PROBLEM SOLVING VIGNETTES

No.3

Donald Rideout

Arithmetic of Remainders

Divisibility is a fundamental concept of number theory and is one of the main ideas that sets it apart from other branches of mathematics. The main 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,

$$\begin{aligned} 3 &\equiv 24 \pmod{7} \quad \text{since } 7|(3-24), \\ 19 &\equiv -2 \pmod{7} \quad \text{since } 7|(19+2), \\ -15 &\equiv -64 \pmod{7} \quad \text{since } 7|(-15+64). \end{aligned}$$

The number m is called the *modulus* of the congruence. Congruences with the same modulus behave in many ways like ordinary equations. In particular, if

$$a \equiv b (\text{mod } m) \text{ and } c \equiv d (\text{mod } m),$$

then

$$a \pm c \equiv b \pm d (\text{mod } m) \text{ and } ac \equiv bd (\text{mod } m).$$

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, we have $15 \cdot 2 \equiv 20 \cdot 2 \pmod{10}$, 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 that c and m do not have common factors, that is $\gcd(c, m) = 1$.

Let a be an integer. For any positive integer m, by the division algorithm, we have

$$a = mq + r \text{ where } 0 \leq r \leq m-1,$$

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 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 -3008.

We will now see how congruences can be used to solve problems that otherwise might be cumbersome to solve. First note that we can make repeated use of the 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,

$$10^{17} \equiv 1^{17} \equiv 1 \pmod{9},$$
$$10^{17} \equiv (-1)^{17} \equiv -1 \equiv 10 \pmod{11}.$$

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."*

Problem 1 *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 $0 \leq a_k \leq 9$ 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 $\sum_{k=0}^{m} a_k \equiv 0 \pmod{9}$. □

Note that 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 $a \equiv c$.

Problem 2 *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.*

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

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

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 $(10, 7) = 1$. □

Problem 3 *Prove that every odd integer other than a multiple of 5 has some multiple that is a string of 1's (called* a repunit*).*

Solution: We will leave the general proof to the reader. We will prove that 7 has a multiple of the form $1111\cdots$. The first $7 + 1$ repunit numbers are

$$1, 11, 111, 1111, 11111, 111111, 1111111, 11111111.$$

The residues (remainders) of these numbers modulo 7 are 1, 4, 6, 5, 2, 0, 1, and 4. Since there are eight numbers, we can apply the pigeon-hole principle: the pigeon-holes are labelled with the seven distinct residues modulo 7, and the pigeons are labelled with the 8 repunit residues; that is, we have one more pigeon than pigeon-holes, so two pigeons must share the same hole. So by the pigeon-hole principle, we must have at least two numbers with the same residue (mod 7). In this instance there are two such pairs. The smallest pair is 1 and 1111111. The difference is 1111110, which must be a multiple of 7. Since $7 \nmid 10$, we can divide by 10. Then $111111 = 7 \times 15873$ is a multiple of 7. □

Problem 4 *If a and b are odd integers, prove that* $a^2 + b^2$ *is never a square.*

Solution: For any integer c,

$$c^2 \equiv 0^2, 1^2, 2^2 \text{ or } 3^2 \pmod 4.$$

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. □

Problem 5 *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! □

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 $a = 1,036,782,394,157,223,963,237,125,215$ and $b = 30,693,385,322,765,657,197,397,208$ (26 digits).

Problem 6 *Prove that* $30|ab(a^4 - b^4)$ *for every pair of integers* a *and* b.

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

Don Rideout is a retired math professor from Memorial University of Newfoundland. He can be reached via `drideout@mun.ca`.

Contact us

We welcome feedback on *MathemAttic* as the newest addition to *Crux*.

If you have questions, comments or ideas, please feel free to email editors at `MathemAttic@cms.math.ca`.