Modular Arithmetic

Stuyvesant Math Team

Aditya and Noam

March 3, 2024

Contents

1 First definitions

It's often useful to talk about the remainder of some number divided by another number. Often, it's so useful that the original number won't be necessary at all — if we know its remainder, then we can solve the problem at hand.

Given this, here's a quick definition of a remainder:

Definition 1.1 — Given integers a and b, where $b > 0$, the **remainder** of a when divided by b is the unique integer r such that

1. $a = bn + r$
2. $0 \leq r < b$

In fact, this is not a definition — it's a theorem. We're claiming that given any a and b, we can find such an r, and that there is exactly one r that works.

The problem with this is that when computing remainders, we often don't necessarily need r to satisfy the second condition until the last step. For example, if we were to compute the remainder of 22782 when divided by 11, we might note that the remainder of 22782 is the same as the remainder of 782, which is 12.

In other words, there's an important relationship not just between a number and its remainder, but between any two numbers that have the same remainder when divided by a fixed n. We want a notational way to express this:

Definition 1.2 — Given integers a, b and n, where $n > 1$, $a \equiv b \pmod{n}$ (read "a is congruent to b mod n") if $n \mid a - b$.

Of course, $n \mid a - b$ means that there exists an integer k such that $a - b = nk$, which means you can read off "$a \equiv b \pmod{n}$" as "$a = b + nk$". We can use this to show that $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.

Nicely enough, we can endow the integers mod n with the structure of addition and multiplication:

Theorem 1.3. Let $n > 2$ be a positive integer. Then, given integers a, b, c, and d satisfying $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, we have

$$a + c \equiv b + d \pmod{n}$$
$$ac \equiv bd \pmod{n}.$$

The upshot of this is that if we know that two numbers have the same remainder upon division by n, then we know they will behave identically mod n, which means we are allowed to haphazardly replace numbers with any congruent numbers when working modulo n.

Proof of Theorem 2.3. Both parts of the theorem use the same idea: write $a = b + nk$ and $c = d + n\ell$. Then, for the first part,

$$a + c = b + d + nk + n\ell = b + d + n(k + \ell),$$

which means that $a + c \equiv b + d \pmod{n}$ since $a + c$ and $b + d$ differ by a multiple of n. For the second part,

$$ac = (b + nk)(d + n\ell) = bd + nk + n\ell + n^2k\ell = bd + n(k + \ell + nk\ell),$$

so ac and bd also differ by a multiple of n and thus $ac \equiv bd \pmod{n}$. □

Of course, since we can work with negative integers mod n, we can also subtract by "adding negative numbers," so we now have access to the operations of addition, subtraction, and multiplication.

Exercise 1.1. Show that exponentiation also behaves nicely in that if $a \equiv b \pmod{n}$, then

$$a^k \equiv b^k \pmod{n}$$

for all positive integers k.

Proof. Note that we can factor $a^k - b^k$ as

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + a^2b^{k-3} + ab^{k-2} + b^{k-1}).$$

The second product must be an integer, so denote it as M. Since $a \equiv b \pmod{n}$, we know that $a - b = jn$ for some integer j, so $a^k - b^k = (jn)M \implies a^k - b^k \equiv 0 \pmod{n} \implies a^k \equiv b^k \pmod{n}$. □

Remark 1.4. There are many other ways to prove this! Here are two of them, for those interested:

1. Since $a = b + jn$, $a^k = (b+jn)^k$. If we expand this out, every term will have a factor of n (and thus be congruent to 0 mod n) except for the last term, b^k. Therefore, $a^k \equiv 0 + 0 + \cdots + 0 + b^k \equiv b^k \pmod{n}$.
2. Since $a \equiv b \pmod{n}$, we know that:

$$\begin{aligned} a^2 &\equiv a^1 \cdot a \equiv b^1 \cdot b \equiv b^2 \pmod{n} \\ a^3 &\equiv a^2 \cdot a \equiv b^2 \cdot b \equiv b^3 \pmod{n} \\ a^4 &\equiv a^3 \cdot a \equiv b^3 \cdot b \equiv b^4 \pmod{n} \end{aligned}$$

...and so on for all positive integers k.

