Some basic modular arithmetic

Fermat's Christmas Theorem series

2025-12-14

ENG ITA

Introduction

We are at the bus stop, waiting for our bus to arrive. On the table it is written that there are three buses arriving soon:

- Bus A arrives in 2 minutes;
- Bus B arrives in 5 minutes;
- Bus C arrives in 10 minutes.

Of course we are not lucky, and we have to wait for bus C. While watching buses arriving and leaving, we ask ourselves:

Question: Will buses A, B, and C ever arrive simultaneously?

We read on the table that:

- Bus A passes every 3 minutes;
- Bus B passes every 24 minutes;
- Bus C passes every 23 minutes.

We have our notebook with us, so we approach the problem in the brutal way. We list all the times at which buses A, B, and C pass (the numbers are the waiting times in minutes):

- Bus A will pass in
$$2, 5, 8, 11, 14, 17, ...$$
- Bus B will pass in
$$5, 29, 53, 77, 101, ...$$

- Bus C will pass in

$$10, 33, 56, 79, 102, ...$$

We do not know whether, by continuing this list, we will find a common number in the three lists (which would mean a simultaneous arrival). This method is tedious, so we want an efficient way to solve this problem in general.

Let's translate the problem into a mathematical setting. What does it mean that bus A passes every 3 minutes and it arrives in 2 minutes? It means that the possible times (in minutes) at which bus A will pass are of the form $3 \cdot n + 2$, where n is a nonnegative integer (i.e. $n = 0, 1, 2, ...$; convince yourself about this). Indeed, all the numbers we listed for A are of this form.

Similarly, the waiting times for bus B are of the form $24 \cdot k + 5$ and the waiting times for bus C are of the form $23 \cdot \ell + 10$. Then, finding a time x (always in minutes) when A, B, and C arrive simultaneously means finding three nonnegative integers n, k, ℓ such that

$$x = 3 \cdot n + 2, \qquad x = 24 \cdot k + 5, \qquad x = 23 \cdot \ell + 10.$$

In other words, the total waiting time x must be of all three forms at the same time.

Congruences of integers

Let's make the notation a little bit better and more helpful.

Definition: Let n, m, and q be integers, with $q > 0$. We write

$$n \equiv_q m$$

if the remainder of the division of n by q and the remainder of the division of m by q are the same.

The writing $n \equiv_q m$ is read as "n is *congruent* to m *modulo* q".

Example 0.1. Consider $n = 14$ and $q = 3$. Then $14 \equiv_3 2$. Indeed,

$$14 = 3 \cdot 4 + 2$$

has remainder 2, and also 2 has remainder 2 when divided by 3.

Remark 0.1. For every integer n and q with $q > 0$, if r is the remainder of the division of n by q, then $n \equiv_q r$.

The following fact is of fundamental importance.

Proposition 0.1. *Let n, m, and q be integers with $q > 0$. Then $n \equiv_q m$ if and only if q divides $n - m$.*

Proof. Suppose that $n \equiv_q m$. Then the remainder of the division of n by q is the same as the remainder of the division of m by q. Let's call this remainder r.

By Euclidean division, there exist integers k and ℓ such that

$$n = q \cdot k + r, \qquad m = q \cdot \ell + r,$$

with $0 \leq r < q$.

Subtract the second equation from the first:

$$n - m = (q \cdot k + r) - (q \cdot \ell + r).$$

Now we simplify it:

$$n - m = q \cdot k + r - q \cdot \ell - r,$$

and cancelling r on the right-hand side we get

$$n - m = q \cdot k - q \cdot \ell.$$

Factor q:

$$n - m = q \cdot (k - \ell).$$

This means exactly that q divides $n - m$.

