MSCM Number Theory

Alan Zhou

2024-25

Contents

1 Proving the Fundamental Theorem of Arithmetic **2**
1.1 Every positive integer is a product of primes . . . 2
1.2 The euclidean algorithm . . . 2
1.3 Bézout's lemma . . . 3
1.4 Divisibility by a prime . . . 3
1.5 Prime factorization is unique . . . 4

2 More on Modular Arithmetic **5**
2.1 Multiplicative inverses . . . 5
2.2 Linear congruences . . . 6
2.3 The Chinese remainder theorem . . . 6
2.4 Euler's totient theorem . . . 8
2.5 Computing the Euler totient function . . . 8
2.6 A preview of further number theory . . . 9

1 Proving the Fundamental Theorem of Arithmetic

The **fundamental theorem of arithmetic** (FTA) states that every positive integer can be written as a product of primes, and that moreover, there is only one way to do this (aside from rearranging the primes in the product). For example, 2024 and 2025 can be written as

$$2024 = 2 \cdot 2 \cdot 2 \cdot 11 \cdot 23 \quad \text{and} \quad 2025 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5.$$

For a given positive integer, the corresponding product of primes is its *prime factorization*.

This handout discusses how to prove the FTA. Knowledge of the material that is already in the textbook (AoPS Volume 1) or in class examples is assumed.

These notes are also available at https://azhou5849.github.io/teaching/.

1.1 Every positive integer is a product of primes

The fact that there is *a* prime factorization requires no additional theory.

Theorem 1.1. *Every positive integer (greater than 1) is prime or can be written as a product of primes.*

A sketch of the proof is as follows: given a positive integer $n > 1$, if n is prime, we are done. Otherwise, we can write n as a product of two positive integers smaller than n, say $n = ab$ where $1 < a, b < n$. If a is prime, then we do not need to do any further work with it, and otherwise, we can write a as a product of two positive integers smaller than n. Continuing in this way going down all possible branches of the resulting factor tree, we have to stop eventually, and this happens precisely when all of the branches end at primes.

Remark. To take this sketch and turn it into a rigorous proof, we can use mathematical induction or a proof by contradiction where we consider the minimal counterexample.

What remains is to prove that there is only one prime factorization (aside from rearrangement), and the rest of the handout is dedicated to this goal.

1.2 The euclidean algorithm

Given integers a and b, any common divisor d also divides $a + b$ and $a - b$. From this, it follows that we always have $\gcd(a, b) = \gcd(a - b, b)$. For example,

$$\begin{aligned} \gcd(70, 91) &= \gcd(70, 21) \\ &= \gcd(49, 21) = \gcd(28, 21) = \gcd(7, 21) \\ &= \gcd(7, 14) = \gcd(7, 7) = \boxed{7}. \end{aligned}$$

This method for calculating GCD is the *euclidean algorithm*.

Instead of repeatedly subtracting the same number over and over again, as in the second line above, we can jump to the end by dividing and extracting the remainder. The same example would then look like

$$\begin{aligned} \gcd(70, 91) &= \gcd(70, 21) && 91 = 1 \cdot 70 + 21 \\ &= \gcd(7, 21) && 70 = 3 \cdot 21 + 7 \\ &= \gcd(7, 0) && 21 = 3 \cdot 7 + 0 \\ &= \boxed{7}. \end{aligned}$$

Remark. Most GCD calculations in middle school competitions involve numbers small enough that we could use factorization instead. The advantage of the euclidean algorithm emerges when we deal with numbers that are difficult to factor efficiently. For instance,

$$\begin{aligned}
\gcd(582133, 268381) &= \gcd(45371, 268381) & 582133 &= 2 \cdot 268381 + 45371 \\
&= \gcd(45371, 41526) & 268381 &= 5 \cdot 45371 + 41526 \\
&= \gcd(3845, 41526) & 45371 &= 1 \cdot 41526 + 3845 \\
&= \gcd(3845, 3076) & 41526 &= 10 \cdot 3845 + 3076 \\
&= \gcd(769, 3076) & 3845 &= 1 \cdot 3076 + 769 \\
&= \gcd(769, 0) & 3076 &= 4 \cdot 769 + 0 \\
&= \boxed{769}.
\end{aligned}$$

For reference, the prime factorizations are $582133 = 757 \cdot 769$ and $268381 = 349 \cdot 769$.