We can use the properties we've learned so far, along with some facts about divisibility, to solve the following problem:

Problem 1.5 (Eötvös Mathematical Competition 1899, Problem 3)

Prove that $A = 2903^n - 803^n - 464^n + 261^n$ is divisible by 1897 for any natural number n.

2 But wait, what about division?

Addition, subtraction, and multiplication all behave nicely with integers, since combining any two integers via those operations will result in another integer. Division, however, requires more careful treatment, since we have no conception of what a "rational number mod n" is.

The point of division in, say, the rational numbers or real numbers is to undo multiplication: namely, multiplying by x and then by x^{-1} (whenever $x \neq 0$) should amount to doing nothing. We want to be able to do something similar when working mod n.

Definition 2.1 — We say that an **inverse mod n** of a number a is an integer a^{-1} such that

$$(a)(a^{-1}) \equiv 1 \pmod{n}.$$

The inverse is also often written $\frac{1}{a}$, but we will mostly avoid that notation in this section to emphasize that a^{-1} is an integer.

This definition of inverses is analogous to that of multiplicative inverses in the real numbers (such as $\sqrt{3}^{-1} = \frac{1}{\sqrt{3}}$, and modular inverses do retain some useful properties of their more familiar analogues:

Theorem 2.2. If a has an inverse mod n, then this inverse is unique mod n (i.e. if b and c are both inverses of a mod n, then $b \equiv c \pmod{n}$). Additionally, the inverse of a^{-1} is a.

Proof. Suppose that there exist b and c such that

$$ab \equiv ac \equiv 1 \pmod{n}.$$

Then,

$$b \equiv b \cdot ac = ab \cdot c \equiv c \pmod{n},$$

so a^{-1} is unique mod n.

For the second part, a is an integer such that $(a^{-1})(a) \equiv 1 \pmod{n}$, so a is an inverse of a^{-1} mod n. □

The upshot of this is that we can unambiguously say "the inverse of a mod n," at least when the inverse exists. However, we are not always guaranteed existence. For example, 2 does not have an inverse mod 6, since $2k$ always has an even (and thus non-one) remainder when divided by 6. In general, we can describe when a number cannot an inverse as follows:

Theorem 2.3. Suppose $\gcd(a, n) > 1$. Then, a does not have an inverse mod n.

Proof. Let $g = \gcd(a, n)$, and write $a = a'g$ and $n = n'g$. Suppose a has some inverse a^{-1}; since $aa^{-1} \equiv 1 \pmod{n}$, we can write $1 = aa^{-1} + kn$ for some integer k. But then

$$1 = aa^{-1} + kn = (a'g)(a^{-1}) + k(n'g) = g(a'a^{-1} + kn'),$$

meaning g divides 1. Since $g > 1$, this is impossible and thus a contradiction, meaning that a cannot have an inverse mod n.

□

The natural question now is whether the other direction of this is true: if a and n are relatively prime, then must a have an inverse mod n? Luckily, the answer is yes!

Theorem 2.4. If $\gcd(a, n) = 1$, then a has an inverse mod n.

Proof. Let R be the set of positive integers less than n and relatively prime to n. Then, consider the set aR, obtained by multiplying each element of R by a and then replacing this element with its remainder upon division by n. For example, when $a = 2$ and $n = 9$, $R = \{1, 2, 4, 5, 7, 8\}$ and $aR = \{2, 4, 8, 1, 5, 7\}$. Notice how R and aR seem to be identical?

It turns out that this is true in general!

We know that every element of R is relatively prime to n, and a is relatively prime to n, so every element of aR must be relatively prime to n. Every element of aR also must be a positive integer less than n, so aR must be a subset of R. We're now much closer to proving that $aR = R$.

To finish, we need to prove that the map sending x to ax never sends two elements of R to two numbers that are congruent mod n.

