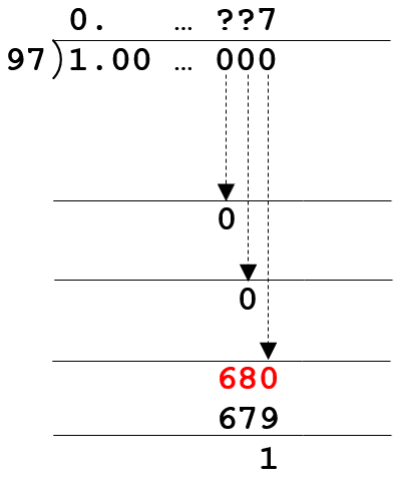
The last digit in this row must be a 9 in order to leave a difference of 1 $(10 - 9 = 1)$.



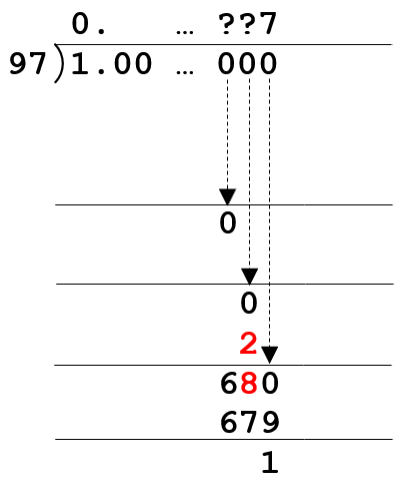
The third $? = 7$ because $97 \times ?$ must end in a 9 and the only digit times 7 that ends in a 9 is 7 $(7 \times 7 = 49)$. Now that we have the third $? = 7$ we can see that $97 \times ? = 97 \times 7 = 679$.



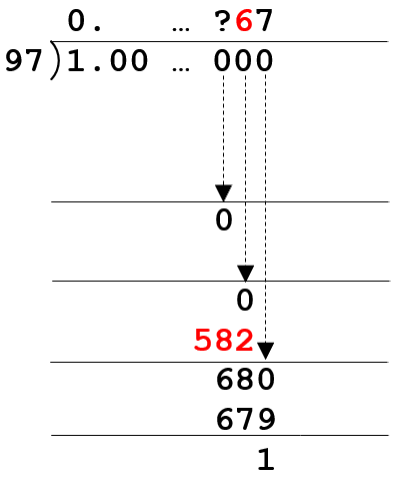
In order to leave a difference of 1 we have to subtract the 679 from 680.



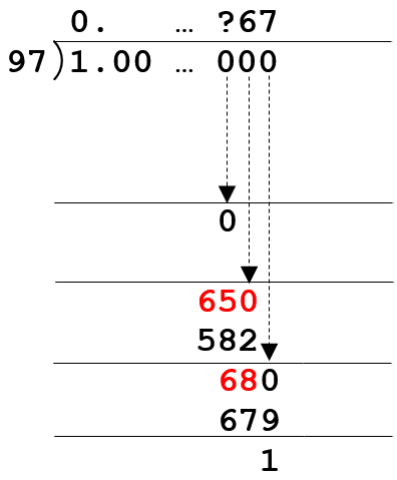
The last digit in the next row up must be a 2 in order to leave a difference of 8 $(10 - 2 = 8)$.



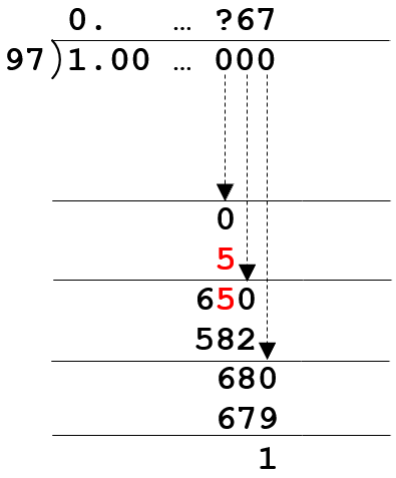
The next $? = 6$ because $97 \times ?$ must end in a 2 and the only digit times 7 that ends in a 2 is 6 ($7 \times 6 = 4\mathbf{2}$). Now that we have the next $? = 2$ we have $97 \times ? = 97 \times 6 = 582$.



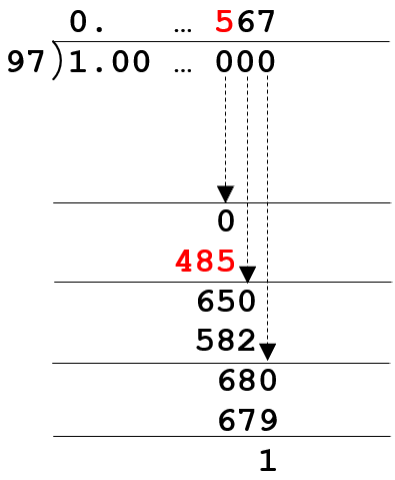
In order to leave a difference of 68 we have to subtract the 582 from 650.



The last digit in the next row up must be a 5 in order to leave a difference of 5 $(10 - 5 = 5)$.



The first $? = 5$ because $97 \times ?$ must end in a 5 and the only digit times 7 that ends in a 5 is 5 $(7 \times 5 = 35)$. Now that we have the next $? = 5$ we have $97 \times ? = 97 \times 5 = 485$.



Of course, we could continue to work backwards but the question only asked for the last three digits of the repetend.

We have reversed engineered (worked backwards) the long division process to find out that the last three digits of the repetend are 567.

■

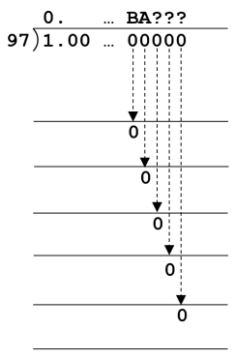
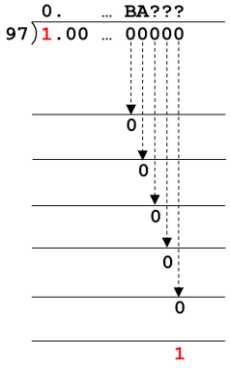
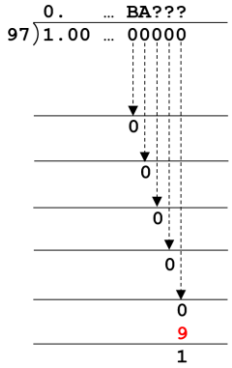
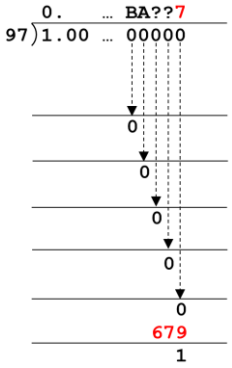
(1T015)

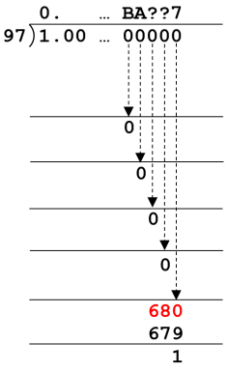
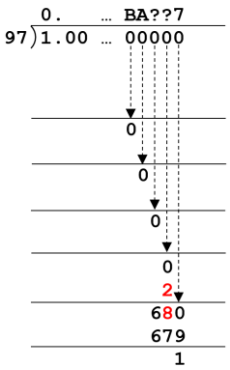
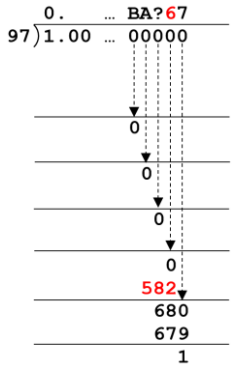
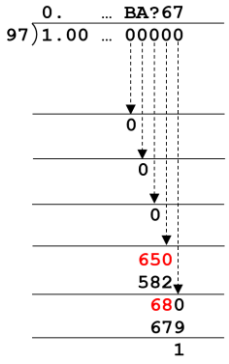
When expanded as a decimal, the fraction $1/97$ has a repetend (the repeating part of the decimal) of 96 digits that start right after the decimal point. If the last five digits of the repetend are $\mathrm{BA}567$, find the digits A and B.

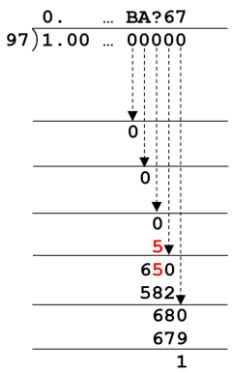
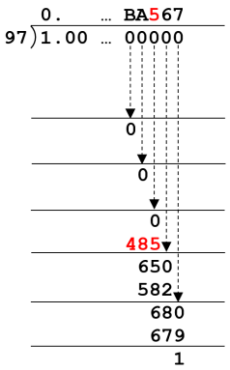
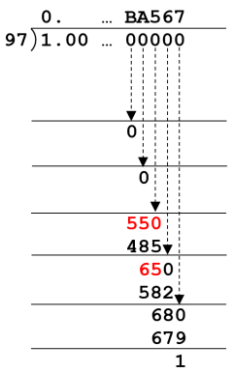
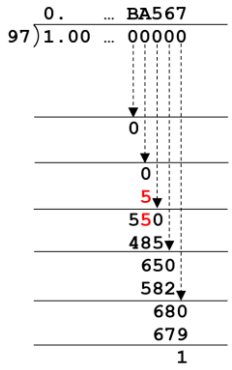
Solution

You need to reverse engineer the standard long-division algorithm.

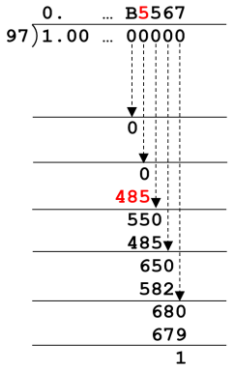
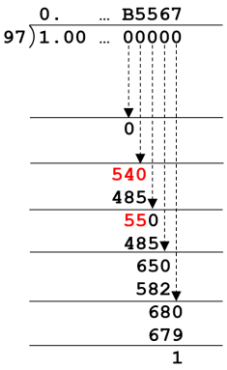
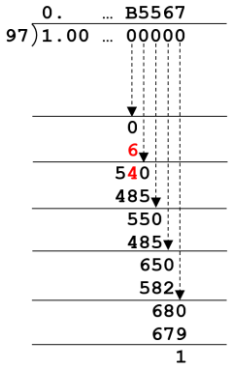
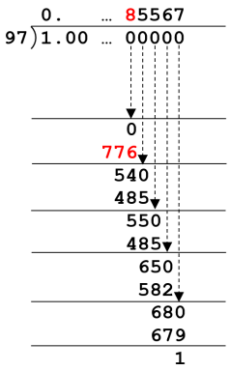
Step 1	Step 2	Step 3	Step 4

			
We want to determine the last five digits in the repetend so draw a five step long-division grid with the five "dropped" 0's in place.	The quotient will restart its repeating pattern when the remainder is the same as the dividend. That is, when the remainder equals 1.	The last digit in this row must be a 9 in order to leave a difference of 1 $(10 - 9 = 1)$.	The third $? = 7$ because $97 \times ? = 7$ must end in a 9 and the only digit times 7 that ends in a 9 is 7 $(7 \times 7 = 49)$. Now that we have the third $? = 7$ we can see that $97 \times ? = 97 \times 7 = 679$.

