

# Modular Arithmetic

Dennis Chen

NPU

This unit can be described in three words: Take mod something.

## § 1 Divisibility, GCD, and LCM

---

### § 1.1 Divisibility

Divisibility seems like such a simple idea; if  $a$  divides  $b$  (which is denoted as  $a \mid b$ ) then  $\frac{b}{a}$  must be an integer. However, this falls apart once we start introducing 0 into the equation. For the purpose of letting our definition stay consistent when 0 is introduced, we say that integers  $a \mid b$  if there exists integer  $c$  such that  $ac = b$ . (We specify  $a, b$  as integer for our useful results to stay consistent.)

This means that all  $a \mid 0$  and  $0 \nmid b$  for all  $b \neq 0$ , implying  $0 \mid 0$ . (Verify this for yourself.)

### § 1.2 Results

Our rigorous definition of divisibility leaves us with some results that we can prove which we would not have obtained using the intuitive method.

#### Fact 1 (Divisibility Results)

1. If  $a \mid b$  and  $b \mid c$  then  $a \mid c$ . (This may be referred to as the "chain rule" of divisibility.)
2. If  $a \mid b$  then  $a \mid bc$  for all integer  $c$ .
3. If  $a \mid b$  and  $a \mid c$ , then  $a \mid b + c$  and  $a \mid b - c$ .

### § 1.3 GCD and LCM

**Definition 1** We define  $\gcd(a_1, a_2 \dots a_n)$  as the largest positive integer such that

$$\gcd(a_1, a_2 \dots a_n) \mid a_1, a_2 \dots a_n.$$

**Definition 2** We define  $\text{lcm}(a_1, a_2 \dots a_n)$  as the smallest **positive** integer such that

$$a_1, a_2 \dots a_n \mid \text{lcm}(a_1, a_2 \dots a_n).$$

As an exercise, list the divisors of 0, the numbers that 0 divides, and find  $\gcd(0, 8)$ .

## § 2 Modular Arithmetic

---

**Definition 3** We say  $a \equiv b \pmod{n}$  if and only if  $n \mid a - b$ .

The intuitive way to think about this is that  $a$  and  $b$  have the same remainder when divided by  $n$ . (Remember that negative numbers also have a remainder when divided.)

That is all.

## § 3 Fermat's Little Theorem

---

Often in number theory problems we will want to take some number to some large power and find its remainder when divided by another number. Fermat's Little Theorem provides a way to make this calculation much easier.

**Theorem 1 (Fermat's Little Theorem)** Consider a prime  $p$ . For relatively prime  $a, p$ ,  $a^{p-1} \equiv 1 \pmod{p}$ .

There are two proofs for this theorem. We present the induction proof first because it requires the least amount of ingenuity.

---

**Proof 1 (Induction):** For the inductive proof, we prove that  $a^p \equiv a \pmod{p}$  instead.

This is obviously true for the base case  $a = 1$ .

Now assume that this is true for  $a = n$ . Then

$$(n+1)^p \equiv n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + 1.$$

But notice that  $\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$  are all divisible by  $p$ , so

$$n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + 1 \equiv n^p + 1 \equiv n + 1,$$

as desired. ■

---

The rearrangement proof requires a little bit more creativity and is more aesthetic. It can also be generalized to Euler's Theorem, where the first proof cannot.

---

**Proof 2 (Rearrangement):** Notice that  $a, 2a, 3a, \dots, a(p-1)$  is a rearrangement of  $1, 2, 3, \dots, p-1$  taken mod  $p$ . We prove this by contradiction. Assume that there are two integers such that  $ax \equiv ay \pmod{p}$ . Since  $\gcd(a, p) = 1$ , we can divide both sides by  $a$  to yield  $x \equiv y$ . But this is obviously not possible. Thus, contradiction.

This implies that  $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$ . As  $\gcd(p, (p-1)!) = 1$ , we can divide both sides by  $(p-1)!$  to get  $1 \equiv a^{p-1} \pmod{p}$ , as desired. ■

---

## § 4 The Totient Function

---

Now we take a look at Euler's Totient Function.

**Definition 4** We define  $\phi(n)$  to be the number of positive integers less than or equal to  $n$  that are also relatively prime to  $n$ .

