MATHEMATICAL GAMES

Gauss's congruence theory was mod as early as 1801

by Martin Gardner

There was a young fellow named Ben
Who could only count modulo ten.
He said, "When I go
Past my last little toe,
I shall have to start over again."

Congruence theory (sometimes called modular arithmetic) is based on principles as old as arithmetic, but it was the German "prince of mathematicians," Karl Friedrich Gauss (he has been called the greatest mathematician who ever lived), who pulled them all together and unified them with a notation so compact and powerful that it is hard to imagine how number theory could have advanced without it. The son of an uneducated bricklayer, Gauss was a child prodigy whose most influential book, *Disquisitiones arithmeticae,* was published by himself in 1801 when he was 24. He had written it four years earlier. It was this book that introduced the concept of number congruence.

Gauss defined two integers a and b to be congruent for a modulus m (modulus is from the Latin for a small measure) if their difference is divisible by a nonzero integer m. To say the same thing another way, two integers are congruent modulo m if they have the same remainder when they are divided by m. Gauss symbolized congruence by three short parallel lines, a symbol still used today: $a \equiv b$ (mod m). Incongruence is indicated like this: $a \not\equiv b$ (mod m).

For example, 17 and 52 are congruent modulo 7 because each has a remainder of 3 when it is divided by 7. Expressed the other way, $52 - 17 = 35$, which is 7×5. If we call the multiplier k (in this instance k is 5) and let a be the larger integer, then $b = a + km$, where m is the modulus and k is some integer. Many of the rules of ordinary arithmetic and algebra (such as addition, subtraction and multiplication) apply to the manipulation of congruences.

Remainders are called residues, and for every modulus m there are m "resi-

even numbers are congruent to 0 (mod 2) and have the infinite residue class $\ldots -4, -2, 0, 2, 4, \ldots$ All odd numbers are congruent to 1 (mod 2) and have the infinite residue class $\ldots -3, -1, 1, 3, 5, \ldots$ For $m = 3$ the residues are 0, 1 and 2. There are three infinite classes (mod 3) and so on for higher values of m.

As Gauss made clear, his congruence algebra provided simple proofs for various rules that determine whether a number is divisible by a given number. (From here on "number" will mean "integer.") Thus n is divisible by 3 if and only if the sum of its digits is congruent to 0 (mod 3). Similarly n is congruent to 0 (mod 9) if and only if the sum of its digits is congruent to 0 (mod 9). A number n is congruent to 0 (mod 4) if and only if its last two digits form a number congruent to 0 (mod 4), and n is congruent to 0 (mod 8) if and only if its last three digits form a number congruent to 0 (mod 8). A number is congruent to 0 (mod 11) if and only if the difference between the sum of its digits in even positions and the sum of its digits in odd positions is congruent to 0 (mod 11).

Congruence algebra led to important theorems about prime numbers and also simplified proving them. For example, Fermat's "little theorem," which is useful in testing for primality, states that if a number a is raised to the power of $(p - 1)$, where p is a prime that does not divide a, then when the result is divided by p, the remainder is always 1. In Gauss's terminology, $a^{(p-1)}$ is congruent to 1 (mod p). Thus a number can be raised to the power of one less than a prime so large that the result can have billions of digits and be far beyond the ability of computers to calculate, yet we know that if we subtract 1 from this unprintable monster, we shall have a number that is a multiple of the prime.