Suppose x and y are elements of R such that $x \not\equiv y \pmod{n}$, and suppose that $ax \equiv ay \pmod{n}$. Then, $a(x - y)$ is a multiple of n by our definition of modular equivalence. Now, since a is relatively prime to n, this forces $n \mid x - y$; however, because x and y are strictly between 0 and n, we see that $0 < |x - y| < n$, meaning that divisibility is impossible.

This proves that every element of aR corresponds to exactly one element of R, so aR and R have the same number of elements. Since all the elements of aR are elements of R, them having the same number of elements means that $aR = R$.

Since $aR = R$, aR must contain 1, so some number $b \in R$ must have multiplied with a to make a 1. We have found an inverse of a mod n. □

Exercise 2.1. Verify that given any prime p, every non-multiple of p has an inverse mod p.

Exercise 2.2. Show that "fractions" work as normal as long as denominators are relatively prime to n; that is, if $\gcd(b, n) = \gcd(d, n) = 1$, then

$$\frac{a}{b} + \frac{c}{d} \equiv \frac{ad + bc}{bd} \pmod{n}.$$

In the notation we've been using so far, this is better written as

$$a \cdot b^{-1} + c \cdot d^{-1} \equiv (ab + bc)(bd)^{-1} \pmod{n}.$$

Exercise 2.2 shows that we can often talk about rational numbers when working mod n; in particular, if $\frac{a}{b} \equiv 0 \pmod{n}$, then, when written in simplest form, the numerator of $\frac{a}{b}$ must be a multiple of n.

Finally, here's a quick application of the theory developed in this section:

Theorem 2.5 (Wilson's theorem)**.** Show that, if p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Let's actually compute $10! \pmod{11}$. Instead of just multiplying, we can pair off inverses, since they cancel each other out:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 1 \cdot 10 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \equiv 10 \pmod{11}$$

After pairing off, it turns out that 1 and 10 are the only unpaired numbers. Why? Well, if a number is unpaired, it must be its own inverse. Suppose in general that a is its own inverse mod p. Then

$$p \mid a^2 - 1 = (a+1)(a-1),$$

so p either divides $a + 1$ or $a - 1$ implying that $a \equiv \pm 1 \pmod{p}$ (as expected, 1 and 10 are $\pm 1 \pmod{11}$).

In other words, when pairing off inverses mod p among 1, 2, ..., $p - 1$, we will form $\frac{p-3}{2}$ pairs and have 1 and $p - 1$ left over, so

$$(p-1)! \equiv 1^{(p-3)/2} \cdot 1 \cdot (p-1) \equiv p - 1 \equiv -1 \pmod{p}.$$

Note: This argument technically assumes that -1 and 1 are not congruent mod p, which is true for almost all numbers... except for 2. We need to check the case where $p = 2$ separately — fortunately, it isn't too hard. Remember this for the future — look out for special cases where the assumptions you've made may not hold, and be sure to check those special cases separately. □

2.1 Patching up some holes

You may have noticed that in our proof of Theorem 2.4, we showed that $a(x - y)$ was a multiple of n, then claimed that since a and n were relatively prime it must be the case that $x - y$ was a multiple of n. This seems reasonable, but we technically don't know that it's true. In this section, we'll build up the theory that justifies this using a result known as Bézout's Lemma.

Theorem 2.6 (Bézout's Lemma)**.** Without using modular inverses, prove that for any integers a and b there exist integers x and y such that $ax + by = \gcd(a, b)$.

Proof. We'll focus on the special case of this where a and b are relatively prime. Let $S = \{ax + by \mid x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$. We want to show that $1 \in S$:

Let d be the smallest number in S, so $d = ak + bj$. We know that d must have a remainder when divided by a, i.e. there exists an integer c between 0 and d such that

$$a = \ell d + c$$

for some integer ℓ. But then

$$c = a - \ell d = a - \ell(ak + bj) - a = a(1 - \ell k) + b(-\ell j)$$

Since $c < d$ and d is the smallest element of S, c cannot be in S. The only way for this to be true is if $c = 0$, as S must only contain positive integers. Thus, $a = \ell d + c = \ell d$, so d divides a.