Step 5	**Step 6**	**Step 7**	**Step 8**
			
In order to leave a difference of 1 we have to subtract the 679 from 680.	The last digit in this row must be a 2 in order to leave a difference of 8 $(10 - 2 = 8)$.	The next $? = 6$ because $97 \times ?$ must end in a 2 and the only digit times 7 that ends in a 2 is 6 $(7 \times 6 = 42)$. Now that we have the next $? = 2$ we have $97 \times ? = 97 \times 6 = 582$.	In order to leave a difference of 68 we have to subtract the 582 from 650.

Step 9	**Step 10**	**Step 11**	**Step 12**
			
The last digit in this next row up must be a 5 in order to leave a difference of 5 $(10 - 5 = 5)$.	The next $? = 5$ because $97 \times ?$ must end in a 5 and the only digit times 7 that ends in a 5 is	In order to leave a difference of 65 we have to subtract the 485 from 550.	The last digit in this next row up must be a 5 in order to leave a difference of 5 $(10 - 5 = 5)$.

	5 ($7 \times 5 = 35$). Now that we have the next $? = 5$ we have $97 \times ? = 97 \times 5 = 485$.		

Step 13	**Step 14**	**Step 15**	**Step 16**
			
$A = 5$ because $97 \times A$ must end in a 5 and the only digit times 7 that ends in a 5 is 5 ($7 \times 5 = 35$). Now that we have $A = 5$ we have $97 \times A = 97 \times 5 = 485$.	In order to leave a difference of 55 we have to subtract the 485 from 540.	The last digit in this next row up must be a 6 in order to leave a difference of 4 ($10 - 6 = 4$).	$B = 8$ because $97 \times B$ must end in a 6 and the only digit times 7 that ends in a 6 is 8 ($7 \times 8 = 56$). Now that we have $B = 8$ we have $97 \times B = 97 \times 8 = 776$.

We have determined that $B = 8$ and $A = 5$ by this reverse engineered long division.

■

(1T996)

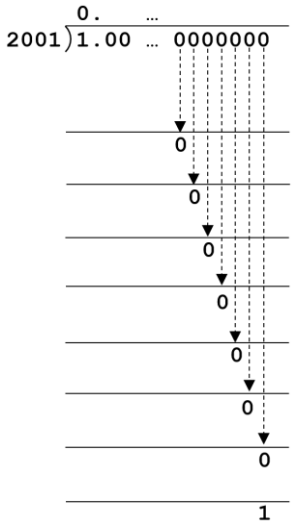
Find the last seven digits of the repetend of the fraction $1/2001$. That is, if we write

$$1/2001 = .abc \ldots efghijkabc \ldots efghijk\overline{abc \ldots efghijk} \ldots,$$

find the digits $efghijk$.

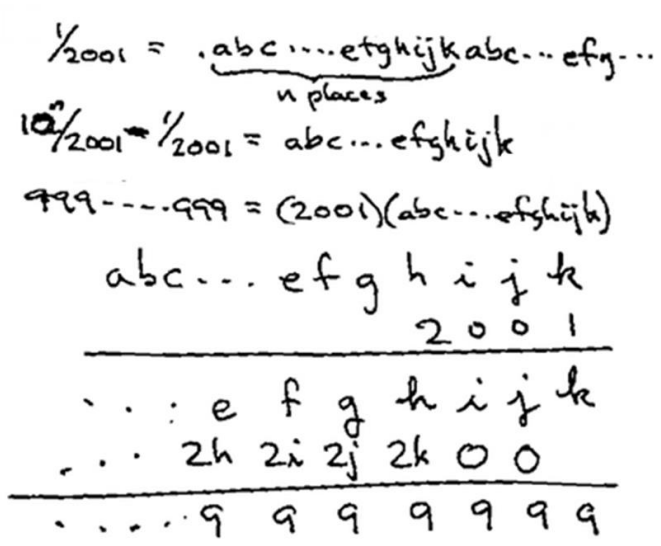
Solution

You can use the following blank "reverse engineered repetend form" as an aid in keeping the columns lined up. It might help to cut, paste and enlarge the blank form on a separate piece of paper.



You should find that the last seven digits are 6001999.

Alternatively,



k=9, j=9, i=9, 2k=18, so
h+8=9, h=1, and we carry 1 to the next place. Then 2j=18, so,
1+g+8=9, g=0. Similarly, 2i=18, so 1+f+8=9, ∴ f=0. Finally, 2h=2
1+e+2=9, so e=6.
∴ Last 7 places in repetend:
6001999

■

What is the maximum number of digits possible in the repeating block when you divide out the rational 1/46229. How do you know this?

The maximum number of digits possible is always one less than the denominator. In this case the maximum number of digits *possible* in the repetend is 46,229-1=46,228. The reason is that given any number the number of possible remainders is always one less than the denominator or the divisor. For example, express 4/7 as a repeating decimal. The possible remainders are 1,2,3,4,5, and 6 when you divide by 7.

Wiki

Fractions with prime denominators [edit]

A fraction in lowest terms with a prime denominator other than 2 or 5 (i.e. coprime to 10) always produces a repeating decimal. The length of the repetend (period of the repeating decimal segment) of 1/*p* is equal to the order of 10 modulo *p*. If 10 is a primitive root modulo *p*, the repetend length is equal to *p* − 1; if not, the repetend length is a factor of *p* − 1. This result can be deduced from Fermat's little theorem, which states that $10^{p-1} \equiv 1 \pmod{p}$.

The base-10 repetend of the reciprocal of any prime number greater than 5 is divisible by 9.[5]

If the repetend length of 1/*p* for prime *p* is equal to *p* − 1 then the repetend, expressed as an integer, is called a **cyclic number**.

Totient rule [edit]

For an arbitrary integer *n* the length $\lambda(n)$ of the repetend of 1/*n* divides $\phi(n)$, where ϕ is the totient function. The length is equal to $\phi(n)$ if and only if 10 is a primitive root modulo *n*.[7]

In particular, it follows that $\lambda(p) = p - 1$ if and only if *p* is a prime and 10 is a primitive root modulo *p*. Then, the decimal expansions of *n*/*p* for *n* = 1, 2, ..., *p* − 1, all have period *p* − 1 and differ only by a cyclic permutation. Such numbers *p* are called full repetend primes.

Other properties of repetend lengths [edit]

Various properties of repetend lengths (periods) are given by Mitchell[9] and Dickson.[10]

The period of 1/*k* for integer *k* is always ≤ *k* − 1.

If *p* is prime, the period of 1/*p* divides evenly into *p* − 1.

If *k* is composite, the period of 1/*k* is strictly less than *k* − 1.

The period of *c*/*k*, for *c* coprime to *k*, equals the period of 1/*k*.

If $k = 2^a 5^b n$ where *n* > 1 and *n* is not divisible by 2 or 5, then the length of the transient of 1/*k* is max(*a*, *b*), and the period equals *r*, where *r* is the smallest integer such that $10^r \equiv 1 \pmod{n}$.

Mu Alpha Theta National Convention 2005, Number Theory Test, Alpha Division, Problem #26

26. Find the smallest natural number, n, such that the decimal form of $\frac{1}{n}$ has at least 18 digits in its block of repeating digits.

A) 13 B) 17 C) 19 D) 49 E) NOTA

Solution

When evaluating the number repeating digits in a decimal expansion, we can note that 1/n has at most n - 1 digits in its expansion. This is due to the fact that there are at most n - 1 distinct positive remainders when dividing by n in long division. Once we have repeated a remainder, a cycle ensues as the next remainder must have been the same as before. Note that I've made the assumption that we stripped powers of 2 and 5 out of n, but the fact that n - 1 is the largest number of digits in the repeating block is still valid.

We now see that n = 19 is the smallest possibility and we note that fortunately, it's the answer:

$$\frac{1}{19} = 0.\overline{052631578947368421}.$$

Further exploration could highlight some facts that make this solution more obvious and the ideas here connect with Euler's Phi Function and other number theoretic ideas. Further exploration is left to the reader both because that's the best way to learn and it could take pages to write up.

■

Chapter 13. Miscellaneous

13.1 Number of Digits

Let $\text{nd}(a)$ represent the number of digits in the (base 10) number a. Then

$$\text{nd}(a) = \lfloor \log_{10}(a) \rfloor + 1.$$

Proof

Suppose $a = 10^x$ for some real number $x \geq 0$. Then a consists of $\lfloor x \rfloor + 1$ digits. We also know that $a = 10^{\log_{10}(a)}$. Therefore, for any positive number a,

$$\text{nd}(a) = \lfloor \log_{10}(a) \rfloor + 1.$$

■

This result is particularly useful when the number a is expressed in exponential form. Consider the following example.

How many digits are there in the integer representation of 2^{2001} ?

Solution

$$\begin{aligned} \text{nd}(2^{2001}) &= \lfloor \log_{10}(2^{2001}) \rfloor + 1 \\ &= \lfloor 2001 \cdot \log_{10}(2) \rfloor + 1 \\ &= \lfloor 602.361 \rfloor + 1 \\ &= 602 + 1 \\ &= 603. \end{aligned}$$

■

(1T885)

Consider the integer $M = 5^{25}$.

(a) How many digits does it take to write M using ordinary base ten notation?
(b) What are the last three digits of M?

Solution

With your calculator, you get

$$5^{25} = \frac{10^{25}}{2^{25}} \approx \frac{10^{25}}{3.3554432\,(10)^7}$$

$\approx .29\ldots \cdot 10^{18}$, an 18 digit integer

(Without a calculator, show $10^{17} < 5^{25} < 10^{18}$)

$5^3 = 125$ $\quad$ $\begin{array}{r} 125 \\ \hline 625 \end{array}$ $\quad$ $\begin{array}{r} 625 \\ \hline 3125 \end{array}$

Once $n \geq 3$, the last three digits oscillate between 125 and 625, with odd n giving 125

Or, one may note $5^5 \equiv 125 \mod 1000$

so $5^{25} \equiv (125)^5 = 5^{15} = (5^5)^3 \mod 100$

Continue in this way to get

$5^{25} \equiv 125 \mod 1000.$

■

College of Charleston

2. If m and n are two positive integers such that $\log_{10} m = 12.3\ldots$ and $\log_{10} n = 15.4\ldots$, how many digits are there in the decimal expansion of the product $m \cdot n$?

   (A) 3 (B) 16 (C) 27 (D) 28 (E) 189

Solution

$$\text{nd}(a) = \lfloor \log_{10}(a) \rfloor + 1$$

$$\begin{aligned} \text{nd}(mn) &= \lfloor \log_{10}(mn) \rfloor + 1 \\ &= \lfloor \log_{10}(m) + \log_{10}(n) \rfloor + 1 \\ &= \lfloor 12.3 + 15.4 \rfloor + 1 \\ &= \lfloor 27.7 \rfloor + 1 \\ &= 27 + 1 = 28. \end{aligned}$$

■

Saint Mary's College Mathematics Contest Problems

246. How many digits are there in 5^{5^5} ?

Caution: 5^{5^5} is the (standard) notation for $5^{(5^5)}$ which is not the same as $(5^5)^5$. Tetration.

Solution

$5^{5^5} = 5^{3125}$. $3125 \log 5 =$
$3125 \times 0.69897 = 2184.3$, so
the number has 2185 digits.

■

Mu Alpha Theta National Convention 2002, Number Theory Test, Alpha Division, Problem # 6

How many digits are in 5^{5^5} ?

Solution

$5^{5^5} = x$ $\quad 5^{3125} = x$ $\quad 3125 \log 5 = \log x$ $\quad 2184.28 = \log x$ $\quad 10^{2185} = x$ # of digits

■

13.1.1 Number of Digits in Base b

Contest problems sometimes ask for the number of digits a base ten number would have if it were expressed in a different base.