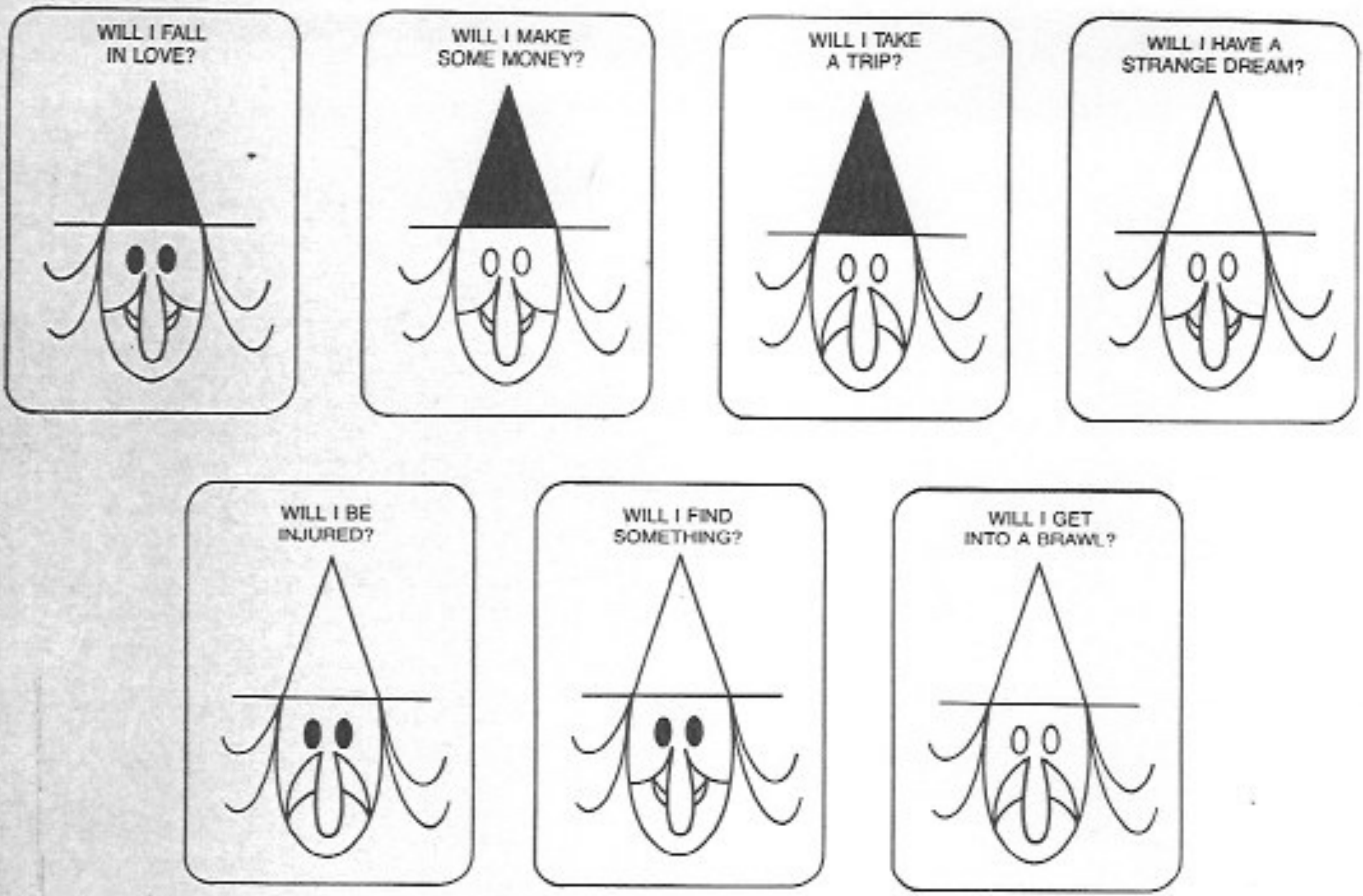
Another famous result related to Fermat's little theorem is known as Wilson's theorem. If you multiply consecutive numbers starting with 1 and stop at any number immediately preceding a prime, the product obviously is divisible by any number up to p but not by p itself. If you add 1 to the product, however, lo and behold the result becomes a multiple of p. For example, 1 times 2 times 3 times 4 is equal to 24, which is not divisible by the next number, 5, a prime. But 24 plus 1 is equal to 25, which *is* a multiple of 5. Using factorial and congruence signs, Wilson's theorem is $(p - 1)! + 1 \equiv 0$ (mod p).

The theorem was known to Leibniz but was rediscovered by a British scholar named John Wilson. Someone credited it to him in an algebra book and remarked that the theorem would never be proved because mathematicians had no good notation for primes. When Gauss was told this, he proved the theorem in five minutes without sitting down, and he commented that for such proofs one needs not *notationes* (notations) but *notiones* (notions). Wilson's theorem is a marvelous criterion for primality, but unfortunately it is of no use in computer searches for big primes.