Notice that we could have replaced a with b in every step of this proof, and we would get the same result! This means that d must divide b as well. But since a and b are relatively prime, the only number that divides both of them is 1, meaning that $d = 1$. Therefore, 1 must be in S. □

> **Exercise 2.3.** Finish the proof of Bézout's Lemma by showing it is true for any pair of integers (hint: use the result from the relatively prime case we just proved).

Bézout's Lemma is very useful because it allows us to understand the structure of multiplication with regards to divisibility. In particular, we can prove the following theorem, known as Euclid's Lemma:

> **Theorem 2.7** (Euclid's Lemma)**.** If a prime p divides the product ab, where a and b are integers, then either p divides a or p divides b, or both.

Proof. We'll do this by contradiction. Assume p does not divide either a or b. Since p does not divide a, p and a must be relatively prime, so we can apply Bézout's Lemma here! We know that there must exists integers x and y such that

$$px + ay = 1$$

Now, multiply by b on both sides to get

$$b = pbx + aby$$

Since $p \mid ab$, $ab = kp$ for some integer k, so

$$b = pbx + kpy = p(bx + ky)$$

This means that p divides b, a contradiction. Therefore, p must divide at least one of a and b, which is what we claimed. □

This is a very fundamental result! As we stated before, we implicitly used it when discussing modular inverses, but you likely also used it implicitly in Problem 1.4.

However, our claim in the previous section was a bit more general — in our case, we didn't know if n was prime.

> **Exercise 2.4.** Extend Euclid's Lemma to prove that if n divides ab, where a and b are integers and $\gcd(a, n) = 1$, then n divides b.

Doing this exercise resolves the assumption we made in our proof of Theorem 2.4.

Remark 2.8. A few of you may have noticed that by using Bézout's Lemma directly, it's fairly easy to find a much faster proof of Theorem 2.4 than the one we presented. Our proof is more convoluted mostly because the structure we developed in it will allow us to prove later theorems far more quickly and because it minimizes the intuitive reliance on Bézout's Lemma (which is more difficult to visualize), but if we were simply focused on understanding inverses we would use a different proof.

3 Chinese Remainder Theorem

We often want to find out which numbers satisfy two different modular equivalences; for example, characterizing which numbers a satisfy both $a \equiv 2 \pmod 3$ and $a \equiv 4 \pmod 7$. If we list out the integers from 1 through 21, we can see that exactly one of these numbers (11) satisfies both congruences.

In general, we can make the following statement:

Theorem 3.1 (Chinese Remainder Theorem)**.** Given relatively prime integers m and n and integers a and b, the system of equations

$$\begin{aligned} k &\equiv a \pmod m \\ k &\equiv b \pmod n \end{aligned}$$

is satisfied by exactly one integer mod mn (i.e. a solution to the system exists, and if k and j are both solutions then $k \equiv j \pmod{mn}$).

Proof. First, we'll prove that if we have two solutions to this system, then they must be congruent mod mn:

Suppose k and j are two solution to the system. Thus

$$k \equiv j \equiv a \pmod m \text{ and } k \equiv j \equiv b \pmod n.$$

Then $k = j + mp$ and $k = j + nq$ for some integers p and q. This means that $mp = nq$, so $m \mid nq$. Since m and n are relatively prime, this implies that $m \mid q$, so $q = mr$ for some integer r. But then

$$k = j + nq = j + nmr \implies k \equiv j \pmod{mn}.$$

Now, we'll prove that there is a solution to the system in the first place:

We want to find an integer k such that

$$k = a + mp = b + nq$$

for some integers p and q. This is equivalent to $mp = (b-a) + nq$, or that $mp \equiv b - a \pmod n$. Since m and n are relatively prime, by Theorem 3.4 we can find an inverse of m mod n. Call this inverse m^{-1}.