Conversely, suppose that q divides $n - m$. This means that there exists an integer t such that

$$n - m = q \cdot t.$$

Rearrange:

$$n = m + q \cdot t.$$

Now divide m by q: by Euclidean division there exist integers ℓ and r with $0 \leq r < q$ such that

$$m = q \cdot \ell + r.$$

Plug this into the previous equation:

$$n = (q \cdot \ell + r) + q \cdot t = q \cdot (\ell + t) + r.$$

So when you divide m by q you get remainder r, and when you divide n by q you also get remainder r. Therefore $n \equiv_q m$. □

Let us now make some examples. Observe that $14 \equiv_3 2$ and that $19 \equiv_3 1$. We ask what is

$$14 + 19 \equiv_3 \ ?$$

Maybe you already guessed it: we have

$$14 + 19 \equiv_3 2 + 1.$$

Therefore we are saying that

$$33 \equiv_3 3.$$

But we also know that $3 \equiv_3 0$ (indeed 3 has remainder 0 when divided by 3), therefore

$$33 \equiv_3 0.$$

What we are saying is that 33 is divisible by 3.

We ask the same for the product:

$$14 \cdot 19 \equiv_3 \ ?$$

We are lucky again: we get

$$14 \cdot 19 \equiv_3 2 \cdot 1,$$

which means that

$$266 \equiv_3 2,$$

i.e. 266 has remainder 2 when divided by 3.

We state this precisely in the following proposition.

Proposition 0.2. *Let n, m, n', m', and q be integers with $q > 0$. If $n \equiv_q m$ and $n' \equiv_q m'$, then*

$$n + n' \equiv_q m + m'$$

and

$$n \cdot n' \equiv_q m \cdot m'.$$

Easy part of Fermat's Christmas Theorem

Proposition 0.3. *Let n be an odd integer that can be written as the sum of two squares. Then $n \equiv_4 1$, or equivalently n has remainder 1 when divided by 4.*

Remark 0.2. In particular, the theorem also tells us that if p is an odd prime that can be written as the sum of two squares, then it has remainder 1 when divided by 4, which is part of what Fermat's Christmas Theorem says.

Proof. If n can be written as the sum of two squares, it means that there exist integers a, b such that

$$n = a^2 + b^2.$$

Observe that n is odd, therefore it has remainder 1 when divided by 2, i.e.

$$n \equiv_2 1.$$

Therefore

$$a^2 + b^2 \equiv_2 1.$$

If both a and b were odd, then $a \equiv_2 1$ and $b \equiv_2 1$, therefore

$$a^2 \equiv_2 1, \qquad b^2 \equiv_2 1,$$

which would mean

$$a^2 + b^2 \equiv_2 1 + 1 \equiv_2 2 \equiv_2 0,$$

and therefore $n \equiv_2 0$, which is impossible since n is odd.

Similarly, if a and b are both even, then $a^2 + b^2 \equiv_2 0$, which is again impossible.

Therefore, one is odd and one is even. Call a the odd one and b the even one. We have

$$a \equiv_2 1, \qquad b \equiv_2 0.$$

Since b is even, when we divide b by 4 we get either remainder 0 or remainder 2 (otherwise it would be odd). So

$$b \equiv_4 0 \quad \text{or} \quad b \equiv_4 2.$$

In both cases we get

$$b^2 \equiv_4 0.$$

Similarly, since a is odd, we have

$$a \equiv_4 1 \quad \text{or} \quad a \equiv_4 3.$$

In both cases (check!) we get

$$a^2 \equiv_4 1.$$

Therefore

$$a^2 + b^2 \equiv_4 1 + 0 \equiv_4 1,$$

which means

$$n \equiv_4 1.$$

□

Invertible numbers modulo q

Recall what the greatest common divisor is:

Definition: Let n and m be two integers different from 0. The greatest common divisor $\gcd(n, m)$ is the product of the common primes appearing in the factorizations of n and m, taken with the least power.

Example 0.2. We compute the greatest common divisor between 72 and 540. We have

$$72 = 2^3 \cdot 3^2, \qquad 540 = 2^2 \cdot 3^3 \cdot 5,$$

therefore

$$\gcd(72, 540) = 2^2 \cdot 3^2.$$

Suppose we have two integers n and q with $q > 0$. We ask when there exists another integer m such that

$$n \cdot m \equiv_q 1.$$

Let's try a few examples:

- If $n = 4$ and $q = 7$, then
$$4 \cdot 2 \equiv_7 1.$$
- If $n = 4$ and $q = 6$, then we cannot find any such m.
- If $n = 3$ and $q = 9$, we cannot find any such m.
- If $n = 3$ and $q = 5$, then
$$3 \cdot 2 \equiv_5 1.$$

Try some examples yourself.