Let $\text{nd}_b(c)$ represent the number of digits in the base b representation of the positive base 10 integer c. Then

$$\text{nd}_b(c) = \lfloor \log_b(c) \rfloor + 1.$$

(Note: Be aware that this result only applies when c is a base 10 number.)

Before proving this result, it will be helpful to consider a very simple example to clarify what this result tells us (and what it doesn't).

Example

How many digits are in the base 3 representation of the base ten number 143?

Solution

$$\text{nd}_3(143) = \lfloor \log_3(143) \rfloor + 1 = \lfloor 4.517 \ldots \rfloor + 1 = 4 + 1 = 5.$$

Let's check by actually writing out the base 3 representation of 143_{10}.

$$143_{10} = 1 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^2 + 2 \cdot 3^1 + 2 \cdot 3^0 = (12022)_3$$

This verifies the result that the base 10 number 143 has 5 digits when expressed in base 3.

Proof

For any integer $b \geq 2$, let $a_0, a_1, a_2, \ldots, a_{r-1}$ be a sequence of integers such that $0 \leq a_j < b$ for all $j = 0,1, \ldots, r-1$ and such that $a_{r-1} \neq 0$. Then we can say that $(a_{r-1} \cdots a_1 a_0)_b$ is a base b number of r digits.

Let c be the base 10 equivalent of $(a_{r-1} \cdots a_1 a_0)_b$. Then c equals

$$c = \sum_{i=0}^{r-1} a_i b^i.$$

Substituting the lower and upper bounds for each a_j we have

$$\sum_{i=0}^{r-1} (\mathbf{0}) b_i + (\mathbf{1}) b^{r-1} \leq \sum_{i=0}^{r-1} a_i b^i \leq \sum_{i=0}^{r-1} (\boldsymbol{b-1}) b^i$$

or

$$b^{r-1} \leq c \leq (b-1) \sum_{i=0}^{r-1} b^i$$

We recognize that

$$\sum_{i=0}^{r-1} b^i = \frac{b^r - 1}{b-1}$$

from our understanding of geometric series. Hence

$$b^{r-1} \le c \le b^r - 1$$

or equivalently

$$b^{r-1} \le c < b^r.$$

Because logarithms are increasing functions, it follows that

$$\log_b(b^{r-1}) \le \log_b(c) < \log_b(b^r)$$

$$(r-1)\log_b(b) \le \log_b(c) < r\log_b(b)$$

$$r - 1 \le \log_b(c) < r$$

Therefore,

$$r - 1 = \lfloor \log_b(c) \rfloor$$

or

$$r = \lfloor \log_b(c) \rfloor + 1$$

■

Mu Alpha Theta National Convention, 2001, Number Theory Test, Mu Division, Problem # 36
A positive integer has 32 digits when expressed in base 2. How many digits are there in the base 10 representation of that number?

Solution

36. The number in question is at least 2^{31} and less than 2^{32}. There are a couple of ways to do the problem from here. Some students may recognize that log2 ≅ .301. (31)(.301) = 9.331 and (32)(.301) = 9.632. Thus both 2^{31} and 2^{32} are ten digit numbers (logs between 9 and 10). It could also be noted that $2^{10} \cong 10^3$ and thus $2^{31} \cong 2(10^9)$ and is a ten digit number (similarly for 2^{32}). Obviously all numbers between 2^{31} and 2^{32} are also ten digit numbers.

■

13.1.2 Number of Digits in a Product

If a and b are positive integers then the number of digits in their product ab is given exactly by

$$dn(ab) =$$

If your two numbers a and b are positive integers then the number of decimal digits in their product is given exactly by

$$n = 1 + \lfloor \log_{10}(ab) \rfloor = 1 + \lfloor \log_{10}(a) + \log_{10}(b) \rfloor$$

where $\lfloor x \rfloor$ means the greatest integer not greater than x.

AMC 1969 Problem #20

Let P equal $3{,}659{,}893{,}456{,}789{,}325{,}678$ and $342{,}973{,}489{,}379{,}256$. The number of digits in P is:

(A) 36	(B) 35	(C) 34	(D) 33	(E) 32

Solution

■

13.2 Simon's Favorite Factoring Trick

Simon's Favorite Factoring Trick

Now let's get back to the magic of subtracting 10 from both sides. How did I know to do this? On math contest sites such as AoPS (https://artofproblemsolving.com/) and Math Stack Exchange (https://math.stackexchange.com/) the idea goes by the name "**Simon's Favorite Factoring Trick**" or just **SFFT**.

The general idea of SFFT is that if you have a Diophantine equation of the form

$$af(x)g(y) + abf(x) + cg(y) = d$$

in the variables x and y then add the constant bc to both sides. In this way the left-hand side will factor as

$$(af(x) + c)(g(y) + b) = d + bc.$$

By writing $d + bc$ in terms of its prime factors you can find $f(x)$ and $g(y)$ by considering cases of splitting the prime factors between the two factors on the left-hand side.

The process of adding bc to both sides is called "completing the rectangle".

(4A113) List **all** possible values of xy, if x and y are integers such that $xy = x + y + 1$.

Solution

Method 1: $xy = x + y + 1 \Rightarrow xy - x - y = 1 \Rightarrow xy - x - y + 1 = 2 \Rightarrow (x-1)(y-1) = 2$. *Since x and y are integers,* $(x-1)$ *and* $(y-1)$ *are also integers, and we consider the factorizations of 2:* *WLOG,* $x-1=2,\ y-1=1 \Rightarrow x=3,\ y=2,\ xy=6$; $x-1=-2,\ y-1=-1 \Rightarrow x=-1,\ y=0,\ xy=0$.

Method 2: $xy = x + y + 1 \Rightarrow xy - y = x + 1 \Rightarrow y(x-1) = x+1 \Rightarrow y = \dfrac{x+1}{x-1}$. *Use the Table feature on a calculator to find when x and y are both integers. Quickly,* $x=3,\ y=2 \Rightarrow xy=6$ *and* $x=-1,\ y=0 \Rightarrow xy=0$ *stand out, and a graph shows these as the only integral solutions.*

■

(1T083)

3. How many ordered pairs (a,b) of positive integers exist such that $\dfrac{1}{a} + \dfrac{5}{b} = \dfrac{1}{2}$?

[Original Source Mass. Math Olympiad, 2007-2008]

Solution

$2b + 10a = ab$ so $a = \dfrac{2b}{b-10} = 2 + \dfrac{20}{b-10}$

Since a is an integer, b-10 divides 20.
See the table. Negative values for b-10 give negative values for either a or b.

b-10	b	$a = 2 + \frac{20}{b-10}$
1	11	22
2	12	12
4	14	7
5	15	6
10	20	4
20	30	3

Alternative Method Using SFFT

$$\frac{1}{a}+\frac{5}{b}=\frac{1}{2}\Leftrightarrow\frac{2b+10a}{ab}=1\Leftrightarrow ab-2b-10a=0$$

$$\Leftrightarrow (a-2)(b-10)=20$$

$a-2=1$	$b-10=20$	$(a,b)=(3,20)$
$a-2=2$	$b-10=10$	$(a,b)=(4,20)$
$a-2=4$	$b-10=5$	$(a,b)=(6,15)$
$a-2=5$	$b-10=4$	$(a,b)=(7,14)$
$a-2=10$	$b-10=2$	$(a,b)=(12,12)$
$a-2=20$	$b-10=1$	$(a,b)=(22,11).$

Notice that if we try

$a-2=-1$	$b-10=-20$	$(a,b)=(-1,-10)$
$a-2=-2$	$b-10=-10$	$(a,b)=(0,0)$
$a-2=-4$	$b-10=-5$	$(a,b)=(-2,5)$
$a-2=-5$	$b-10=-4$	$(a,b)=(-3,6)$
$a-2=-10$	$b-10=-2$	$(a,b)=(-8,8)$
$a-2=-20$	$b-10=-1$	$(a,b)=(-18,9)$

which all fail the requirement that a and b are both positive integers. So there are a total of 6 ordered pairs for (a,b) that will satisfy the given requirements.

■

(5A934) or maybe (5D934)

4. Let $S=\left\{(m,n): m \text{ and } n \text{ are positive integers that satisfy } \frac{4}{m}+\frac{3}{n}=1\right\}$.

(a) How many ordered pairs are there in S?

(b) Find the ordered pair in S that has the largest value of m.

Solution

$4n + 3m = mn$

$mn - 4n - 3m + 12 = 12$

$(m - 4)(n - 3) = 12$

$m-4$ and $n-3$ must be integers.

We can tabulate all possibilities:

$m-4$	$n-3$	m	n
1	12	5	15
2	6	6	9
3	4	7	7
4	3	8	6
6	2	10	5
→ 12	1	16	4

(Note: Simon's Favorite Factoring Trick ?)

■

AMC 2007B Problem #23

How many non-congruent right triangles with positive integer leg lengths have areas that are numerically equal to 3 times their perimeters?

(A) 6	(B) 7	(C) 8	(D) 10	(E) 12

Solution

Involves Simon's Favorite Factoring Trick

■

National Mu Alpha Theta Convention 1991, Number Theory Topic Test, Problem #21

Find all Pythagorean triangles with the property that the area of the triangle equals the perimeter.

Solution

Let the positive integers a, b and c be the three sides of a Pythagorean triangle with hypotenuse c. Then $a^2 + b^2 = c^2$. Using this notation

$$\text{Area } \Delta = \frac{1}{2}ab \text{ and Perimeter } \Delta = a + b + c.$$

We are given the additional information that Area Δ = Perimeter Δ. With simplification we find that

$$\frac{1}{2}ab = a + b + c = a + b + \sqrt{a^2 + b^2}$$
$$ab = 2a + 2b + 2\sqrt{a^2 + b^2}$$
$$2\sqrt{a^2 + b^2} = ab - 2a - 2b$$
$$4(a^2 + b^2) = (ab - 2a - 2b)^2$$
$$4a^2 + 4b^2 = a^2b^2 - 2a^2b - 2ab^2 - 2a^2b + 4a^2 + 4ab - 2ab^2 + 4ab + 4b^2$$
$$0 = a^2b^2 - 4a^2b - 4ab^2 + 8ab$$
$$ab(ab - 4a - 4b + 8) = 0.$$

We are constrained by a, b positive integers so $ab \neq 0$. Therefore, we know

$$ab - 4a - 4b + 8 = 0.$$

Applying SFFT we see that this means

$$(a - 4)(b - 4) = 8.$$

The set of all factors of 8 are $\pm 1, \pm 2, \pm 4$ and ± 8. Considering each of these eight cases as a value for $a - 4$ produces the following results.

$$\begin{array}{llcll}
a-4=-8, & b-4=-1 & \Leftrightarrow & a=-4, & b=3 \\
a-4=-4, & b-4=-2 & \Leftrightarrow & a=0, & b=2 \\
a-4=-2, & b-4=-4 & \Leftrightarrow & a=2, & b=0 \\
a-4=-1, & b-4=-8 & \Leftrightarrow & a=3, & b=-4 \\
a-4=1, & b-4=8 & \Leftrightarrow & a=5, & b=12 \\
a-4=2, & b-4=4 & \Leftrightarrow & a=6, & b=8 \\
a-4=4, & b-4=2 & \Leftrightarrow & a=8, & b=6 \\
a-4=8, & b-4=1 & \Leftrightarrow & a=12, & b=5
\end{array}$$

We can throw out the first four answers because a and b must both be positive integers. This leaves us with two or four solutions for (a, b, c), $(5,12,13), (6,8,10), (8,6,10)$ and $(12,5,13)$, depending on whether we consider the two legs as distinct or not.