Now, let $p = (b-a)m^{-1}$. By our definition of an inverse,

$$mp \equiv m(m^{-1}(b-a)) \equiv 1 \cdot (b-a) \equiv b - a \pmod n,$$

which is what we wanted to prove. This means that we've found a solution to this system. □

Another way to think about this construction is as follows: we know that we can find an integer ℓ such that $m \cdot \ell \equiv 1 \pmod n$. If we let $k = a + m\ell(b-a)$, then

1. $k \equiv a + m\ell(b-a) \equiv a \pmod m$
2. $k \equiv a + m\ell(b-a) \equiv a + 1 \cdot (b-a) \equiv a + b - a \equiv b \pmod n$

so k satisfies the system of equivalences.

Exercise 3.1. Let $a_1, a_2, \dots, a_n$ be integers such that each pair of these integers is relatively prime, and let $N = a_1 \cdot a_2 \cdots a_n$. Prove that given integers $b_1, b_2, \dots, b_n$, the system of equations

$$\begin{aligned} k &\equiv b_1 \pmod{a_1} \\ k &\equiv b_2 \pmod{a_2} \\ &\dots \\ k &\equiv b_n \pmod{a_n} \end{aligned}$$

is satisfied by exactly one integer mod N.

4 Fermat's little theorem and Euler's Theorem

If we look at successive powers of 2 mod 7, we can see that there's a pattern that cycles after a set interval:

$$\begin{aligned} 2^1 &\equiv 2 \pmod 7 \\ 2^2 &\equiv 4 \pmod 7 \\ 2^3 &\equiv 1 \pmod 7 \\ 2^4 &\equiv 2 \pmod 7 \\ 2^5 &\equiv 4 \pmod 7 \\ 2^6 &\equiv 1 \pmod 7 \\ 2^7 &\equiv 2 \pmod 7 \\ &\dots \end{aligned}$$

We can also find cycles for other numbers mod 7, using arrows to represent the next power:

$$\begin{aligned} &1 \to 1 \to 1 \to 1 \to 1 \to 1 \to 1 \to \cdots \\ &3 \to 2 \to 6 \to 4 \to 5 \to 1 \to 3 \to \cdots \\ &6 \to 1 \to 6 \to 1 \to 6 \to 1 \to 6 \to \cdots \end{aligned}$$

Notice that the sixth number of each of these sequences turns out to be 1!

Exercise 4.1. Suppose $\gcd(a, n) = 1$. Why in general should the function $f(x)$, defined as the remainder of a^x when divided by n, be periodic? That is, argue that there exists some positive integer p for which $f(x) = f(x + t)$ is true for all nonnegative integers x.

Our goal is to try figuring out some information about what this period t is, and that is exactly what Fermat's little theorem promises us.

Theorem 4.1 (Fermat's Little Theorem)**.** Let p be a prime and let a be an integer that is not a multiple of p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Consider the set of integers $\{a, 2a, 3a, \dots, (p-1)a\}$. In Theorem 3.4, we proved that this set has one number congruent to each of $1, 2, 3, \dots, p-1$ mod p. Therefore

$$\left(\prod_{k=1}^{p-1} k\right)\left(a^{p-1}\right) \equiv \prod_{k=1}^{p-1}(ak) \equiv \prod_{k=1}^{p-1} k \pmod{p}$$

So $a^{p-1} \equiv 1 \pmod{p}$. □

Fermat's Little Theorem tells us that the cycle length is forced to be at most $p-1$ (can you say something stronger?).

We can also extend Fermat's Little Theorem to composite numbers as follows:

Theorem 4.2 (Euler's Theorem)**.** Let n be a natural number, let a be an integer relatively prime to n, and let $\phi(n)$ be the number of integers between 0 and n that are relatively prime to n. Then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Try to show this yourself — the proof is analogous to that of Fermat's Little Theorem (in fact, Fermat's Little Theorem is the special case of Euler's Theorem for prime numbers).

Finally, a neat practice problem:

Problem 4.3

Determine all positive integers relatively prime to all terms of the infinite sequence defined by

$$a_n = 2^n + 3^n + 6^n - 1, \quad n \geq 1.$$