Thousands of basic theorems in number theory are compactly expressed and their proofs made easy and elegant by modular theory, and endless puzzles have been based on such theorems. For example, suppose a manufacturer of dice ships his product to wholesalers in large cubical boxes. A wholesaler removes one row of dice from the cubical array to test them for possible flaws, and during the tests these dice are destroyed. The remaining dice are packed into small boxes, six to a box. How many dice are left over? Surprisingly, regardless of the size of the original box none are left over. This follows from the congruence theorem $n^3 - n \equiv 0$ (mod 6).

Here is a problem that demonstrates

1. Call the year Y. Subtract 1900 from Y and call the difference N.
2. Divide N by 19. Call the remainder A.
3. Divide $(7A + 1)$ by 19. Ignore the remainder and call the quotient B.
4. Divide $(11A + 4 - B)$ by 29. Call the remainder M.
5. Divide N by 4. Ignore the remainder and call the quotient O.
6. Divide $(N + Q + 31 - M)$ by 7. Call the remainder W.
7. The date of Easter is $25 - M - W$. If the result is positive, the month is April. If it is negative, the month is March (interpreting 0 as March 31, -1 as March 30, -2 as March 29 and so on to -9 for March 22.



The Wicked Witch of the West's magic precognition cards

the power of congruence algebra to provide solutions. (I found it in Allan Gottlieb's "Puzzle Corner" in *Technology Review* for May, 1978.) You want to prove the curious theorem that every integer n has some multiple that consists of a string of 1's followed by a string of 0's. How can you go about it? One way is to list n "rep unit" numbers starting with 1, 11, 111, 1111 up through n such numbers. The number of possible remainders when any number is divisible by n is obviously n. To our list of n rep-unit numbers we add one more. On the pigeonhole principle at least two numbers on this list must have the same remainder and therefore be congruent modulo n. Now, the difference between any two numbers that are congruent modulo n is congruent to 0 (mod n), which means that the difference is a multiple of n. Therefore we subtract the smaller of the pair of congruent rep-unit numbers from the larger, and the result will be a number of the form we seek.

To see better how this works, let us find a number of the form 111 . . . 0 . . . that is a multiple of 7. The first eight rep-unit numbers are 1, 11, 111, 1111, 11111, 111111, 1111111 and 11111111. Their residues (mod 7) are respectively 1, 4, 6, 5, 2, 0, 1 and 4. Since there are eight numbers, we must have at least two numbers with the same residues (mod 7). In this instance there are two such pairs. The smallest pair is 1 and 1111111. The difference is 1111110, or 7 × 158730. It is the smallest number of the form we seek.

Measurements of time in most cultures are made in modular systems. We measure hours by a mod-12 arithmetic. If it is 3:00 now and we want to know what time it will be 1,000 hours from now, we simply add 1,000 to 3, then divide 1,003 by 12. The residue, 7:00, is our answer. The clock is such a familiar model of a modular system that when schoolteachers introduce number congruences, they like to call it "clock arithmetic." The U.S. armed forces use a mod-24 clock. Days of the week conform to mod-7 arithmetic, the months of the year to mod 12 and the years of the century to mod 100.

Many problems about the calendar yield readily to congruence formulas. Gauss himself gave algorithms for determining the day of the week when one is given the year and the day of the month, and also algorithms for calculating the date of Easter. According to the Gospels, the resurrection of Jesus took place on a Sunday morning during the Jewish Passover week, celebrated after the first full moon of spring. The early Christians wanted to keep the symbolic connection between the Passover sacrifice and the sacrifice of Christ, and so it was decided at the First Council of Nicaea (A.D. 325) that Easter would be the first Sunday after the first full moon after the vernal equinox. Unfortunately the old Julian calendar made the year slightly longer than it actually is, so that the vernal equinox kept creeping closer to winter. By 1582 it was getting dangerously near February. When Pope Gregory XIII introduced the present calendar in 1582, he did so mainly to restore Easter to spring. It is a sad commentary on mathematics in the Middle Ages that calculating the exact dates of Easter was then one of the most important of all applications of mathematics to nature.