**Theorem 2 (Multiplicity)** For relatively prime  $m, n$ ,  $\phi(m) \cdot \phi(n) = \phi(mn)$ .

**Proof:** This is obvious by the product formula. ■

**Theorem 3 (Euler's Totient Theorem)** For relatively prime  $a, n$ ,  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

**Proof:** This is very similar to the rearrangement proof for Fermat's Little Theorem.<sup>1</sup>

Let the set of positive integers less than and relatively prime to  $n$  be  $x_1, x_2, \dots, x_{\phi(n)}$ . Then note that  $ax_1, ax_2, \dots, ax_{\phi(n)}$  is a rearrangement of  $x_1, x_2, \dots, x_{\phi(n)}$ .

We proceed by contradiction. Assume that there are two integers such that  $ax \equiv ay \pmod{n}$ . Since  $\gcd(a, n) = 1$ , we can divide both sides by  $a$  to yield  $x \equiv y$ . But this is obviously not possible. Thus, contradiction.

This implies that  $x_1 x_2 \dots x_{\phi(n)} \equiv (x_1 x_2 \dots x_{\phi(n)}) a^{\phi(n)} \pmod{n}$ . Dividing both sides by  $x_1 x_2 \dots x_{\phi(n)}$  yields  $a^{\phi(n)} \equiv 1 \pmod{n}$ , as desired. ■

Also notice that Fermat's is just special case of Euler's.

**Theorem 4 (Product Formula)** For  $n = p_1^{e_1} \cdot p_2^{e_2} \dots p_n^{e_n}$ ,  $\phi(n) = n \frac{p_1-1}{p_1} \cdot \frac{p_2-1}{p_2} \dots \frac{p_n-1}{p_n}$ .

**Proof:** Let  $n = \prod_{i=1}^x p_i^{e_i}$ .

We complementary count.

Note that the amount of numbers such that  $\gcd(j, n) > 1$  can be counted by PIE. Let  $|P_i|$  be the set of numbers from 1 to  $n$  such that  $p_i | n$ . Then by PIE,

$$\left| \bigcup_{i=1}^x P_i \right| = \sum_{i=1}^x (-1)^{i+1} \sum_{\text{sym}} \left| \bigcap_{j=1}^i P_j \right|.$$

We induct. The base case of  $x = 1$  is obvious.

Let  $\prod_{i=1}^x p_i^x = n$ .

Then we see that

$$\begin{aligned} \left| \bigcup_{i=1}^{x+1} P_i \right| &= \sum_{i=1}^{x+1} (-1)^{i+1} \sum_{\text{sym}} \left| \bigcap_{j=1}^i P_j \right| \\ \left| \bigcup_{i=1}^{x+1} P_i \right| &= \sum_{i=1}^x (-1)^{i+1} \sum_{\text{sym}} \left| \bigcap_{j=1}^i P_j \right| + \sum_{i=1}^x (-1)^i |P_{x+1} \cap \bigcap_{j=0}^i P_j| + |P_{x+1}|. \end{aligned}$$

Note that  $\sum_{i=1}^x (-1)^{i+1} \sum_{\text{sym}} \left| \bigcap_{j=1}^i P_j \right| = p_{x+1}^{e_{x+1}} (n - \phi(n))$ , as we assume this holds for  $x$  and we are just multiplying by  $p_{x+1}^{e_{x+1}}$ , which is relatively prime to  $n$ . Also,

$$\sum_{i=0}^x (-1)^i |P_{x+1} \cap \bigcap_{j=0}^i P_j| = -p_{x+1}^{e_{x+1}-1} (n - \phi(n)),$$

<sup>1</sup>So similar, in fact, that I copy-pasted the proof for Fermat's and made minor adjustments.

as we multiply by  $p_{x+1}^{e_{x+1}}$  but also require the new numbers to be divisible by  $p_{x+1}$ .<sup>2</sup> Also,  $|P_{x+1}| = p_{x+1}^{e_{x+1}-1} \phi(n)$ .  
So

$$\begin{aligned} \left| \bigcup_{i=1}^{x+1} P_i \right| &= p_{x+1}^{e_{x+1}} (n - \phi(n)) - p_{x+1}^{e_{x+1}-1} (n - \phi(n)) + p_{x+1}^{e_{x+1}-1} n \\ \left| \bigcup_{i=1}^{x+1} P_i \right| &= np_{x+1}^{e_{x+1}} - p_{x+1}^{e_{x+1}-1} (p-1) \phi(n), \end{aligned}$$

and

$$\phi(np_{x+1}^{e_{x+1}}) = np_{x+1}^{e_{x+1}} - \left| \bigcup_{i=1}^{x+1} P_i \right| = p_{x+1}^{e_{x+1}-1} (p-1) \phi(n).$$

■

The proof looks bad but is essentially just brute-force counting the number of relatively numbers with PIE.