■

13.3 Mediants

In mathematics, the **mediant** of two fractions, generally made up of four positive integers

$$\frac{a}{c} \quad \text{and} \quad \frac{b}{d} \quad \text{is defined as} \quad \frac{a+b}{c+d}.$$

- **The mediant inequality:** An important property (also explaining its name) of the mediant is that it lies strictly between the two fractions of which it is the mediant: If $a/c < b/d$ and $a, b, c, d \geq 0$, then

$$\frac{a}{c} < \frac{a+b}{c+d} < \frac{b}{d}.$$

This property follows from the two relations

$$\frac{a+b}{c+d}-\frac{a}{c}=\frac{bc-ad}{c(c+d)}=\frac{d}{c+d}\left(\frac{b}{d}-\frac{a}{c}\right)$$

and

$$\frac{b}{d}-\frac{a+b}{c+d}=\frac{bc-ad}{d(c+d)}=\frac{c}{c+d}\left(\frac{b}{d}-\frac{a}{c}\right).$$

- Assume that the pair of fractions *a*/*c* and *b*/*d* satisfies the determinant relation $bc-ad=1$. Then the mediant has the property that it is the *simplest* fraction in the interval (*a*/*c*, *b*/*d*), in the sense of being the fraction with the smallest denominator. More precisely, if the fraction a'/c'

Elementary Number Theory, Uspensky, Heaslet, Problem 2, Page 40.

■ The mediant of the fractions a/c and b/d, namely,

$$\frac{a+b}{c+d}$$

is irreducible if $|ad-bc|=1$.

Proof

Now we know that $\frac{a+b}{c+d}$ is expressed in simplest terms if and only if $\gcd(a+b,c+d)=1$.

But recall that, in general, the $\gcd(\alpha,\beta)$ is the least positive integer that is expressible as a integral linear combination of the integers α and β.

So it is sufficient to find integers m,n (positive or negative) such that

$$m(a+b)+n(c+d)=1.$$

Take $m=-c,n=a$. Then

$$\begin{gathered}|(-c)(a+b)+(a)(c+d)|\\=|-ac-bc+ac+ad|\\=|ad-bc|\\=1\ \text{ by hypothesis.}\end{gathered}$$

So, if

$$(-c)(a+b)+(a)(c+d)=1$$

then we are done. Otherwise

$$(-c)(a+b)+(a)(c+d)=-1$$

and

$$(c)(a+b)+(-a)(c+d)=1.$$

So in all cases we have found integers m,n such that $m(a+b)+n(c+d)=1$. Therefore, $\gcd(a+b,c+d)=1$ which implies

$$\frac{a+b}{c+d}$$

is irreducible.

■

https://artofproblemsolving.com/community/c4931_2005_india_national_olympiad
The Indian National Mathematical Olympiad (INMO) is a high school mathematics competition held annually in India since 1989.

2005 Indian National Mathematical Olympiad, Problem #2

Let α and β be positive integers such that $\frac{43}{197} < \frac{\alpha}{\beta} < \frac{17}{77}$. Find the minimum possible value of β.

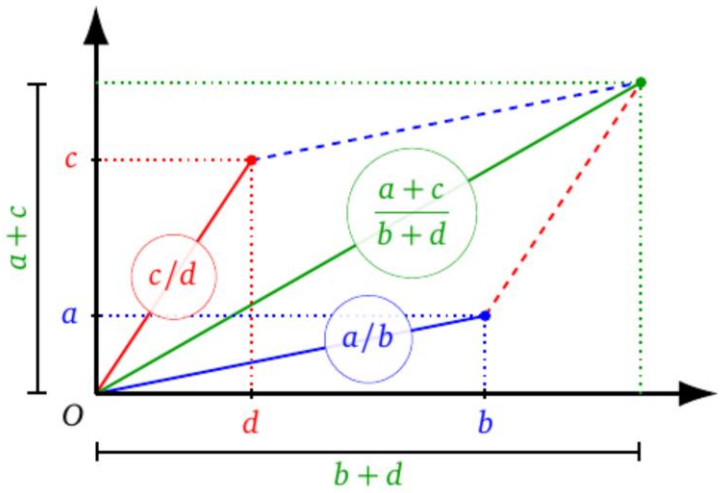
Solution
https://math.stackexchange.com/questions/4122009/fraction-with-the-smallest-entries

This can be done simply by a **binary search using Farey mediants**. The idea is as follows: given an interval $(a/b, c/d)$ containing our fractions we compare them to the mediant "midpoint" $m = (a + c)/(b + d)$. If they are both less then m then we replace the upper bound c/d by m. If the are both greater then m we replace the lower bound a/b by m. Else m lies between them, and by basic properties of Farey sequences it is the fraction with least denominator between them.

We start with the containing interval $(0/1, 1/0) = (0, \infty)$. Its mediant $(0+1)/(1+1) = 1/1$ exceeds both so our new upper bound is 1/1. The mediant of 0/1, 1/1 is 1/2 which still exceeds so 1/2 is our new upper bound. This continues till we reach upper bound 1/4 which then yields a mediant $(0+1)/(1+4) = 1/5$ which is smaller than both, so our new interval is (1/5, 1/4) Continuing this way yields the sequence below, till we reach 7/32 between them.

$$\frac{0}{1} < \frac{1}{5} < \frac{3}{14} < \frac{5}{23} < \frac{43}{197} < \frac{7}{32} < \frac{17}{77} < \frac{2}{9} < \frac{1}{4} < \frac{1}{3} < \frac{1}{2} < \frac{1}{1} < \frac{1}{0}$$

Remark Note that the mediant $\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$ can be viewed geometrically as the slope of the diagonal of a parallelogram with sides of slope a/b and c/d formed by the vectors (b, a) and (d, c), which makes its "inter*mediate*" property intuitively clear geometrically, i.e. the diagonal lies between the sides, as illustrated below.



■

https://math.stackexchange.com/questions/2494774/questions-concerning-smallest-fraction-between-two-given-fractions

Find the smallest positive integer n such that there exists an integer m satisfying

$$0.33000 = \frac{33}{100} < \frac{m}{n} < \frac{1}{3} = 0.33333333.$$

Solution

Notice that

$$\frac{33}{100} < \frac{1}{3} \text{ and } |33(3) - 100| = 1.$$

Therefore, the mediant

$$\frac{33+1}{100+3} = \frac{34}{103} = \frac{m}{n}.$$

■

If we started with the interval $\left(\frac{a}{b}, \frac{c}{d}\right)$ where $|ad - bc| \neq 1$ then we would have to go through an iterative process as demonstated below.

$$\frac{0}{1} < \frac{1}{0}$$
$$\frac{0}{1} < \frac{\mathbf{1}}{\mathbf{1}} < \frac{1}{0}$$
$$\frac{0}{1} < \frac{\mathbf{1}}{\mathbf{2}} < \frac{1}{1}$$
$$\frac{0}{1} < \frac{\mathbf{1}}{\mathbf{3}} < \frac{1}{2}$$

$$\frac{0}{1} < \mathbf{\frac{1}{4}} < \frac{1}{3}$$
$$\frac{1}{4} < \mathbf{\frac{2}{7}} < \frac{1}{3}$$
$$\frac{2}{7} < \mathbf{\frac{3}{10}} < \frac{1}{3}$$
$$\frac{3}{10} < \mathbf{\frac{4}{13}} < \frac{1}{3}$$
$$\frac{4}{13} < \mathbf{\frac{5}{16}} < \frac{1}{3}$$
$$\frac{5}{16} < \mathbf{\frac{6}{19}} < \frac{1}{3}$$
$$\frac{6}{19} < \mathbf{\frac{7}{22}} < \frac{1}{3}$$
Etc.

$$0.33 < \frac{m}{n} < \frac{1}{3} \implies (\frac{33}{100} < \frac{m}{n}) \wedge (\frac{m}{n} < \frac{1}{3})$$
$$\implies (33n < 100m) \wedge (3m < n)$$

and thus $n = 3m + 1$.

So

$$33n < 100m \implies 33(3m + 1) < 100m$$
$$\implies 99m + 33 < 100m$$
$$\implies m > 33$$

Taking $m \geq 34$, we find that $n = 34 \times 3 + 1 = 103$

If $c = 1$, then the smallest positive integer n such that there exists an integer m satisfying $\frac{a}{b} < \frac{m}{n} < \frac{1}{d}$ is given by

$$\left(\left\lfloor \frac{a}{b - da} \right\rfloor + 1 \right) d + 1$$

■

https://artofproblemsolving.com/wiki/index.php/2018_AMC_12B_Problems/Problem_17

2018 AMC 12B Problems/Problem 17

Let p and q be positive integers such that

$$\frac{5}{9} < \frac{p}{q} < \frac{4}{7}$$

and q is as small as possible. What is $q - p$?

(A) 7 **(B)** 11 **(C)** 13 **(D)** 17 **(E)** 19

Solution

Notice that $|5(7) - 9(4)| = 1$. Therefore, the mediant of $\frac{5}{9}$ and $\frac{4}{7}$ gives the answer.

$$\frac{p}{q} = \frac{5+4}{9+7} = \frac{9}{16}$$
$$q - p = 16 - 9 = 7.$$

■

Find the smallest positive integer n such that there exists an integer m satisfying

$$\frac{1}{3} < \frac{m}{n} < \frac{3}{4}.$$

Solution

First note that we are starting with an interval $\left(\frac{a}{b}, \frac{c}{d}\right)$ where $|ad - bc| = |1(4) - 3(3)| \neq 1$ so we have to engage in an iterative process as demonstated below.

Step 1. $\frac{0}{1} < \frac{1}{0}$ Start with $\left(\frac{0}{1}, \frac{1}{0}\right)$ and calculate the mediant $\frac{0+1}{1+0} = \mathbf{\frac{1}{1}}$.

Step 2. $\frac{0}{1} < \mathbf{\frac{1}{1}} < \frac{1}{0}$ $\frac{1}{3}$ and $\frac{3}{4}$ are both $< \frac{1}{1}$ so replace $\frac{1}{0}$ with $\frac{1}{1}$ and iterate.

Step 3. $\frac{0}{1} < \mathbf{\frac{1}{2}} < \frac{1}{1}$ $\frac{1}{3} < \frac{1}{2}$ and $\frac{3}{4} > \frac{1}{2}$. Stop. New mediant $\frac{1}{2}$ is the answer.

$$\frac{m}{n} = \frac{1}{2}.$$

■

13.4 Midy's Theorem

(**Midy's Theorem.**) The following was proved in 1837 by E. Midy (Dickson, 2005, p.163):

For a prime p, if the repetend of $1/p$ has $2n$ digits, then digit $(n + k) = 9 - digit\ (k)$

In 1769 Lambert noted that the number of the digits of the repetend of a repeating decimal, $1/a$, divides $a - 1$ for $a = 3$ or a prime greater than 5.

13.5 Counting Integer Solutions of $1/x + 1/y = 1/n$.

(Are these problems just examples of SFFT ?)

How many solutions are there to

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$$

where x, y and n are positive integers?

