Arithmetic of Remainders (Congruences)

Donald Rideout, Memorial University of Newfoundland[1]

Divisibility is a fundamental concept of number theory and is one of the concepts that sets it apart from other branches of mathematics. Another approach to divisibility questions is through the arithmetic of remainders, or the theory of congruences as it is now commonly known. The concept was first introduced by Carl Friedrich Gauss (1777-1855) in his *Disquisitiones Arithmeticae*; this monumental work, which appeared in 1801 when Gauss was 24 years old, laid the foundations of modern number theory.

We say that a is *congruent to* b modulo m, and we write

$$a \equiv b \pmod{m},$$

if m divides the difference $a-b$; that is, provided $a-b=km$ or $a=b+km$ for some integer k. If $m \nmid (a-b)$, then we say that a is *incongruent to* b modulo m and in this case we write $a \not\equiv b \pmod{m}$. For example, $3 \equiv 24 \pmod{7}$, $19 \equiv -2 \pmod{7}$, $-15 \equiv -64 \pmod{7}$ since $7 \mid (3-24)$, $7 \mid (19+2)$, and $7 \mid (-15+64)$, respectively.

The number m is called the *modulus* of the congruence. Congruences with the same modulus behave in many ways like ordinary equations. For if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \pm c \equiv b \pm d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

A warning is in order here. It is not always possible to divide congruences. If $ac \equiv bc \pmod{m}$, it need not be true that $a \equiv b \pmod{m}$. For example, $15 \cdot 2 \equiv 20 \cdot 2 \pmod{10}$, but $15 \not\equiv 20 \pmod{10}$. Even more distressing is that we can have $ab \equiv 0 \pmod{m}$ with $a \not\equiv 0 \pmod{m}$ and $b \not\equiv 0 \pmod{m}$. For example, $6 \cdot 4 \equiv 0 \pmod{12}$, while clearly $6 \not\equiv 0 \pmod{12}$ and $4 \not\equiv 0 \pmod{12}$. However, it is permissible to cancel c from the congruence $ac \equiv bc \pmod{m}$ provided $(c, m) = 1$.

Let a be an integer. For any positive integer m, by the division algorithm, we have $a = mq + r$ where $0 \leq r \leq m-1$, and clearly $a \equiv r \pmod{m}$. The number r is called the *least positive residue* modulo m. Hence, every a is congruent modulo m to one and only one of the integers in the set $\{0, 1, 2, ..., m-1\}$, namely the (unique) remainder when divided by m. (Hence the justification of Gauss' phrase *arithmetic of remainders*.) It should be clear now that $a \equiv b \pmod{m}$ if and only if a and b have the same remainders when divided by m. We say that a and b are in the same *equivalence class* modulo m if they have the same remainder. We can think

[1]Talk given at CMC Seminar, Waterloo, June 1997

of $\equiv$ as behaving almost exactly like $=$ if we do not make a fuss over the difference between numbers in a particular equivalence class. Hence modulo 10 we see very little difference, so to speak, between 2 and 12 and 202 and -3002.

We will now see how congruences can be used to solve some problems, that otherwise might be cumbersome to solve. First note that we can make repeated use of the useful result that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, imply $a \pm c \equiv b \pm d \pmod{m}$ and $ac \equiv bd \pmod{m}$. For example, if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$. Hence, for example, $10^{17} \equiv 1^{17} \equiv 1 \pmod{9}$ and $10^{17} \equiv (-1)^{17} \equiv -1 \equiv 10 \pmod{11}$. Note that 10^{17} is quite a large number, but we found the remainders quite effortlessly! We quote the limerick by Martin Gardner about the modulus 10:

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."