## § 5 Modular Inverses

In normal arithmetic, we define  $a \cdot a^{-1} = 1$ . We can do something similar in modular arithmetic.

**Definition 5** We define  $a^{-1}$  to be the number mod  $n$  such that  $a \cdot a^{-1} \equiv 1 \pmod{n}$ . We say that  $a^{-1}$  is the inverse of  $a \pmod{n}$ .

Of course, the modular inverse is defined if and only if  $\gcd(a, n) = 1$ .

## § 6 Wilson's Theorem

Factorials rarely appear in number theory (at least for the AMCs and the AIME). But Wilson's Theorem is still one of the standard tools you need to have at your disposal.

**Theorem 5 (Wilson's Theorem)** For prime  $p$ ,

$$(p-1)! \equiv -1 \pmod{p}.$$


**Proof:** Notice that the numbers  $2, 3, 4, \dots, p-2$  all have modular inverses. In addition, modular inverses come in pairs. Since  $p$  is odd (the case where  $p = 2$  is very easy to deal with), then the modular inverses all multiply to 1. This leaves us with  $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$ , as desired. ■


As an exercise, prove that  $(p-2)! \equiv 1 \pmod{p}$ . (This is quite easy to do directly with Wilson's.)

<sup>2</sup>The factor of  $-1$  comes because we added an extra term, multiplying everything by  $-1$ .


## §7 Problems


---

Minimum is [54]. Problems with the  symbol are required.


[1]  **Problem 1** Find the inverse of 2 (mod  $p$ ) for odd prime  $p$  in terms of  $p$ .


[1]  **Problem 2** Find the remainder of  $97!$  when divided by 101.


[1]  **Problem 3** (Find the remainder of  $(p-2)!$  when divided by  $p$ , provided that  $p$  is prime.)


[2]  **Problem 4** (AMC 12A 2003/18) Let  $n$  be a 5-digit number, and let  $q$  and  $r$  be the quotient and the remainder, respectively, when  $n$  is divided by 100. For how many values of  $n$  is  $q+r$  divisible by 11?

[2]  **Problem 5** (MAST Diagnostic 2020) How many integer values of  $1 \leq x \leq 100$  makes  $x^2 + 8x + 5$  divisible by 10?

[2]  **Problem 6** (1001 Problems in Number Theory) For which positive integers  $n$  is it true that  $1 + 2 + \cdots + n \mid 1 \cdot 2 \cdots n$ ?


[2]  **Problem 7** What is the residue of  $\frac{1}{1 \cdot 2} \cdot \frac{1}{2 \cdot 3} \cdots \frac{1}{11 \cdot 12}$  (mod 13)?


[2]  **Problem 8** (AMC 10A 2020/18) Let  $(a, b, c, d)$  be an ordered quadruple of not necessarily distinct integers, each one of them in the set  $0, 1, 2, 3$ . For how many such quadruples is it true that  $a \cdot d - b \cdot c$  is odd? (For example,  $(0, 3, 1, 1)$  is one such quadruple, because  $0 \cdot 1 - 3 \cdot 1 = -3$  is odd.)


[3]  **Problem 9** (AMC 10B 2018/16) Let  $a_1, a_2, \dots, a_{2018}$  be a strictly increasing sequence of positive integers such that

$$a_1 + a_2 + \cdots + a_{2018} = 2018^{2018}.$$


What is the remainder when  $a_1^3 + a_2^3 + \cdots + a_{2018}^3$  is divided by 6?


[3]  **Problem 10** (PUMaC 2018) Find the number of positive integers  $n < 2018$  such that  $25^n + 9^n$  is divisible by 13.


[3]  **Problem 11** Prove  $\phi(n)$  is composite for  $n \geq 7$ .


[3]  **Problem 12** (AMC 10B 2019/14) The base-ten representation for  $19!$  is  $121,6T5,100,40M,832,H00$ , where  $T$ ,  $M$ , and  $H$  denote digits that are not given. What is  $T + M + H$ ?