Solution

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$$
$$\frac{x+y}{xy}=\frac{1}{n}$$
$$xy-nx-ny=0$$
$$(x-n)(y-n)-n^2=0$$
$$(x-n)(y-n)=n^2$$

Let m be any divisor of n^2. Then

$$x-n=m, y-n=\frac{n^2}{m}$$

is a solution. Therefore

$$x=m+n, y=\frac{n^2}{m}+n$$

is a solution for every divisor m of n^2.

Suppose n^2 has r divisors including 1 and n^2. Then there will be r positive integral solutions to the above equation if we count (a, b) as distinct from (b, a) and there will be $(r+1)/2$ solutions otherwise.

■

For example, let $n=6$. How many positive integer solutions are there to

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{6}\ ?$$

Solution

Then the divisor of $n^2=6^2=2^2 3^2=36$ are

$$\{2^0 3^0, 2^0 3^1, 2^0 3^2, 2^1 3^0, 2^1 3^1, 2^1 3^2, 2^2 3^0, 2^2 3^1, 2^2 3^2\}$$
$$=\{1,3,9,2,6,18,4,12,36\}$$

$$x=m+n, y=\frac{n^2}{m}+n$$

$$(x,y)=\left(m+6,\frac{36}{m}+6\right),m\in\{1,3,9,2,6,18,4,12,36\}$$

$$(x,y)\in\{(7,42),(9,18),(15,10),(8,24),(12,12),(24,8),(10,15),(18,9),(42,7)\}$$

$$\frac{1}{7}+\frac{1}{42}=\frac{1}{6}$$
$$\frac{1}{9}+\frac{1}{18}=\frac{1}{6}$$
$$\frac{1}{15}+\frac{1}{10}=\frac{1}{6}$$
$$\frac{1}{8}+\frac{1}{24}=\frac{1}{6}$$
$$\frac{1}{12}+\frac{1}{12}=\frac{1}{6}$$
$$\frac{1}{24}+\frac{1}{8}=\frac{1}{6}$$
$$\frac{1}{10}+\frac{1}{15}=\frac{1}{6}$$
$$\frac{1}{18}+\frac{1}{9}=\frac{1}{6}$$
$$\frac{1}{42}+\frac{1}{7}=\frac{1}{6}.$$

A total of 9 solutions. If we don't want to count

$$\frac{1}{a}+\frac{1}{b}$$

as separate from

$$\frac{1}{b}+\frac{1}{a}$$

then there are 5 solutions.

■

Let p be a prime. What are the integer solutions (x,y) of $\frac{1}{x}+\frac{1}{y}=\frac{1}{p}$?

Solution

$$\frac{x+y}{xy}=\frac{1}{p}$$
$$xy-xp-yp=1$$
$$(x-p)(y-p)-p^2=1 \quad \text{(SFFT)}$$
$$(x-p)(y-p)=p^2$$
$$\big((x-p),(y-p)\big)\in\left\{(1,p^2),(p,p),(p^2,1)\right\}$$

$$(x, y) \in \{(1 + p, p^2 + p), (2p, 2p), (p^2 + p, 1 + p)\}$$

■

Mu Alpha Theta National Convention 2002, Number Theory Test, Alpha Division, Problem # 21

How many pairs of integers (m, n) satisfy the equation $\frac{1}{m} + \frac{1}{n} = \frac{1}{10}$?

Solution

21. **A** Rearranging yields $10(m+n) = mn$, or

$$(m-10)(n-10) = 100.$$

Since 100 has 9 divisors, there are 9 values $m-10$ can take on (with $n-10$ equal to $100/(m-10)$). Moreover, $m-10$ and $n-10$ could both be negative, yielding another 9 solutions. However, we must omit the solution $m = n = 0$ since that would give us $1/0+1/0 = 1/10$ as our initial problem. Thus, there are 17 solutions.

■

AMC 1993 Problem #19

How many ordered pairs (m, n) of positive integers are solutions to

$$\frac{4}{m} + \frac{2}{n} = 1?$$

(A) 1	(B) 2	(C) 3	(D) 4	(E) more than 4

Solution

■

13.5.1 Counting Integer Solutions of $1/x + 1/y + 1/z = 1/n$.

See *Indeterminate Equation*, Xing Zhou, Section 3.3, Page 21.

13.6 Perfect Squares

13.6.1 Properties of Perfect Squares

Properties of Perfect Squares (in Base 10)

1) The last digit is $0, 1, 4, 5, 6,$ or 9.

2) The digital root is always $1, 4, 7, 9$.
3) If the last digit is 6, then the penultimate digit must be odd.
4) If the last digit is not 6, then the penultimate digit is even.
5) If the last digit is 5, then the penultimate digit must be 2.
6) The last two digits cannot both be odd.
7) If the last digit is zero, it must also end in an even number of zeros.
8) Even square numbers have an even square root. Odd squares have an odd square root.
9) The remainder after dividing by 3 is either 1 or 0.
10) The remainder after dividing by 4 is either 1 or 0.
11) They always have an odd number of prime factors.

(wiki, Perfect Squares)
Proof of (3) and (4).
Every perfect square may be represented by $(10a + b)^2$ where a is a nonnegative integer and b is nonnegative integer less than 10.
Now $(10a + b)^2 = 100a + 20ab + b^2 = 2(10)(5a + ab) + b^2$. It follows that the tens digit of $(10a + b)^2$ is an odd number if and only if the tens digit of b^2 is an odd number.
But by checking all cases we see that the tens digit of $(10a + b)^2$ is an odd number only for $4^2 = 16$ and $6^2 = 36$.

$0^2 = 00$	$5^2 = 25$
$1^2 = 01$	$6^2 = 36$
$2^2 = 04$	$7^2 = 49$
$3^2 = 09$	$8^2 = 64$
$4^2 = 16$	$9^2 = 81$

And in both of these cases the units digit equals 6. Hence we can state that the tens digit of $(10a + b)^2$ is odd if and only if the units digit of $(10a + b)^2$ is 6.

■

Theorem
If p is a perfect square then pq is a perfect square if and only if q is a perfect square.
Proof

$$pq = n^2, p = k^2$$

$$p \mid pq \Leftrightarrow k^2 \mid n^2 \Leftrightarrow k \mid n \Leftrightarrow n = rk \text{ for some integer } r$$

$$q = \frac{pq}{p} = \frac{n^2}{k^2} = \frac{(rk)^2}{k^2} = r^2.$$

■

19. Let a and b be positive integers such that $(a, b) = 1$ and ab is a perfect square. Prove that a and b are perfect squares. Prove that the result generalizes to kth powers.

https://www.quora.com/The-number-8A3BC5-is-a-perfect-square-of-a-number-that-is-divisible-by-3-What-is-A-B-C-if-A-B-and-C-are-different-digits

The number $8A3BC5$ is a perfect square of a number that is divisible by 3. What is $A + B + C$ if A, B, and C are different digits?

Solution

From the list of properties of perfect squares we can immediately see that $C = 2$.

$$8A3B25 = (3 \cdot n)^2$$

So $8A3B25$ is divisible by 9. Therefore

$$8 + A + 3 + B + 2 + 5 = 18 + A + B$$

must be divisible by 9. Hence $A + B$ must be divisible by 9. This means $A + B = 0, A + B = 9$ or $A + B = 18$. But we can rule out $A + B = 0$ and $A + B = 18$ because this requires $A = B = 0$ or $A = B = 9$ and we are given that $A \neq B$.

So $A + B = 9$. And we already know that $C = 2$. Therefore, $A + B + C = 11$.

■

https://www.flyingcoloursmaths.co.uk/ask-uncle-colin-a-six-digit-square/

$ABCDEF$ is a six-digit perfect square (*i.e.* $A \neq 0$) in base ten such that $DEF = 8 \times ABC$, what is the sum of $A + B + C + D + E + F$?

Solution

$$\begin{aligned} ABCDEF &= 1000 \cdot ABC + DEF \\ &= 1000 \cdot ABC + 8 \cdot ABC \\ &= 1008 \cdot ABC \\ &= 2^4 \cdot 3^2 \cdot 7 \cdot ABC \end{aligned}$$

We are given that $ABCDEF$ is a perfect square which means that all prime factors occur to an even power. Therefore ABC must be a multiple of 7.

We note that if $A > 125$ then $8 \times ABC$ will be a four-digit number and hence cannot equal DEF. Furthermore $A \neq 0$. Therefore, $100 \leq ABC \leq 125$.

The multiples of 7 between 100 and 125 are $\{105,112,119\}$. That is, $ABC \in \{105,112,119\}$. Therefore,

$$ABCDEF = 1008 \cdot ABC \in \{105840, 112896, 119952\}.$$

We can use our list of properties of perfect squares to rule out 105840 and 119952. (A perfect square cannot end with an odd number of 0's and cannot end with a 2.)

Therefore, $ABCDEF = 112896$. (If a calculator was allowed on your test, you could directly verify that $112896 = 336^2$ is the only perfect square in this list of candidates.)

Hence,

$$A+B+C+D+E+F=1+1+2+8+9+6=27.$$

■

Saint Mary's College Mathematics Contest Problems

18. In what bases (less than or equal to 12) is 2101 a perfect square?

Solution

■

Saint Mary's College Mathematics Contest Problems

97. What is the smallest base in which 213 is odd and a perfect square?

Solution

■

AMC

62

22. The number 121_b, written in the integral base b, is the square of an integer for

(A) $b = 10$, only **(B)** $b = 10$ and $b = 5$, only **(C)** $2 \leq b \leq 10$
(D) $b > 2$ **(E)** no value of b

Solution

■

Find all positive integer n such that $n^2+4n+10$ is a perfect square, *i.e.* $n^2+4n+10=k^2$ for some positive integer k.

Solution

We know that $a^2 \equiv 0$ or $1 \pmod 4$ for all integer a. Therefore, $k^2 \equiv 0$ or $1 \pmod 4$. But

$$k^2=n^2+4n+10=(n+2)^2+6$$

and

$$(n+2)^2 \equiv 0 \text{ or } 1 \pmod 4.$$

Therefore,

$$k^2=(n+2)^2+6 \equiv 0+6 \text{ or } 1+6 \pmod 4$$

$$\equiv 2 \text{ or } 3 \pmod 4$$

which is a contradiction. Hence there are no values of n where $n^2 + 4n + 10$ is a perfect square.

■

Find all positive integer n such that $n^2 + n + 109$ is a perfect square, *i.e.* $n^2 + n + 109 = k^2$ for some positive integer k.