Problems:

1. Let $f(x) = 375x^5 - 131x^4 + 15x^2 - 435x - 2$. Find the remainder when $f(97)$ is divided by 11.

2. Prove that a number is divisible by 8 if and only if the integer formed by its last three digits is divisible by 8.

3. Prove that a number is divisible by 3 if and only if the sum of its digits is divisible by 3, and that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

   Solution: We prove the rule for divisibility by 9. Let $N = \sum_{k=0}^{m} a_k 10^k$ where $0 \leq a_i \leq 9$ and $a_m \neq 0$. Clearly $N \equiv \sum_{k=0}^{m} a_k \pmod{9}$, since $10^k \equiv 1^k \equiv 1 \pmod{9}$. Hence $N \equiv 0 \pmod{9}$ if and only if $\sum_{k=0}^{m} a_k \equiv 0 \pmod{9}$.[2]

4. Given the number 2492, double the units digit and subtract it from the number formed by the other digits. We get $249 - 2 \times 2 = 245$. Repeating this algorithm we get $24 - 2 \times 5 = 14$. Since 14 is clearly divisible by 7, the original number 2492 must be divisible by 7. Prove this rule for checking divisibility by 7.

[2]We are instinctively using the following rules for congruences which really need proof: for any modulus m, $a \equiv b$ implies $b \equiv a$, and $a \equiv b$, $b \equiv c$, imply $a \equiv c$.

Solution: Let $N = \sum_{k=0}^{m} a_k 10^k$ where $0 \leq a_i \leq 9$ and $a_m \neq 0$. Then

$$\begin{aligned} N &= 10(\sum_{k=1}^{m} a_k 10^{k-1}) + a_0 \\ &\equiv 10(\sum_{k=1}^{m} a_k 10^{k-1}) - 20a_0 \pmod 7 \\ &\equiv 10(\sum_{k=1}^{m} a_k 10^{k-1} - 2a_0) \pmod 7. \end{aligned}$$

Hence $N \equiv 0 \pmod 7$ if and only if $\sum_{k=1}^{m} a_k 10^{k-1} - 2a_0 \equiv 0 \pmod 7$, since $(10, 7) = 1$.

5. The residues modulo 7 of the powers of 10, starting with 10^0 are

$$1, 3, 2, 6, 4, 5, 1, 3, 2, \cdots.$$

Let $w_0 = 1, w_1 = 3, w_2 = 2, w_3 = 6, w_4 = 4, w_5 = 5, w_6 = 1, w_{n+6} = w_n$ for $n \geq 0$. Prove that $N = \sum_{k=0}^{m} a_k 10^k$ is divisible by 7 if and only if $\sum_{k=0}^{m} a_k w_k$ is divisible by 7. (Repeat the process until we get an integer that is EASY to check for divisibility by 7.)

6. Prove that an integer is divisible by 11 if and only if the difference between the sum of the digits in the odd places and the sum of the digits in the even places is divisible by 11. (Use congruence modulo 11, otherwise you will have to establish some other way that $11 \mid (10^k + 1)$ if k is odd, and $11 \mid (10^k - 1)$ if k is even.)

7. Prove that every odd integer other than a multiple of 5 has some multiple that is a string of 1's (called *a repunit*).

8. If a and b are odd integers, prove that $a^2 + b^2$ is never a square.

Solution: For any integer c, $c^2 \equiv 0^2, 1^2, 2^2$, or $3^2 \pmod 4$. That is, $c^2 \equiv 0$ or $1 \pmod 4$. The odd squares can only be congruent to 1 modulo 4. Hence $a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 4$. But 2 is not a square modulo 4.

9. Prove that $a^2 - 11b^2 = 13$ has no integer solutions.

Solution: Modulo 11 we have for any solution a and b that $a^2 \equiv 13 \equiv 2 \pmod{11}$. But the squares modulo 11 are 0, 1, 4, 9, 5, and 3. The number 2 is not

in this list![3] You should try to prove that the above equation has no solutions by some other method.

10. Prove that $6 \mid (n^3 - n)$ for any integer n.

11. Prove that $30 \mid ab(a^4 - b^4)$ for ever pair of integers a and b.

    Solution: The most efficient way to solve this problem is probably by using congruence modulo 2, 3, and 5. Consider each number in turn. For example, for the modulus 5, either $5 \mid a$ or $5 \mid b$ or, by checking the numbers $a \equiv 1$, 2, 3, and 4 (mod 5), we have $a^4 \equiv 1 \pmod 5$. Similarily for b. Hence $a^4 - b^4 \equiv 1 - 1 \equiv 0 \pmod 5$. That is, $5 \mid (a^4 - b^4)$.