Definition: Let n and q be integers with $q > 0$. We say that n is *invertible modulo* q if there exists an integer m such that

$$n \cdot m \equiv_q 1.$$

The answer to the question is given by the following proposition.

Proposition 0.4. *Let n and q be integers with $q > 0$. Then n is invertible modulo q if and only if* $\gcd(n, q) = 1$.

Chinese Remainder Theorem

We now state the theorem that will let us solve our bus problem efficiently.

Theorem 0.1. *Let $s, t > 1$ be integers with $\gcd(s,t) = 1$. Then for all integers a and b there exists an integer x such that*

$$x \equiv_s a \qquad \textit{and} \qquad x \equiv_t b.$$

Proof. We want

$$x \equiv_s a \qquad \text{and} \qquad x \equiv_t b.$$

The first congruence $x \equiv_s a$ means that $x - a$ is divisible by s, hence x is of the form

$$x = a + s \cdot n$$

for some integer n.

Now we impose the second congruence. We want $x \equiv_t b$, i.e.

$$a + s \cdot n \equiv_t b.$$

Subtract a from both sides:

$$s \cdot n \equiv_t b - a.$$

So the whole problem becomes: can we solve

$$s \cdot n \equiv_t (b - a)?$$

Since $\gcd(s,t) = 1$, by Proposition 0.4 the number s is invertible modulo t. This means that there exists an integer u such that

$$s \cdot u \equiv_t 1.$$

Now multiply the congruence $s \cdot n \equiv_t (b - a)$ by u:

$$(s \cdot u) \cdot n \equiv_t u \cdot (b - a).$$

But $s \cdot u \equiv_t 1$, so the left-hand side becomes

$$1 \cdot n \equiv_t u(b - a),$$

that is,

$$n \equiv_t u(b - a).$$

Therefore, if we choose $n := u(b - a)$, we get our solution, which is

$$x = a + s \cdot u(b - a).$$

□

Remark 0.3. Observe that Theorem 0.1 tells us about the *existence* of a solution. However, in general the solution is not unique. Indeed, suppose that we have a solution x. Then also $x + st$ is a solution, because

$$x + st \equiv_s x, \qquad x + st \equiv_t x.$$

In particular, after having found a solution x, all the other solutions are of the form $x + st \cdot k$ with k an integer.

Solution to the bus problem

Let x be the waiting time (in minutes) until a simultaneous arrival.

From the data, we get:

- Bus A: passes every 3 minutes and arrives in 2 minutes, so $x = 3 \cdot n + 2$, i.e.

$$x \equiv_3 2.$$

- Bus B: passes every 24 minutes and arrives in 5 minutes, so

$$x \equiv_{24} 5.$$

- Bus C: passes every 23 minutes and arrives in 10 minutes, so

$$x \equiv_{23} 10.$$

So we want to understand whether there exists an x such that

$$x \equiv_3 2, \qquad x \equiv_{24} 5, \qquad x \equiv_{23} 10.$$

Since 24 is a multiple of 3, from $x \equiv_{24} 5$ we get that 24 divides $x - 5$. In particular, 3 divides $x - 5$, so $x \equiv_3 5$.

But $5 \equiv_3 2$, therefore $x \equiv_3 2$ automatically.

So the condition for bus A is already forced by the condition for bus B, and the problem reduces to solving only

$$x \equiv_{24} 5, \qquad x \equiv_{23} 10.$$

Once we find such an x, bus A will also arrive at time x. Theorem 0.1 tells us that such a solution exists, since $\gcd(24, 23) = 1$. Therefore, the buses will arrive simultaneously some time in the future (you can check that $x = 125$ works).

This article is part of the series *Fermat's Christmas Theorem*.

Previous: How many primes are there?