Solution

$$ax^2 + bx + c = a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a} + c$$

$$n^2 + n + 109 = \left(n + \frac{1}{2}\right)^2 - \frac{1}{4} + 109$$

$$= \frac{(2n+1)^2}{4} + \frac{4(109) - 1}{4}$$

$$= \frac{(2n+1)^2 + 435}{4}$$

So

$$4k^2 = (2n+1)^2 + 435$$

$$4k^2 - (2n+1)^2 = 435$$
$$(2k - 2n - 1)(2k + 2n + 1) = 435$$

Now $435 = 3 \cdot 5 \cdot 29$. So, we have the following possible cases to solve for (k, n).

$$2k - 2n - 1 = 1, 2k + 2n + 1 = 435$$
$$2k - 2n - 1 = 3, 2k + 2n + 1 = 145$$
$$2k - 2n - 1 = 29, 2k + 2n + 1 = 15$$
$$2k - 2n - 1 = 15, 2k + 2n + 1 = 29$$
$$2k - 2n - 1 = 87, 2k + 2n + 1 = 5$$
$$2k - 2n - 1 = 145, 2k + 2n + 1 = 3$$
$$2k - 2n - 1 = 435, 2k + 2n + 1 = 1$$

$$2k = 2n + 1 + 1, (2n + 2) + 2n + 1 = 435$$
$$4n + 3 = 435, n = 108, k = 218$$

$$4k^2 (\text{mod } 4) \equiv 0 (\text{mod } 4)$$
$$435 \pmod 4 \equiv 3 (\text{mod } 4)$$

Therefore, we need

$$(2n+1)^2 \equiv 1 (\text{mod } 4)$$

which implies that

$$2n+1 \equiv 1 (\text{mod } 4) \text{ or } 2n+1 \equiv 3 (\text{mod } 4)$$
$$2n \equiv 0 (\text{mod } 4) \text{ or } 2n \equiv 2 (\text{mod } 4)$$
$$n \equiv 0 (\text{mod } 4) \text{ or } n \equiv 1 (\text{mod } 4)$$

$$0^2 \equiv 0 (\text{mod } 4)$$
$$1^2 \equiv 1 (\text{mod } 4)$$
$$2^2 \equiv 0 (\text{mod } 4)$$
$$3^2 \equiv 1 (\text{mod } 4)$$

AMC 1965

40. Let n be the number of integer values of x such that

$$P = x^4 + 6x^3 + 11x^2 + 3x + 31$$

is the square of an integer. Then n is:

(A) 4 (B) 3 (C) 2 (D) 1 (E) 0

Solution

Let $$P = x^4 + 6x^3 + 11x^2 + 3x + 31$$
$$= (x^2 + 3x + 1)^2 - 3(x - 10) = y^2.$$

When $x = 10$, $P = (x^2 + 3x + 1)^2 = 131^2 = y^2$. To prove that 10 is the only possible value we use the following lemma: If

$$| N | > | M |,$$

N, M integers, then

$$N^2 - M^2 \geq 2 | N | - 1.$$

(This lemma is easy to prove; try it.)

Case I If $x > 10$, then

$$3(x - 10) = (x^2 + 3x + 1)^2 - y^2 \geq 2 | x^2 + 3x + 1 | - 1,$$

an impossibility.

Case II If $x < 10$, then

$$3(10 - x) = y^2 - (x^2 + 3x + 1)^2$$
$$\geq 2 | y | - 1 > 2 | x^2 + 3x + 1 | - 1.$$

This inequality holds for the integers

$$x = 2, 1, 0, -1, -2, -3, -4, -5, -6,$$

but none of these values makes P the square of an integer.

$$x^4 + 6x^3 + 11x^2 + 3x + 31 = (ax^2 + bx + c)^2 + lower\ terms\ rem$$
$$= a^2x^4 + 2abx^3 + (2ac + b^2)x^2 + 2bcx + c^2 + lower\ terms\ rem$$
$$a = 1, b = 3, c = 1$$
$$(x^2 + 3x + 1)^2 + 6x + 1 + ???$$

Not sure where I am heading with this!

■

435

Writing as a square:

In this method take the desired quantity and write it as the square of some number, perhaps involving some or all of the original expression. Then see what makes sense.

In this problem from the 2002 NC State Math Contest, we are asked to find the four values for which $n^2+n+109$ is a perfect square.

$n^2+n+109=(n+k)^2=n^2+2nk+k^2$

$\Rightarrow n+109=2nk+k^2 \Rightarrow n(1-2k)=k^2-109$ Now check values of k from 1 through 10.

$\Rightarrow n=\dfrac{109-k^2}{2k-1}$

$$\frac{109-k^2}{2k-1}=-\left(\frac{k^2-109}{2k-1}\right)=-\left(\frac{2k+1}{4}-\frac{435}{4(2k-1)}\right)$$

$$435=3*5*29$$

$$\left[\frac{2x+1}{4}, -\frac{435}{4}\right]$$

■

Perfect Squares notes by John Goebel

6. For what positive integer values of n is $n^2-19n+99$ a perfect square? **AIME 1999**

If $n^2-19n+99=(n-k)^2=n^2-2nk+k^2 \Rightarrow -19n+99=2nk+k^2 \Rightarrow$ $k^2-99=n(2k-19) \Rightarrow n=\dfrac{k^2-99}{2k-19}=\dfrac{2k+19}{4}-\dfrac{35}{4(2k-19)}$. $2k-19$ must then divide 35, giving $k=-8,6,7,9,10,12,13,27$ and $n=1,9,10,18$

Perfect Squares notes by John Goebel

7. For how many positive integers n is $n^2-2004n$ a perfect square?

If, $n^2 - 2004n = m^2$, then $n^2 - m^2 = (n+m)(n-m) = 2004n$ is even, so $n-m$ is even. If $n^2 - 2004n = (n-2k)^2 = n^2 - 4nk + 4k^2 \Rightarrow n(4k-2004) = 4k^2$

$n = \dfrac{k^2}{k-501} = k + 501 + \dfrac{251001}{k-501}$. $251001 = 3^2 \cdot 167^2$, so for integer n, $k = -250500, -83166, -27388, -10020, 334, 492, 498, 500, 502, 504, 510, 668, 1002, 2004, 28390, 84168, 251502$. For the first nine k's, this produces non-positive n, for the other nine k's, $n = 252004, 84672, 28900, 2672, 2004, 2672, 28900, 84672, 252004$, respectively, giving 5 distinct n.

(1T075)

5. K is a positive two digit number. When its digits are reversed to form the two digit number L, $L \neq K$, then $K^2 - L^2$ is a perfect square? What is that perfect square?

Solution

Let $K = 10m + n$; then $L = 10n + m$

$K^2 - L^2 = 100m^2 + 20mn + n^2$

$\quad - (100n^2 + 20mn + m^2)$

$= 99(m^2 - n^2) = 9 \cdot 11 (m+n)(m-n)$

Clearly either $m+n$ or $m-n$ must be 11, but $m-n$ won't work, $m+n = 11$

Also, since $m-n > 0$, $m > n$; and $m-n$ will have to be a perfect square. Consider the possibilities

m	n	m − n
9	2	7
8	3	5
7	4	3
6	5	1 ← The only square

[MML March 2006]

$m = 6$; $n = 5$

The perfect square $= 9 \cdot 11 \cdot 11 = 1089$

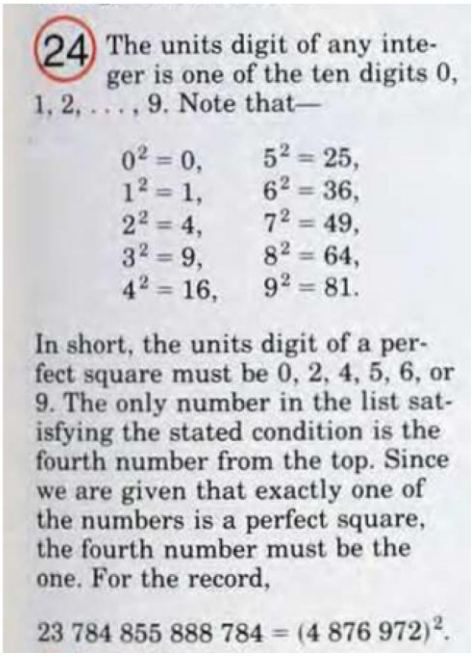
■

Mathematics Teacher, Calendar Problem Number 24, October 1990

24 Exactly one of the following six numbers is a perfect square; can you determine which one?

64 844 231 096 378
75 406 651 906 592
55 432 988 756 447
23 784 855 888 784
19 830 005 200 433
66 971 114 742 058

Solution



24 The units digit of any integer is one of the ten digits 0, 1, 2, . . . , 9. Note that—

$0^2 = 0$, $5^2 = 25$,
$1^2 = 1$, $6^2 = 36$,
$2^2 = 4$, $7^2 = 49$,
$3^2 = 9$, $8^2 = 64$,
$4^2 = 16$, $9^2 = 81$.

In short, the units digit of a perfect square must be 0, 2, 4, 5, 6, or 9. The only number in the list satisfying the stated condition is the fourth number from the top. Since we are given that exactly one of the numbers is a perfect square, the fourth number must be the one. For the record,

$23\,784\,855\,888\,784 = (4\,876\,972)^2$.

■

***The Pentagon*, Volume 15, Number 2, Spring 1956, Problem Corner, Problem #90, page 106**

A merchant buys an odd number of felt hats at $\$10$ each and one cloth hat for a whole number of dollars less than $\$10$. How much does the cloth hat cost if the total amount of money involved is a perfect square?

Solution

Let n be the number of felt hats the merchant buys and let m be the cost of a cloth hat. From the information given we know that

$$10n + m = r^2$$

where n is odd, $m \in \{1,2, \ldots ,9\}$ and r is a positive integer. The tens digit of $10n + m$ does not depend on m and the tens digit of $10n$ is odd because n is odd.

This means that the tens digit of r^2 is odd. But we have shown above that the tens digit of r^2 is odd if and only if the units digit of r^2 equals 6.

That is, if and only if $m = 6$.

■

Mu Alpha Theta National Convention 2004, Number Theory Test, Mu Division, Problem #11

11. Which of the following is the list of possible units digit of a perfect square that ends with 4 identical digits?

A. 0 only B. 0 or 4 only C. 0, 1, or 4 only D. 0, 1, 4, or 6 only E. NOTA

Solution

11. **A** All but 0 and 4 are easily dismissed by noting that only 00 or 44 could be repeated last 2 digits. An ending of 4444 can be dismissed by noting that any such number is of the form 16k+12, which cannot be a perfect square.

■

ARML 1995 #I-3

Find all primes p such that $p^{1994} + p^{1995}$ is a perfect square.

Solution

$$p^{1994} + p^{1995} = p^{1994}(p+1)$$

p^{1994} is a perfect square therefore $p^{1994} + p^{1995}$ is a perfect square if and only if $p+1$ is a perfect square.

Let $p+1 = k^2$. Then $p = k^2 - 1 = (k-1)(k+1)$. But p is prime, therefore $k-1 = 1$ and $k = 2$. Hence $p = 3$. That is, $p = 3$ is the only prime such that $p^{1994} + p^{1995}$ is a perfect square.

Note: The same argument shows that $p^{2n} + p^{2n+1}$ is a perfect square for prime p if and only if $p = 3$.

■

Find all (m, n, x) positive integer triples satisfying the equation

$$2^m + 3^n = x^2.$$

Solution

Let (m, n, x) be such a triple. Then $(2^m + 3^n) \equiv x^2 \bmod 3$.