12. Fermat's Little Theorem: If p is a prime and $p \nmid a$, prove that $a^{p-1} \equiv 1 \pmod p$. (Hint: Show that $(k+1)^p - k^p \equiv 1 \pmod p$ for $k = 0, 1, 2, \cdots$.)

13. Find the remainder when 319^{566} is divided by 23, and also when divided by 17.[4]

14. Our present calendar, the Gregorian calendar, was introduced by Pope Gregory XIII in 1582 to correct a slight error in the Julian calendar (introduced by Julius Caesar in 46 B.C.) which was gradually accumulating into a significant error. The Julian calendar is the same as the Gregorian calendar, except that every year (such as 1900) divisible by 100 is a leap year. Thus the Julian calendar has three extra days every four centuries. In 1582, the Julian calendar was in error by 10 days; thus October 5, 1582 (Julian calendar) was converted to October 15, 1582 (Gregorian calendar). (Actually there is still a slight error in the Gregorian calendar which will amount to a full day in about 3300 years.) The Gregorian calendar was adopted in 1582 by France and Spain, but England and her North American colonies waited until 1752 to adopt it and Russia did not adopt it until after the revolution in 1917. In 1976 J. H. Conway composed the following limerick to compute the day of the week on which any date from 46 B.C. can be computed.

[3] These so-called *Pell* equations have infinitely many solutions in many cases. For example, the equation $a^2 - 1141b^2 = 1$ has infinitely many positive integer solutions, the smallest one being $a = 1036782394157223963237125215$ and $b = 30693385322765657197397208$.

[4] Computing large powers $a^k \pmod m$ has a real-world use in creating secure codes. In order to create these codes, it is necessary to find two large primes, say between 100 and 200 digits, and then the modulus m is the product of these primes. If the primes are kept secret, it is impossible to factor m even with the fastest computers to retrieve the two primes.

The last of Feb., or of Jan. will do
(Except that in Leap Years it's Jan. 32)
Then for even months use the month's own day,
*And for odd ones add 4, or take it away**

Now to work out your doomsday the orthodox way
Three things you should add to the century day
Dozens, remainder, and fours in the latter,
(If you alter by sevens of course it won't matter)

In Julian times, lackaday, lackaday
Zero was Sunday, centuries fell back a day
But Gregorian 4 hundreds are always Tues.
And now centuries extra take us back twos.

**According to length or simply remember,*
you only subtract for September, or November.

J. H. Conway, Jan., 1976

The first stanza gives a date for each month which falls on the same day of the week, called the doomsday. These dates are January 31/32, February 28/29, March 3 + 4, April 4, May 5 + 4, June 6, July 7 + 4, August 8, September 9 - 4, October 10, November 11 - 4, and December 12. Note that in 1997 this common doomsday is Friday. The method to determine the doomsday is explained in the second stanza, and the century day is defined in the third stanza. On what days of the week did the following events occur?

January 28, 1986	Disaster of the 25th Apollo Mission.
February 14, 1982	Ocean Ranger sinking.
October 14, 1942	S. S. Caribou sunk.
August 10, 1941	Start of meeting of Churchill and Roosevelt in Placentia Bay.
June 11, 1929	Probable date of the launching of the *Bessie Marie*, the l ast three-mast schooner built in Newfoundland by the great grandfather of the author.
January 23, 1862	Birthdate of the mathematician David Hilbert.
May 31, 1832	The great mathematician Évariste Galois died at the age of 20 of peritonitis after a gun dual with pistols at 25 paces.
June 19, 1623	Birth of Blaise Pascal.
December 25, 1642	Sir Isaac Newton was born.
December 21, 1571	Johann Kepler was born in longitude $29°7'$, latitude $48°54'$.
January 25, 1736	Joseph Louis Lagrange was born in Turin, Italy.
October 31, 1517	Martin Luther nailed 95 Articles to the door of Wittenburg Church.
March 23, 1749	Pierre Simon de Laplace was born at Beaumont-ln-Auge, a Normandy village in sight of the English Channel.