1.3 Bézout's lemma

The euclidean algorithm lets us write the GCD in terms of the original integers. More specifically,

Lemma 1.2 (Bézout)**.** *Let a and b be positive integers. There exist integers m and n (which are not necessarily positive) such that*

$$ma + nb = \gcd(a, b).$$

Using the example of 70 and 91, we have

$$7 = 70 - 3 \cdot 21,$$

from the last step of the euclidean algorithm that involves a non-zero remainder. The previous step gives us $21 = 91 - 1 \cdot 70$, and we substitute this in to get

$$7 = 70 - 3 \cdot (91 - 1 \cdot 70) = 4 \cdot 70 - 3 \cdot 91.$$

To match the form of the lemma, this says that

$$4 \cdot 70 + (-3) \cdot 91 = \gcd(70, 91).$$

A more involved example is that

$$\begin{aligned}
769 &= 1 \cdot 3845 - 1 \cdot 3076 = 1 \cdot 3845 - (41526 - 10 \cdot 3845) \\
&= 11 \cdot 3845 - 1 \cdot 41526 = 11 \cdot (45371 - 1 \cdot 41526) - 1 \cdot 41526 \\
&= 11 \cdot 45371 - 12 \cdot 41526 = 11 \cdot 45371 - 12 \cdot (268381 - 5 \cdot 45371) \\
&= 71 \cdot 45371 - 12 \cdot 268381 = 71 \cdot (582133 - 2 \cdot 268381) - 12 \cdot 268381 \\
&= 71 \cdot 582133 - 154 \cdot 268381.
\end{aligned}$$

1.4 Divisibility by a prime

Proposition 1.3. *Let p be a prime number and let a and b be integers. If p divides ab, then p divides a or p divides b.*

Proof. It suffices to show that if p divides ab but p does not divide a, then p divides b. Since the only divisors of p are 1 and p, we must have $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. The latter implies p divides a, so it must be the case that $\gcd(a, p) = 1$. Now, Bézout's lemma implies that we can find integers m and n such that

$$ma + np = 1.$$

Multiplying through by b,

$$m(ab) + (nb)p = b.$$

Both terms of the left hand side are divisible by p, so the right hand side b is divisible by p. □

It follows that if a prime p divides a product of integers of any length (not necessarily just two factors), then p divides at least one of the integers in the product.

1.5 Prime factorization is unique

We can now prove that no positive integer can have two genuinely different prime factorizations. Suppose that the positive integer n has prime factorizations

$$n = p_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s,$$

where $p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq q_3 \leq \cdots \leq q_s$ are primes. Suppose $p_1 \leq q_1$. By the previous section's result, the prime number p_1 divides the product $q_1 q_2 q_3 \cdots q_s$, so p_1 must divide one of the factors $q_1, q_2, q_3, \ldots, q_s$. Since those factors are all prime, the only way this can happen is for p_1 to be equal to one of those factors. Since $p_1 \leq q_1$, which is the smallest of the factors, we must have $p_1 = q_1$. If we suppose instead that $q_1 \leq p_1$, we reach the same conclusion with the same argument. Thus we have $p_1 = q_1$ in any case, and we can cancel this common factor to get

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

We then continue this process to show $p_2 = q_2$, then $p_3 = q_3$, and so on. If one side ever runs out of factors before the other, then we end up with one side of the equation being 1 and the other side being a product of one or more primes, which is impossible. Thus the two factorizations have the same length and use the same primes.

2 More on Modular Arithmetic

For a positive integer m and integers a and b, we say that $a \equiv b \pmod{m}$, read as "a is congruent to b modulo m," if a and b have the same remainder when dividing by m. Equivalently, $a \equiv b \pmod{m}$ if and only if $a - b$ is divisible by m. From the latter, we can prove that "congruence modulo m" is an equivalence relation on the integers, meaning that

(a) (reflexive) $a \equiv a \pmod{m}$ for all integers a,

(b) (symmetric) if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$,

(c) (transitive) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

What makes congruence useful, beyond just keeping track of remainders, is that we can still do arithmetic. More specifically, if $a \equiv b \pmod{m}$, then for any integer c,

(d) $a + c \equiv b + c \pmod{m}$,

(e) $a - c \equiv b - c \pmod{m}$,

(f) $ac \equiv bc \pmod{m}$.

Combining some of the above properties allows us to show more generally that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

(g) $a + c \equiv b + d \pmod{m}$,

(h) $a - c \equiv b - d \pmod{m}$,

(i) $ac \equiv bd \pmod{m}$.

In what follows, we develop some further important results in modular arithmetic, both for contest math and for continued studies of number theory.

These notes are also available at https://azhou5849.github.io/teaching/.

2.1 Multiplicative inverses

In the rational and real number systems, division is formally defined as multiplication by the reciprocal. In modular arithmetic, we are limited to integers, but we can look for integers which fulfill the same role.