Gauss's algorithms for determining Easter dates in both the Julian and the Gregorian calendars are complicated, and they have to be patched by special rules to take care of exceptions. If we limit our concern to the years from 1900 to 2099 inclusive, however, there is a straightforward procedure, with no exceptions, that was devised by Thomas H. O'Beirne of Glasgow and first published in his paper "The Regularity of Easter" (*Bulletin of the Institute of Mathematics and Its Applications*, Vol. 2, No. 2, pages 46–49; April, 1966). O'Beirne found he could memorize his procedure and as a party stunt give the date of Easter for any year during the relevant period by making all the calculations mentally.

O'Beirne's algorithm is summarized

in the illustration on page 17. Easter always falls in March or April. The earliest possible date is March 22. It last happened in 1818 (when it fell on a full-moon day), and it will not happen again until 2285. The latest possible date is April 25. It last happened in 1943, and it will not happen again until 2038. You might like to test O'Beirne's procedure to see that it correctly gives April 6 for Easter in 1980, April 19 for 1981 and April 11 for 1982. April 19 is the most frequent of all Easter dates, with April 18 running a close second.

Countless magic tricks, particularly with numbers and playing cards, are based on congruences, and many have been described in previous columns by me. A trick I have not discussed earlier depends on the fact that the sum of all the values of the 52 cards in a deck is $364 \equiv 0 \pmod{13}$. (Jacks count as 11, queens as 12 and kings as 13.) Let someone shuffle the deck, then remove a card without anyone's seeing its face. After dealing just once through the deck of 51 cards, looking at the face of each card, you correctly name the card that was removed.

Magicians have devised many algorithms for this trick, but the following one seems to me the easiest. As you deal the cards keep in your head a running total of the values but cast out 13 as you go along. In other words, whenever the total goes above 13, subtract 13 and keep in mind only the difference. The task is greatly simplified by two rules:

1. Ignore all kings. Their value, 13, is congruent to 0 (mod 13); therefore they do not alter the number you keep in mind.

2. For 10's, jacks and queens, instead of adding 10, 11 and 12, subtract 3, 2 or 1 respectively. This reflects the fact that in the mod-13 system 10 is congruent to -3, 11 is congruent to -2 and 12 is congruent to -1.

After the last card is turned subtract the number in your head from 13 to get the value of the missing card. If the result is 0, the card is a king.

How do you know the suit? A good procedure is to use your feet for secret calculating in mod-2 arithmetic. Start with both feet flat on the floor. For each spade raise or lower your left heel. For each club raise or lower your right heel. For each heart alter the positions of both feet simultaneously. Ignore all diamonds. After the deal your feet indicate the suit of the missing card as follows:

If only the left heel is up, the card is a spade.

If only the right heel is up, the card is a club.

If both heels are up, it is a heart.

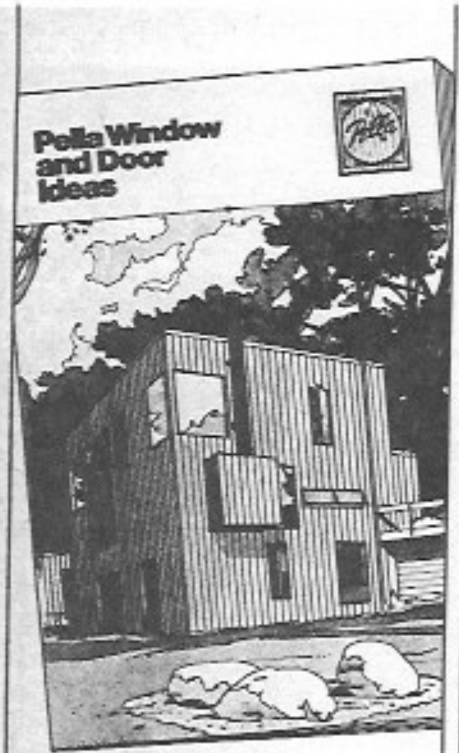
If both heels are down, it is a diamond.

After some practice it is surprising how quickly you can deal through the deck and name the missing card.

