Fractions in Modular Arithmetic

Rishabh Das

New York City Math Team

1 Multiplicative Inverses

1.1 Definitions

Definition (Multiplicative Inverse)

When $\gcd(a, n) = 1$, we say that the *multiplicative inverse of a mod n*" is the number b such that

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

We then write $b \equiv a^{-1} \pmod{n}$ or $b \equiv \frac{1}{a} \pmod{n}$.

As an example, we say $\frac{1}{2} \equiv 13 \pmod{25}$ since $2 \cdot 13 \equiv 1 \pmod{25}$.
Note that $x \cdot a^{-1} \equiv x \cdot \frac{1}{a} \pmod{n}$ can also be written as

$$\frac{x}{a} \pmod{n}.$$

1.2 Existence and Non-Existence

Proof (Proof For Existence)

Let $\{n_1, n_2, \ldots, n_{\varphi(n)}\}$ be the set of positive integers less than or equal to n that are relatively prime to n. Note that an_i is relatively prime to n. Also note that if $an_i \equiv an_j \pmod{n}$:

$$an_i \equiv an_j \pmod{n} \implies a(n_i - n_j) \equiv 0 \pmod{n}.$$

Since $\gcd(a, n) = 1$, we must have $n_i - n_j \equiv 0 \pmod{n}$. Since $1 \leq n_i, n_j \leq n$, this implies $n_i = n_j$, or $i = j$. Thus, $\{n_1, n_2, \ldots n_{\varphi(n)}\} \equiv \{an_1, an_2, \ldots an_{\varphi(n)}\} \pmod{n}$.
Since $n_1 = 1$, this means that $an_i \equiv 1 \pmod{n}$ for some i. Thus, $n_i \equiv a^{-1} \pmod{p}$.

Thus, we have shown that when $\gcd(a, n) = 1$, the multiplicative inverse of a mod p exists. We now show that when $\gcd(a, n) \neq 1$, the multiplicative inverse of a mod p doesn't exist.

Proof (Proof For Non-Existence)

We do a proof by contradiction. Suppose $\gcd(a, n) \neq 1$ and $ab \equiv 1 \pmod{n}$. Then there exists a c such that $ab - nc = 1$. Note that $\gcd(a, n) \mid a$ and $\gcd(a, n) \mid n$, so $\gcd(a, n) \mid ab - nc = 1$. Thus, $\gcd(a, n)$ must be equal to 1, a contradiction.

Warning

Whenever using multiplicative inverses and/or fractions mod n for any n, make sure that the denominator is relatively prime to n.

2 Computation With Fractional Mods

From here on out, we assume any denominators are relatively prime to n, where we are taking everything mod n.

2.1 Multiplication

Fractions modulo n work exactly how we would like/expect them to.

Lemma (Multiplying Fractions mod n)
We have
$$\frac{a}{c} \cdot \frac{b}{d} \equiv \frac{ab}{cd} \pmod{n}.$$

Proof. The left side is just
$$\left(a \cdot \frac{1}{c}\right) \cdot \left(b \cdot \frac{1}{d}\right) \equiv ab \cdot \frac{1}{c} \cdot \frac{1}{d} \pmod{n}$$
while the right side is
$$(ab) \cdot \frac{1}{cd} \pmod{n}.$$
Thus, if we show $\frac{1}{c} \cdot \frac{1}{d} \equiv \frac{1}{cd}$, then we would be done. Let $\frac{1}{c} \equiv x \pmod{n}$ and $\frac{1}{d} \equiv y \pmod{n}$. Then
$$\frac{1}{c} \cdot \frac{1}{d} \equiv xy \pmod{n}.$$
We are left to show that $xy \equiv \frac{1}{cd} \pmod{n}$, or that $(xy)(cd) \equiv 1 \pmod{n}$. However, note that
$$(xy)(cd) \equiv (xc)(yd) \equiv 1 \cdot 1 \equiv 1 \pmod{n},$$
so we are done. $\square$