[4]  **Problem 13** Find the remainder of  $5^{31} + 5^{17} + 1$  when divided by 31.

[4]  **Problem 14** Prove that the equation  $x^2 + y^2 + z^2 = x + y + z + 1$  has no solutions over the rationals.

[4]  **Problem 15** (MAST Diagnostic 2021) Find the remainder of  $(1^3)(1^3 + 2^3)(1^3 + 2^3 + 3^3) \cdots (1^3 + 2^3 + 3^3 + \cdots + 99^3)$  when divided by 101.

[6]  **Problem 16** Prove that for all prime  $p \geq 5$ , we have  $p^2 \mid (p-1)! \left( \sum_{i=1}^{p-1} \frac{1}{i} \right)$ .

[6]  **Problem 17** (AIME 1989/9) One of Euler's conjectures was disproved in the 1960s by three American mathematicians when they showed there was a positive integer such that  $133^5 + 110^5 + 84^5 + 27^5 = n^5$ . Find the value of  $n$ .

[6]  **Problem 18** (USAMO 1979/1) Determine all non-negative integral solutions  $(n_1, n_2, \dots, n_k)$ , if any, apart from permutations, of the Diophantine equation

$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599.$$

[6] **Problem 19** (AIME II 2017/8) Find the number of positive integers  $n$  less than 2017 such that

$$1 + n + \frac{n^2}{2!} + \frac{n^3}{3!} + \frac{n^4}{4!} + \frac{n^5}{5!} + \frac{n^6}{6!}$$

is an integer.

[9] **Problem 20** (IMO 1970/4) Find all positive integers  $n$  such that the set  $\{n, n+1, n+2, n+3, n+4, n+5\}$  can be partitioned into two subsets so that the product of the numbers in each subset is equal.

[9] **Problem 21** (IMO 2005/4) Determine all positive integers relatively prime to all the terms of the infinite sequence

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

[13] **Problem 22** (AIME I 2013/15) Let  $N$  be the number of ordered triples  $(A, B, C)$  of integers satisfying the conditions

- ♦  $0 \leq A < B < C \leq 99$ ,
- ♦ there exist integers  $a, b$ , and  $c$ , and prime  $p$  where  $0 \leq b < a < c < p$ ,
- ♦  $p$  divides  $A - a$ ,  $B - b$ , and  $C - c$ , and
- ♦ each ordered triple  $(A, B, C)$  and each ordered triple  $(b, a, c)$  form arithmetic sequences.

Find  $N$ .

## §7.1 Period of a Repeating Decimal

[2] **Problem 23** The expansion of  $\frac{1}{7}$  is  $0.\overline{142857}$ , which is a repeating decimal with a 6 digit long sequence. How many digits long is the expansion of  $\frac{1}{13}$ ?

[3] **Problem 24** We define the cycle of a repeating fraction  $\frac{m}{n}$  as the minimum number  $i$  such that  $\frac{m}{n} = 0.\overline{a_1 a_2 a_3 \dots a_i}$ . Find the cycle of  $\frac{1}{23}$ .

[3] **Problem 25** (AMC 10A 2019/18) For some positive integer  $k$ , the repeating base- $k$  representation of the (base-ten) fraction  $\frac{7}{51}$  is  $0.\overline{23}_k = 0.232323\dots_k$ . What is  $k$ ?

[4] **Problem 26 (e-dchen Mock MATHCOUNTS)** What is the sum of all odd  $n$  such that  $\frac{1}{n}$  expressed in base 8 is a repeating decimal with period 4?

[6] **Problem 27** (AMC 12A 2014/23) The fraction

$$\frac{1}{99^2} = 0.\overline{b_{n-1} b_{n-2} \dots b_2 b_1 b_0},$$

where  $n$  is the length of the period of the repeating decimal expansion. What is the sum  $b_0 + b_1 + \dots + b_{n-1}$ ?

[6] **Problem 28** (AMC 12B 2016/22) For a certain positive integer  $n$  less than 1000, the decimal equivalent of  $\frac{1}{n}$  is  $0.\overline{abcdef}$ , a repeating decimal of period 6, and the decimal equivalent of  $\frac{1}{n+6}$  is  $0.\overline{wxyz}$ , a repeating decimal of period 4. Find  $n$ .