Robert Hummer, a magician, has

000 You will dream about a relative.
001 You will have an argument on the telephone.
002 You will dream about elephants.
003 You will exchange angry words with a plumber.
010 You will find a lost ring.
011 Something you say will harm you.
012 You will find the weather abominable.
013 Be alert for an injury to your foot.
020 You will dream about an old friend.
021 Yes, but it will be a fight *you* did not start.
022 You will dream about an airplane.
023 Not if you can control your temper.
030 You will find a coin on the street.
031 Only a slight nick while shaving your face or your legs.
032 You will find a lost object in the pocket of an old bathrobe.
033 No, but you will injure someone else.
100 No, because you know counterfeiting is illegal.
101 You will make a trip to the liquor store.
102 Just the usual amount.
103 You will make a short journey south.
110 You will fall in love with a cat.
111 Maybe.
112 You will fall in love with a stranger in a self-service laundry.
113 Absolutely not.
120 An unexpected check will come by mail.
121 You will trip over a beer can.
122 Not more than $1,000.
123 You will visit an out-of-town friend.
130 You will fall in love with a new car.
131 Positively yes.
132 You will fall in love with a real estate agent.
133 Foolish question.
200 You will dream you are a bird.
201 You *never* get in brawls.
202 A dream will wake you in the middle of the night.
203 You will have a falling-out with an old friend.
210 You will find a lost key.
211 No injury of any sort for the next seven days, but be careful on the eighth.
212 You will find something unpleasant in your bed.
213 Watch out for a punch on your nose.
220 You will dream of coconut pie.
221 Avoid arguments on a bus.
222 You will dream about a flying saucer.
223 Be careful not to antagonize anyone named Harvey.
230 You will find this trick puzzling.
231 It is a dangerous week to stand on stepladders.
232 You will find the news tomorrow disturbing.
233 Climbing stairways can be dangerous.
300 Yes, *lots* of money.
301 You will not leave your neighborhood all week.
302 On the contrary, you will *lose* some money.
303 You will take a marvelous trip in your imagination.
310 You will not fall in love with anyone for a change.
311 *You* can answer that as well as I can.
312 You will fall for someone in show business.
313 Whom do you think you are kidding?
320 Yes, but most of it will go for taxes.
321 Yes, but you will not enjoy the trip.
322 Some, but you will spend it immediately.
323 You will go on a long trip by plane.
330 You will fall in love *twice*.
331 I don't know.
332 You will fall *out* of love.
333 You should be ashamed to ask such a question.

The Wicked Witch's answers



been unusually productive in inventing mathematical tricks, and many of his creations are based on mod-2, or odd-even, principles. I give here for the first time a set of mysterious fortunetelling cards that is one of Hummer's most ingenious ideas.

First you must make a set of the seven cards shown in the illustration on page 18. Photocopy them, paste them on a sheet of cardboard and cut them out. Here is how they are used.

You are allowed to ask the Wicked Witch of the West only one question a day. Of course, you may experiment with more questions if you like, but the answers are not guaranteed to be trustworthy. Each answer applies only to a period of seven days following the day the question is asked. Select the card with the desired question and put it aside. Shuffle the remaining six cards and hold them face down in one hand. Wave your other hand over the packet and slowly pronounce the mystic precognitive mantra "Puthoffa Targu."

From the top of the packet remove the first pair of cards. If the colors of the hats match, put the cards aside to form a pile. Discard them if the hats fail to match. Repeat with the next pair. If the colors of the hats match, put the pair on top of the pile. Otherwise discard them. Check the remaining pair and repeat the procedure. Now count the number of matching pairs. The number will be 0, 1, 2 or 3. Write this down as the first digit of a three-digit number.

Assemble the six cards, shuffle, pronounce the mystic mantra and repeat the procedure, except this time look for matching eyes. Record the number of matching pairs as the second digit of your number.

Shuffle the six cards for the third and last time, say the mantra and go through the packet by pairs as before. This time look for matching expressions (smile or frown). The matching pairs are counted—remember, you count pairs, not single cards—to get the last digit of your number.

Find your number in the illustration on the preceding page and read the answer. Even though the digits of your number were randomly obtained, you will find a specific answer that applies only to the question asked.

If you want to ask the Wicked Witch a yes-no question that is not on any card, you may do so, but now you must use all seven cards. Follow the same procedure, looking first at the hats, then at the eyes and then at the expression. This time, however, you must form two piles, one of matching pairs and one of nonmatching pairs. Ignore the last card. Subtract the number of pairs in the smaller pile from the number of pairs in the larger and record the number. After three trials you will have a three-digit number that gives the answer to your question.

