Modular arithmetic

Dr Richard Kenderdine

Kenderdine Maths Tutoring

Modular arithmetic works with the remainders when an integer is divided by a positive integer. If we divide m by n then the remainder is 0 if m is a multiple of n. Otherwise the remainder varies from 1 to n - 1.

Two integers a and b are said to be congruent mod n if n divides the difference a - b. This is written as $a \equiv b \pmod{n}$ and just means that a and b have the same remainder when divided by n.

Rules for congruences

Two rules that are useful are, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

(1) $a + c \equiv b + d \pmod{n}$.

For example:
$15 \equiv 3 \pmod 4$ and $34 \equiv 2 \pmod 4$ so $15 + 34 \equiv 3 + 2 = 5 \equiv 1 \pmod 4$.
Alternatively, $15 + 34 = 49 \equiv 1 \pmod 4$

(2) $a\,c \equiv b\,d \pmod{n}$

For example:
$11 \equiv 3 \pmod 4$ and $13 \equiv 1 \pmod 4$ so $11 \times 13 \equiv 3 \times 1 = 3 \pmod 4$,
Alternatively, $11 \times 13 = 143 \equiv 3 \pmod 4$

Problem solving with congruences

Congruences are useful in solving many types of divisibility problems. First we need to find all the possible remainders when powers of the integers 2, 3, ..., 9 are divided by 2, 3,...., 9 (the base). Table 1 shows the prevailing pattern of remainders, in order, with these explanations:

(1) some bases produce constant remainders for powers of certain integers. For example, powers of 7 always have a remainder of 1 when divided by 3. This is because $7 \equiv 1 \pmod 3$ and hence $7^k \equiv 1^k = 1 \pmod 3$.

(2) other bases have two possible remainders. For example, powers of 5 have remainders of either 5 or 1 when divided by 6 ($5^1 = 5$, $5^2 \equiv 1$, $5^3 \equiv 5$, $5^4 \equiv 1$ ... .. (mod 6))

(3) bases 5, 7 and 9 can have more than three possible remainders.
Consider the powers of 2 (mod 5):

$2^1 = 2$, $2^2 = 4$, $2^3 \equiv 3$, $2^4 \equiv 1$, $2^5 \equiv 2$ ... ..(mod 5) and the pattern repeats unending.

(4) the remainders for powers of 2 and 6 (mod 8) are shown as always 0. This is the prevailing remainder for powers greater than 2. We have $6^2 \equiv 4 \pmod 8$ but $6^3 = 2^3 \times 3^3$ which is divisible by 8 and hence all higher powers of 6 will be divisble by 8.

	Base							
Powers of	2	3	4	5	6	7	8	9
2	0	2, 1	0	2, 4, 3, 1	2, 4	2. 4, 1	0	2, 4, 8, 7, 5
3	1	0	3, 1	3, 4, 2, 1	3	3, 2, 6, 4, 5, 1	3, 1	0
4	0	1	0	4, 1	4	4, 2, 1	0	4, 7, 1
5	1	2, 1	1	0	5, 1	5, 4, 6, 2, 3, 1	5, 1	5, 7, 8, 4, 2, 1
6	0	0	0	1	0	6, 1	0	0
7	1	1	3, 1	2, 4, 3, 1	1	0	7, 1	7, 4, 1
8	0	2, 1	0	3, 4, 2, 1	2, 4	1	0	8, 1
9	1	0	1	4, 1	3	2, 4, 1	1	0

Table 1: Remainders of powers of 2, 3, ..., 9 when divided by base 2. 3...., 9

Now look at the remainders when all square numbers are divided by 2, 3, ..., 9. Table 2 shows these remainders as recurring series. For example, in mod 7 we have $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 2$, $5^2 \equiv 4$, $6^2 \equiv 1$, $7^2 \equiv 0$, $8^2 \equiv 1$ and the series repeats from then on.

Base	Remainders
2	0, 1
3	1, 0
4	0, 1
5	4, 4, 1, 0, 1
6	4, 3, 4, 1, 0, 1
7	4, 2, 2, 4, 1, 0, 1
8	4, 1, 0
9	4, 0, 7, 7, 0, 4, 1, 0, 1

Table 2: Remainders of the square numbers n^2 mod(base) for $n \geq 2$ and bases 2 - 9

Note that if an integer is even it can be expressed as $2m$ where m is an integer. An odd integer can be expressed as $2m + 1$. These expression squared are $4\,m^2$ and $4\,m^2 + 4\,m + 1$ respectively. Therefore the square of an even number is conguent to 0 mod 2 or 4 while the square of an odd number is congruent to 1 mod 2 or 4. The opposite is true for mod 3.

Here is a list of the first 20 square numbers:

```
In[2]:= Table[n^2, {n, 1, 20}]
Out[2]= {1, 4, 9, 16, 25, 36, 49, 64, 81, 100,
  121, 144, 169, 196, 225, 256, 289, 324, 361, 400}
```

The units digit follows the pattern {1, 4, 9, 6, 5, 6, 9, 4, 1, 0}. There is a reverse symmetry here with the digits {1, 4, 9, 6} in a block and {0, 5} being dividers between the blocks..

The important fact to note is that {2, 3, 7, 8} are never the units digit for square numbers.

This is shown by the remainders for base 5 in Table 2, the remainder is never 2 or 3.

The pattern for the units digit for square numbers is set by the squares of the first 10 numbers. This is because the units digit of the product of two numbers is solely determined by the product of the units digits of the two numbers and these can only be 0 - 9.

A problem to solve

The 2016 Australian Mathematical Olympiad contained the following question:

Find all positive integers n such that $2^n + 7^n$ is a perfect square.

We can use the information provided above to answer this question. Table 3 shows the results for a few values of *n*:

n	2	3	4	5	6	7
2^n	4	8	16	32	64	128
7^n	49	343	2401	16807	117649	823543
$2^n + 7^n$	53	351	2417	16839	117713	823671

Table 3: Sum of powers of 2 and 7

Note that when *n* is even the units digit of the sum is 3 or 7. We know fhat the units digit of a square number cannot be either 3 or 7 so therefore the sum of even integer powers of 2 and 7 never results in a perfect square.

Now consider when *n* is odd. Obviously the result is true for *n* = 1 as 2 + 7 = 9.
For other odd values we use the results for mod 4 in Table 1. The powers of 2 are congruent to 0 mod 4 while odd powers of 7 are congruent to 3 mod 4. Hence the sum of odd powers of 2 and 7 is congruent to 3 mod 4. But we know from Table 2 that square numbers are always congruent to 0 or 1 mod 4. Hence there are no odd integers *n* > 1 that result in a perfect square.

To conclude, the only value of *n* that results in $2^n + 7^n$ being a perfect square is 1.