We can see that 3 divides 3^n but 3 does not divide 2^m. Therefore,

$3^n \equiv 0 \bmod 3$ and $2^m \not\equiv 0 \bmod 3$	
	$\Longrightarrow (2^m \bmod 3) + (3^n \bmod 3) \not\equiv 0 \bmod 3$
	$\Longrightarrow (2^m + 3^n) \not\equiv 0 \bmod 3$
	$\Longrightarrow x^2 \not\equiv 0 \bmod 3$

Now the square of an integer is never equivalent to 2 mod 3 (as the following simple argument shows).

$$(3k)^2 \bmod 3 \equiv 0$$

$$(3k+1)^2 \bmod 3 \equiv (9k^2 + 6k + 1) \bmod 3$$

$$\equiv \Big(3(3k^2 + 2k)\Big) \bmod 3 + 1 \bmod 3 \equiv 1 \bmod 3$$

$$(3k+2)^2 \bmod 3 \equiv (9k^2 + 12k + 4) \bmod 3$$

$$\equiv \Big(3(3k^2 + 2k + 1)\Big) \bmod 3 + 1 \bmod 3 \equiv 1 \bmod 3$$

Therefore, it must be that $x^2 \equiv 1 \bmod 3$. But $3^n \equiv 0 \bmod 3$ tells us that $2^m \equiv x^2 \bmod 3$. Therefore, we can conclude that

$$2^m \equiv 1 \bmod 3.$$

But

$$2^m \equiv 1 \bmod 3 \iff m \text{ is even}$$

as the following simple argument will show.

$$2^{2k} \bmod 3 \equiv (2^2)^k \bmod 3 \equiv 4^k \bmod 3$$

$$4^k \bmod 3 \equiv (4 \bmod 3)^k \bmod 3 \equiv 1^k \bmod 3 \equiv 1 \bmod 3$$

$$2^{2k+1} \bmod 3 \equiv (2^2)^k \cdot 2 \bmod 3 \equiv 4^k \cdot 2 \bmod 3$$

$$4^k \cdot 2 \bmod 3 \equiv (4 \bmod 3)^k \bmod 3 \cdot 2 \bmod 3$$

$$\equiv \Big((1^k \bmod 3) \cdot (2 \bmod 3)\Big) \bmod 3$$

$$\Big((1^k \bmod 3) \cdot (2 \bmod 3)\Big) \bmod 3 \equiv (1 \cdot 2) \bmod 3 \equiv 2 \bmod 3$$

Now consider the equation $2^m + 3^n = x^2$ modulo 4. Then $(2^m + 3^n) \equiv x^2 \bmod 4$.

Because m is (by assumption) greater than or equal to 1 and because we have just shown that m is even, we can now conclude that $m \geq 2$.

Therefore, $2^m \equiv 0 \bmod 4$. But clearly 4 does not divide 3^n so $3^n \not\equiv 0 \bmod 4$. Therefore, it has to also be true that $x^2 \not\equiv 0 \bmod 4$.

However the square of an integer is never equivalent to 2 or $3 \bmod 4$ (as the following simple argument shows).

$$(4k)^2 \bmod 4 \equiv 0$$

$$(4k+1)^2 \bmod 4 \equiv \Big(4(4k^2+2k)+1\Big) \bmod 4 \equiv 1 \bmod 4$$

$$(4k+2)^2 \bmod 4 \equiv \Big(4(4k^2+4k+1)\Big) \bmod 4 \equiv 0 \bmod 4$$

$$(4k+3)^2 \bmod 4 \equiv \Big(4(4k^2+2k+2)+1\Big) \bmod 4 \equiv 1 \bmod 4$$

Therefore, it must be that $x^2 \equiv 1 \bmod 4$. But $2^m \equiv 0 \bmod 4$ tells us that $3^n \equiv x^2 \bmod 4$. Therefore, we can conclude that

$$3^n \equiv 1 \bmod 4.$$

But

$$3^n \equiv 1 \bmod 4 \iff n \text{ is even}$$

as the following simple argument will show.

$$3^{2k} \bmod 4 \equiv (3^2)^k \bmod 4 \equiv 9^k \bmod 4$$

$$9^k \bmod 4 \equiv (9 \bmod 4)^k \bmod 4 \equiv 1^k \bmod 4 \equiv 1 \bmod 4$$

$$3^{2k+1} \bmod 4 \equiv (3^2)^k \cdot 3 \bmod 4 \equiv 9^k \cdot 3 \bmod 4$$

$$9^k \cdot 3 \bmod 4 \equiv (9 \bmod 4)^k \bmod 4 \cdot 3 \bmod 4$$

$$\equiv \Big((1^k \bmod 4) \cdot (3 \bmod 4)\Big) \bmod 4$$

$$\Big((1^k \bmod 4) \cdot (3 \bmod 4)\Big) \bmod 4 \equiv (1 \cdot 3) \bmod 4 \equiv 3 \bmod 4$$

So now we know that m and n are both even. This means that 2^m and 3^n are perfect squares.

$$2^m + 3^n = x^2.$$

This means that $2^{m/2}$ and $3^{n/2}$ are positive integers. It follows that

$$2^m + 3^n = \left(2^{m/2}\right)^2 + \left(3^{n/2}\right)^2 = x^2$$

where $2^{m/2}$ and $3^{n/2}$ are positive integers.

That is, $\left(2^{m/2}, 3^{n/2}, x\right)$ is a Pythagorean triple! Is a primitive Pythagorean triple? Yes.

We note that $2^{m/2}$ only has factors of 2 and $3^{n/2}$ only has factors of 3. [Don't forget that we have just shown that $m/2$ and $n/2$ are integers.]

Therefore, $\gcd\left(2^{m/2}, 3^{n/2}\right) = 1$. But this tells us that $\gcd\left(2^{m/2}, 3^{n/2}, x\right) = 1$. [Show this.]

Therefore, $\left(2^{m/2}, 3^{n/2}, x\right)$ is a primitive Pythagorean triple.

■

The USSR Olympiad Problem Book: Selected Problems and Theorems of Elementary Mathematics, Shklarsky, Chentzov, Yaglom

Problem 110(a)

Find a four-digit number which is an exact square and such that its first two digits are the same and its last two digits are the same.

Solution

110. (a) Let a be the first digit, and b the last digit, of the desired integer N. Then the integer can be written as

$$N = 1000a + 100a + 10b + b\,,$$

or as

$$N = 1100a + 11b = 11(100a + b)$$

Since this integer is to be a perfect square, and since it clearly must be divisible by 11, it must also be divisible by 121; that is, $\frac{N}{11} = 100a + b$ must be divisible by 11. But

$$100a + b = 99a + (a + b) = 11 \cdot 9a + (a + b)$$

Hence $a + b$ must be divisible by 11. Since neither a nor b exceeds 9, and since a is not 0, it follows that $1 \leqq a + b \leqq 18$, whence $a + b = 11$.

This implies that

$$100a + b = 11 \cdot 9a + 11 = 11(9a + 1)\,,$$

$$\frac{N}{121} = \frac{100a + b}{11} = 9a + 1$$

Since N is a perfect square, $\frac{N}{121}$ is also a square. But among the integers of form $9a + 1$, where a ranges through the integer values 1 to 9, only $9 \cdot 7 + 1 = 64$ is a perfect square. This means that $N = 121 \cdot 64 = 7744 = 88^2$.

■

13.7 Repunits

For the repunits R_n, where $R_n = (10^n - 1)/9$, verify the assertion.

If $\gcd(n, m) = 1$, then $\gcd(R_n, R_m) = 1$.

HINT: Assume that $m < n$; then $R_n - 10^{n-m}R_m = R_{n-m}$, so

$$R_n = \underbrace{11\cdots11}_{n \text{ ones}} = \frac{10^n - 1}{9}$$

Suppose $m < n$. Then

$$\underbrace{11\cdots11}_{n \text{ ones}} - \underbrace{11\cdots11}_{m \text{ ones}}\underbrace{00\cdots00}_{n-m \text{ ones}} = \underbrace{11\cdots11}_{n-m \text{ ones}}.$$

That is,

$$R_n - 10^{n-m}R_m = R_{n-m}.$$

Suppose $a - kb > 0$. Then

$$\gcd(a, b) = \gcd(a - kb, b)$$

Proof

If $r|b$ then $r|kb$.

If $r|a$ and $r|kb$ then $r|(a - kb)$.

If $r|(a - kb)$ and $r|b$ then $r|\big((a - kb) + kb\big)$.

So $r|a$ and $r|b$ if and only if $r|(a - kb)$ and $r|b$. Therefore $\gcd(a, b) = \gcd(a - kb, b)$.

$$\begin{aligned}\gcd(R_n, R_m) &= \gcd(R_n - 10^{n-m}R_m, R_m)\\ &= \gcd(R_n, R_{n-m})\end{aligned}$$

$$\begin{aligned}\gcd(52,14) &= \gcd(52 - 14,14) = \gcd(38,14) = \gcd(24,14) = \gcd(10,14)\\ &= \gcd(14,10) = \gcd(4,10) = \gcd(10,4) = \gcd(6,4) = \gcd(2,4)\\ &= \gcd(4,2) = \gcd(2,2) = 2\end{aligned}$$

$$\begin{aligned}\gcd(R_{52}, R_{14}) &= \gcd(R_{38}, R_{14}) = \gcd(R_{24}, R_{14}) = \gcd(R_{10}, R_{14})\\ &= \gcd(R_{14}, R_{10}) = \gcd(R_4, R_{10}) = \gcd(R_{10}, R_4) = \gcd(R_6, R_4)\\ &= \gcd(R_2, R_4) = \gcd(R_4, R_2) = \gcd(R_2, R_2) = R_2 = R_{\gcd(52,14)}\end{aligned}$$

$$\begin{aligned}\gcd(52,15) &= \gcd(52 - 15,15) = \gcd(37,15) = \gcd(22,15) = \gcd(15,7)\\ &= \gcd(8,7) = \gcd(1,7) = 1\end{aligned}$$

$$\begin{aligned}\gcd(R_{52}, R_{15}) &= \gcd(R_{37}, R_{15}) = \gcd(R_{22}, R_{15}) = \gcd(R_{15}, R_7)\\ &= \gcd(R_8, R_7) = \gcd(R_1, R_7) = \gcd(1, R_7) = 1 = R_{\gcd(52,15)}\end{aligned}$$

$$r_n = \underbrace{11\cdots11}_{n \text{ ones}}$$

Suppose $n = km$. Then

$$10^n - 1 = (10^m - 1)\left(10^{(k-1)m} + 10^{(k-2)m} + \cdots + 10^m + 1\right)$$

$$10^{km} + 10^{(k-1)m} + \cdots + 10^{2m} + 10^m - 10^{(k-1)m} - 10^{(k-2)m} - \cdots - 10^m - 1$$
$$= 10^{km} = 10^n$$

Conclusion

If $m|n$ then $R_m|R_n$.

■

If $d|R_n$ and $d|R_m$, then $d|R_{n+m}$

Proof

$$R_n - 10^{n-m}R_m = R_{n-m}.$$

Therefore,

$$R_{n+m} - 10^{(n+m)-m}R_m = R_{(n+m)-m}$$
$$R_{n+m} = 10^m R_m + R_n$$

Therefore, if $d|R_n$ and $d|R_m$, then $d|R_{n+m}$

■

Repdigit

Example (Source: Mu Alpha Theta 2001 National Convention, Mu Division, Number Theory Topic Test, Problem 30)

A number N expressed in base $(A+1)$ is $AAAA$. If $N = Q(Q-2)$, what is Q expressed in base $(A+1)$?

Solution

$$N = (AAAA)_{A+1} = A \cdot (A+1)^3 + A \cdot (A+1)^2 + A \cdot (A+1)^1 + A$$

$$(AA00)$$

$$(A+1)^2(A(A+1)+A) + (A(A+1)+A)$$

$$((A+1)^2 + 1)(A(A+1)+A)$$

$$(1(A+1)^2 + 0(A+1)^1 + 1(A+1)^0)(A(A+1)^1 + A(A+1)^0)$$

$$(101)_{A+1}(AA)_{A+1}$$

30. Notice that AAAA can be factored into (AA)(101). Also, AA + 2 = 101. Q is thus 101.

Question 7. [p 194. #11]

A *repunit* is an integer with decimal expansion containing all 1's.

Determine which repunits are divisible by 3; and which are divisible by 9.