As an example, we see that
$$\frac{7}{2} \cdot \frac{8}{14} \equiv \frac{7 \cdot 8}{2 \cdot 14} \equiv 2 \pmod{11}.$$
In fact, what we were taking the expression modulo didn't matter, as long it is coprime to 2 and 14; the result will always be 2.
If we wanted to check this, we could note
$$\frac{7}{2} \equiv 7 \cdot \frac{1}{2} \equiv 7 \cdot 6 \equiv 42 \equiv 9 \pmod{11}$$
while
$$\frac{8}{14} \equiv \frac{4}{7} \equiv 4 \cdot \frac{1}{7} \equiv 4 \cdot 8 \equiv 32 \equiv 10 \pmod{11},$$
so the product of the two is
$$\frac{7}{2} \cdot \frac{8}{14} \equiv 9 \cdot 10 \equiv 90 \equiv 2 \pmod{11}.$$
However, note how much more efficient it is to just multiply the fractions!

Exercise 1. Show that we can reduce fractions mod n as well.

2.2 Addition

Surprisingly, fractions modulo n work exactly how we would like them to.

Lemma (Adding Fractions mod n)

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

Proof. Again let $\frac{1}{c} \equiv x \pmod{n}$ and $\frac{1}{d} \equiv y \pmod{n}$. We have already shown above that $\frac{1}{cd} \equiv xy \pmod{n}$. Thus, the right side is
$$(ad+bc)\cdot\frac{1}{cd} \equiv (ad+bc)\cdot(xy) \equiv (ax)(dy) + (by)(cx) \equiv (ax)\cdot 1 + (by)\cdot 1 \equiv ax + by \equiv a\cdot\frac{1}{c} + b\cdot\frac{1}{d}$$
$$\equiv \frac{a}{c} + \frac{b}{d} \pmod{n}$$
as desired. □

2.3 Exercises

Exercise 1. Compute $13^9 \pmod{25}$.

Exercise 2. Compute $\left(\frac{1}{3} + \frac{1}{4}\right)\cdot\frac{8}{3} \pmod{17}$.

Exercise 3. Compute $2020^{39} \pmod{41}$.

3 An Example of the Power of Fractional Mods

Here is an example from the 2005 IMO.

Example (2005 IMO/4)

Determine all positive integers relatively prime to all the terms of the infinite sequence
$$a_n = 2^n + 3^n + 6^n - 1,\ n \geq 1.$$

Solution. We claim that only 1 is relatively prime to each term of the sequence, which it clearly is. To show no other positive integer works, we will show that any prime p divides some term of the sequence.
If $p = 2$ or $p = 3$, then take $n = 2$. This means
$$a_2 = 2^2 + 3^2 + 6^2 - 1 = 48,$$
a multiple of both 2 and 3. Otherwise, assume $p \geq 5$.
We will pick our n very cleverly. We will pick $n = p - 2$. Note that by Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$ for all a not a multiple of p. However, we can rewrite this as
$$a^{p-2} \equiv \frac{1}{a} \pmod{p}$$
for all a not a multiple of p. Thus, when we take $n = p - 2$, we see
$$a_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \equiv 0 \pmod{p},$$
so a_{p-2} is a multiple of p.
Thus, for any prime p, there is a term of the sequence that is a multiple of p, so no positive integer other than 1 can be relatively prime to all terms in the sequence.

Exercise

Why are the cases of $p = 2$ and $p = 3$ separated from the rest of the primes in the above proof?

4 Problems

Enjoy!

Problem 1 (2012 PUMaC Individual Finals)**.** Let p be a prime number greater than 5. Prove that there exists a positive integer n such that p divides $20^n + 15^n - 12^n$.

Problem 2 (2019 NEMO Individual/14)**.** Find all primes $p \geq 5$ such that p divides $(p-3)^{p-3} - (p-4)^{p-4}$.

Problem 3 (2011 PUMaC Number Theory/3)**.** What is the sum of all primes p such that $7^p - 6^p + 2$ is divisible by 43?

Problem 4 (2020 HMMT February Algebra and Number Theory/7)**.** Find the sum of all positive integers n for which

$$\frac{15 \cdot n!^2 + 1}{2n - 3}$$

is an integer.