Larger sets of cards can be designed for answering a larger number of questions. The number of cards must be one less than a power of 2. In 1980 Karl Fulves published *Bob Hummer's Collected Secrets*, a compilation of all known Hummer tricks. This gold mine of ideas for mathematical magic is available postpaid from Fulves for $20 sent to Box 433, Teaneck, N.J. 07666. Page 77 of the book describes a set of 15 fortunetelling cards, each with four features that may or may not match, to be used with a fortunetelling book (not provided!) of $8^4 = 4,096$ answers. I leave it to readers to puzzle out why the answers are always appropriate.

Having opened with an anonymous limerick about congruences, I shall close with one by John McClellan, an artist living in Woodstock, N.Y., whose work reflects a lifelong interest in recreational mathematics and wordplay:

A lady of 80 named Gertie
Had a boyfriend of 60 named Bertie.
She told him emphatically
That viewed mathematically
By modulo 50 she's 30.

Two questions about prime-number patterns were left unanswered in my December column. The first concerned a procedure that seems to generate only primes. Did you recognize this as a clever disguise of Euler's famous prime-generating formula $41 + x^2 + x$? Letting x have integral values starting with 0, the formula generates 40 primes. It fails for $n = 40$, which gives the composite number $1,681 = 41^2$.

Leo Moser's triangle pattern is based on the properties of a sequence known as Farey fractions. It produces a sequence with a prime number of numbers for the first nine rows, but it fails for $n - 10$, which gives a sequence of 33 numbers. If one counts digits instead of numbers, the 10th sequence has 37 digits, a prime, but the next sequence has $57 = 3 \times 19$ digits.

To obtain the k numbers for the nth row, add 1 to the sum of the Euler totients for numbers 1 through n. The Euler totient for a natural number n is the number of natural numbers not greater than n that have no common divisors with n other than 1. For 1 through 10 the Euler totients are 1, 1, 2, 2, 4, 2, 6, 4, 6 and 4. The sum of these numbers is 32. Adding 1 gives the composite number 33 for the 10th row. I do not know if Moser ever published this curiosity.

The largest pair of twin primes given in the December column has now been surpassed by an even larger pair discovered in 1980 by A. O. L. Atkin and Neil W. Rickert, the same two mathematicians at the University of Illinois at Chicago Circle who previously held the record. The new pair of twin primes, which has more than 1,000 digits, is $1024803780 \times 2^{3424} \pm 1$.

Established 1845 **SCIENTIFIC AMERICAN** February 1981 Volume 244 Number 2

ARTICLES

DEPARTMENTS

SCIENTIFIC AMERICAN (ISSN 0036-8733), PUBLISHED MONTHLY BY SCIENTIFIC AMERICAN, INC., 415 MADISON AVENUE, NEW YORK, N.Y. 10017. COPYRIGHT © 1981 BY SCIENTIFIC AMERICAN, INC. ALL RIGHTS RESERVED. PRINTED IN THE U.S.A. NO PART OF THIS ISSUE MAY BE REPRODUCED BY ANY MECHANICAL, PHOTOGRAPHIC OR ELECTRONIC PROCESS, OR IN THE FORM OF A PHONOGRAPHIC RECORDING, NOR MAY IT BE STORED IN A RETRIEVAL SYSTEM, TRANSMITTED OR OTHERWISE COPIED FOR PUBLIC OR PRIVATE USE WITHOUT WRITTEN PERMISSION OF THE PUBLISHER. CONTROLLED CIRCULATION POSTAGE PAID AT NEW YORK, N.Y. (USPS 509-530), AND AT CHICAGO, ILL. (USPS 508-030). AUTHORIZED AS SECOND-CLASS MAIL BY THE POST OFFICE DEPARTMENT, OTTAWA, CANADA, AND FOR PAYMENT OF POSTAGE IN CASH. SUBSCRIPTION RATE: $21 PER YEAR, U.S., ITS POSSESSIONS AND CANADA; $27 PER YEAR, ALL OTHER COUNTRIES. POSTMASTER: SEND ADDRESS CHANGES TO SCIENTIFIC AMERICAN, 415 MADISON AVENUE, NEW YORK, N.Y. 10017