SOLUTION: If

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0,$$

then

$$n \equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \pmod 3$$

and

$$n \equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \pmod 9.$$

So a repunit is divisible by 3 if and only if the number of decimal digits is a multiple of 3, and a repunit is divisible by 9 if and only if the number of decimal digits is a multiple of 9.

Question 8. [p 194. #12]

Determine which repunits are divisible by 11.

SOLUTION: Again, since

$$\begin{aligned} n &= a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv (-1)^k a_k + \cdots - a_1 + a_0 \pmod{11}, \end{aligned}$$

and for a repunit $a_0 = a_1 = \cdots = a_k = 1$, then any repunit with an even number of decimal digits is divisible by 11.

https://math.stackexchange.com/questions/881503/length-of-smallest-repunits-divisible-by-primes

I want to prove this statement from Wikipedia:

> It was found very early on that for any prime p greater than 5, the period of the decimal expansion of 1/p is equal to the length of the smallest repunit number that is divisible by p.

Thanks Erick Wong, I understand it now. So we need $p|10^k - 1$, so

$$\frac{10^k - 1}{p} = \frac{10^k}{p} - \frac{1}{p} = n$$

So we need the fractional parts of $\frac{10^k}{p}$ and $\frac{1}{p}$ to be equal: that will happen for the first time if $k = \text{period}_{\frac{1}{p}}$: For example,

$$\frac{1}{13} = 0.(076923), 10^6 \cdot \frac{1}{13} = 76923.(076923)$$

And the difference is 76923

The repunits are 1, 11, 111, 1111, ... the next repunit to **x** will always be x*10+1. If the remainder left by **x** repunit is **r** then remainder left by the next repunit will always be **(r*10+1)%n.** Since the repunit can be very large, there is no need to find the repunit number. Simply counting the number of ones will give us the answer.
So, find out the remainders of all repunit numbers until the remainder becomes 0. Once it does, then the count of iterations done to make remainder 0 will be the number of 1's.

Find the number of digits in the smallest repunit divisible by 19.
https://math.stackexchange.com/questions/3824172/finding-the-number-of-digits-in-repunit

https://mathlesstraveled.com/2011/11/17/fun-with-repunit-divisors-more-solutions/

My previous post explained two different proofs. At the end of "Fun with repunit divisors" I also posed a series of follow-up challenges; here are solutions to those.

1. *Compute a repunit which is divisible by 2011 (you'll probably want to use a computer!).*
   As we now know from the second proof (using Fermat's Little Theorem), the repunit with 2010 ones must be divisible by 2011. So I guess a computer is not really necessary after all! However, what if we want to compute the *smallest* repunit which is divisible by 2011? In that case we can compute $1 \bmod 2011, 11 \bmod 2011, 111 \bmod 2011, \dots$ until we get zero. However, we don't have to actually compute a bigger and bigger repunit each time! Each repunit is related to the previous one by an application of the function $f(x) = 10x + 1$. So it suffices to keep only the *remainder* $(\bmod 2011)$ at each step, and apply $f(x) = 10x + 1$ to each remainder to get the next (reducing $(\bmod 2011)$ when needed). For example, we start out by computing $1, 11, 111, 1111$, but at the next step we can reduce $11111 \bmod 2011$ to get 1056. Then we compute $(1056 \cdot 10 + 1) \bmod 2011 = 10561 \bmod 2011 = 506$, then $5061 \bmod 2011 = 1039$, and so on. Iterating this process on a computer is very fast, and in a fraction of a second we find that $(10^{670} - 1)/9$ is the smallest repunit divisible by 2011. For example, I computed this using Haskell by defining

Question

(a) Let $p > 5$ be prime. If R_n is the smallest repunit for which $p|R_n$, establish that $n|p-1$. For example, R_8 is the smallest repunit divisible by 73, and $8|72$. [Hint: The order of 10 modulo p is n.] (b) Find the smallest R_n divisible by 13.

Explanation Verified

- [a)]Let $p > 5$ be prime. Let R_n be the smallest repunit for which $p \mid R_n$. Recall that a repunit is of the form

$$R_n = \underbrace{11\dots11}_{n \text{ times}} \frac{10^n - 1}{10 - 1} = \frac{10^n - 1}{9}$$

Each digit in the n-digit number N is 1. What is the smallest value of n for which N is divisible by 333,333?

Since $N = 11\ldots11$ (with n ones) is divisible by 333333, we can write $N = 11\ldots11 = 333333 \cdot k$ for some integer k.

Multiply both sides by 9 to get: $9N = 99\ldots99 = 9 \cdot 333333 \cdot k$.

Now, notice that $99\ldots99$ (with n nines) is one less than 10^n. Thus, $99\ldots99 = 10^n - 1$.

Also, we can factor $9 \cdot 333333 = 3 \cdot 999999 = 3(10^6 - 1)$

Therefore, we want to find positive integers n, k such that $10^n - 1 = 3(10^6 - 1)k$.

By Fermat's Little Theorem, $10^6 \equiv 1 \pmod 7$, thus, $10^6 - 1$ is divisible by 7. So, $10^n - 1$ must also be divisible by 7, i.e. $10^n \equiv 1 \pmod 7$.

Looking at powers of ten $\pmod 7$, we see that:
$10^0 \equiv 1,\ 10^1 \equiv 3,\ 10^2 \equiv 2,\ 10^3 \equiv 6,\ 10^4 \equiv 4,\ 10^5 \equiv 5,\ 10^6 \equiv 1.$

Since the cycle repeats every 6 powers of ten, $10^n \equiv 1 \pmod 7$ iff n is a multiple of 6.

Now we try $n = 6, 12, 18, \ldots$:

$n = 6$: $3(10^6 - 1)k = 10^6 - 1$, so $3k = 1$, i.e. $k = 0.33\ldots$ (not an integer)

$n = 12$: $3(10^6 - 1)k = 10^{12} - 1 = (10^6 - 1)(10^6 + 1)$, so $3k = 10^6 + 1$, so $k = 333333.66\ldots$ (not an integer)

$n = 18$: $3(10^6 - 1)k = 10^{12} - 1 = (10^6 - 1)(10^{12} + 10^6 + 1)$, so $3k = 10^{12} + 10^6 + 1 = 1000001000001$, which is divisible by 3.

Hence, the smallest value of n that meets the criteria is $n = 18$.

THE 26th ANNUAL (2004) UNIVERSITY OF MARYLAND
HIGH SCHOOL MATHEMATICS COMPETITION
PART I MULTIPLE CHOICE

25. Let $m = 1111\cdots111$ (2004 ones) and $n = 1111\cdots111$ (666 ones). The greatest common divisor of m and n is
a. 111 b. 333 c. 111111 (6 ones) d. 333333 e. 111111111111 (12 ones)

Solution

Let d be the greatest common divisor. Then d is a divisor of $m-10^{2004-666}n-10^{2004-2\cdot 666}n-10^6 n = 111111$. Since 111111 is a divisor of m and n, we have $d = 111111$. The answer is $\mathbf{(c)}$.

■

Alberta High School Mathematics Competition
First Round, 2007

1. The positive integer A has 1001 digits all of which are 1's. That is, $A = \overbrace{11\cdots 11}^{1001\text{ 1's}}$. Find $A \bmod(1001)$.

Solution

We can expand A as follows:

$$\begin{aligned}\overbrace{11\cdots 11}^{1001\text{ 1's}} &= 10^{1000} + 10^{999} + 10^{998} + \cdots + 10^3 + 10^2 + 10^1 + 10^0 \\ &= (10^{1000} + 10^{997}) + (10^{999} + 10^{996}) + \cdots + (10^4 + 10^1) + (10^3 + 10^0) + 10^2 \\ &= 10^{997}(1001) + 10^{996}(1001) + \cdots + 10^1(1001) + 10^0(1001) + 10^2.\end{aligned}$$

From here we can immediately see that $A \bmod(1001) = 10^2 = 100$.

Alternatively, we could expand A as

$$\begin{aligned}A &= \overbrace{111111}^{\text{six 1's}}\overbrace{0\cdots 0}^{995\text{ 0's}} + \overbrace{111111}^{\text{six 1's}}\overbrace{0\cdots 0}^{989\text{ 0's}} + \cdots + \overbrace{111111}^{\text{six 1's}}\overbrace{0\cdots 0}^{11\text{ 0's}} + \overbrace{111111}^{\text{six 1's}}\overbrace{0\cdots 0}^{5\text{ 0's}} + \overbrace{11111}^{5\text{ 1's}} \\ &= \left(\overbrace{111111}^{\text{six 1's}}\right)\cdot(10^{995} + 10^{989} + \cdots + 10^{11} + 10^6) + \left(\overbrace{11111}^{\text{five 1's}}\right) \\ &= \left(1001\cdot 111\right)\cdot(10^{995} + 10^{989} + \cdots + 10^{11} + 10^6) + \left(1001\cdot 11 + 100\right)\end{aligned}$$

from which it is again immediate that $A \bmod(1001) = 100$.

■

13.8 Need to Generalize

Saint Mary's College Mathematics Contest Problems

117. How many ways could one make \$2.43 with 5¢ and 8¢ stamps?

Solution

■

13.9 Else

(5T895) Two seventh grade students were allowed to enter a chess tournament otherwise comprised of eighth-graders. Each contestant played one match against every other contestant. In this tournament, a contestant received 1 point for a win, 0 for a loss, and in the case of a tie, each contestant received $1/2$ point. The two seventh grade students amassed a total of 8 points, and each eighth-grader scored the same number of points. What is the largest number of eighth-graders that might have participated? [This is not an original problem, but the source is lost.]

Solution

With this setup we can see that the total number of games played equals the sum of the points earned by all the contestants.

Let n be the number of eighth grade contestants and let p equal the number of points scored by each eighth grader.

Then, the total number of contestants equals $n+2$ and the total number of games played equals $\binom{n+2}{2}$, as each contestant plays one match against every other contestant . And as noted above, this implies the sum of the points earned by all the contestants also equals $\binom{n+2}{2}$.

But we also know that the sum of the points earned by all the contestants equals $np+8$.

Therefore, we have

$$np+8=\binom{n+2}{2}=\frac{(n+2)!}{2!\,n!}=\frac{(n+2)(n+1)}{2}.$$

This gives us a quadratic equation in the variable n.

$$2np+16=(n+2)(n+1)$$

or

$$n^2+(3-2p)n-14=0.$$

We know that n is an integer and we know that the only possible integer solutions of this quadratic are the factors of 14. That is, $n\in\{1,2,7,14\}$.

Now consider the value of p for each possible value of n. Note that on solving for p in the above quadratic equation we have

$$p=\frac{n^2+3n-14}{2n}.$$

Therefore,

$$n=1\Rightarrow p=\frac{1^2+3(1)-14}{2(1)}=-5$$

$$n = 2 \Longrightarrow p = \frac{2^2 + 3(2) - 14}{2(2)} = -1$$

$$n = 7 \Longrightarrow p = \frac{7^2 + 3(7) - 14}{2(7)} = 4$$

$$n = 14 \Longrightarrow p = \frac{14^2 + 3(14) - 14}{2(14)} = 8.$$

p, the number of points scored by each eight-grade contestant, cannot be a negative number. Therefore, we can eliminate the cases of $n = 1$ and $n = 2$. Hence there are two possible scenarios. Either there are $n = 7$ eight-grade contestants and each scored $p = 4$ points or there are $n = 14$ eight-grade contestants and each scored $p = 8$ points.
The problem asks for the largest possible number of eight-grade contestants, which is 14.

■