Definition 2.1 (Multiplicative inverse)**.** Let m be a positive integer and a be an integer. A *(multiplicative) inverse of a (modulo m)* is an integer b with the property that $ab \equiv 1 \pmod{m}$.

Inverses are unique modulo m, meaning that if b and c are both inverses of a modulo m, then $b \equiv c \pmod{m}$. To prove this, we compute

$$b \equiv b \cdot 1 \equiv b \cdot (ac) \equiv (ba) \cdot c \equiv 1 \cdot c \equiv c \pmod{m}.$$

This means that when an inverse of a modulo m exists, we can use the notation a^{-1} for any such inverse (while we work modulo m).

The matter of existence is less straightforward than with reciprocals of rational or real numbers, however. For example, suppose x is an inverse to 2 modulo 6. This means that $2x \equiv 1 \pmod{6}$,

so there is an integer k such that $2x = 6k + 1$. However, this is impossible: the left hand side is divisible by 2 while the right hand side is not.

The key issue here is that 2 and 6 share a common factor greater than 1. More generally, if $\gcd(a, m) = d > 1$, then $ax \equiv 1 \pmod{m}$ has no solutions, as in the corresponding integer equation $ax = km + 1$, both ax and km are divisible by d while 1 is not.

On the other hand, if $\gcd(a, m) = 1$, then by Bézout's lemma (Lemma 1.2), there exist integers x and y such that $ax + my = 1$. This means that $ax \equiv 1 \pmod{m}$, so x is an inverse of a.

Putting this together, we have

Theorem 2.2. *Let m be a positive integer and a be an integer. An inverse of a modulo m exists if and only if $\gcd(a, m) = 1$.*

2.2 Linear congruences

When $\gcd(a, m) = 1$, the congruence $ax \equiv b \pmod{m}$ is solved by $x \equiv a^{-1}b \pmod{m}$. For an example, consider the congruence $3x \equiv 4 \pmod{10}$. Given that 7 is an inverse of 3 modulo 10, we can multiply the given congruence by 7 to get $21x \equiv 28 \pmod{10}$, or $x \equiv 8 \pmod{10}$.

This method requires us to find an inverse of 3 modulo 10 first. While an inverse can be found algorithmically (see section 1.3), in contest situations it is usually faster to take a slightly different approach to solve the original congruence. For the above example, $3x \equiv 4 \equiv 24 \pmod{10}$, and "dividing" the congruence $3x \equiv 24 \pmod{10}$ by 3, we get $x \equiv 8 \pmod{10}$. To justify this, note that in the background, dividing is multiplying by 3^{-1}, and whatever the value of 3^{-1} is,

$$3^{-1} \cdot 24 \equiv 3^{-1} \cdot 3 \cdot 8 \equiv 8 \pmod{10}.$$

Even when $\gcd(a, m) > 1$, we can still use the method of converting congruences to equations. Consider the congruence $6x \equiv 8 \pmod{10}$, which is equivalent to the equation $6x = 10k + 8$ with integer-valued variables. Dividing through by the common factor of 2, we get $3x = 5k + 4$, which we convert back to modular arithmetic by reducing modulo 5 to get $3x \equiv 4 \pmod{5}$. Now, the coefficient of x is relatively prime to the modulus, so we can use our earlier methods. We have $3x \equiv 4 \equiv 9 \pmod{5}$, so $x \equiv 3 \pmod{5}$ is the solution to $6x \equiv 8 \pmod{10}$. (In the original modulus, $x \equiv 3 \pmod{10}$ or $x \equiv 8 \pmod{10}$.)

In general, we get the following result.

Proposition 2.3. *The congruence $ax \equiv b \pmod{m}$ has no solution if $d = \gcd(a, m)$ does not divide b. If d does divide b, then the solution to the congruence is $x \equiv (a')^{-1}b' \pmod{m'}$, where $a' = a/d$, $b' = b/d$, and $m' = m/d$. (The inverse is computed modulo m'.)*

2.3 The Chinese remainder theorem

Suppose instead of a single congruence, we have a system of linear congruences such as

$$\begin{aligned} x &\equiv 5 \pmod{8}, \\ x &\equiv 9 \pmod{13}. \end{aligned}$$

To solve this system, we once again create equations. If x is a solution, then there are integers a and b for which

$$x = 8a + 5 = 13b + 9.$$

Focusing on the latter two expressions, we can reduce the equation $8a + 5 = 13b + 9$ modulo 8 to $5 \equiv 5b + 1 \pmod 8$, or $5b \equiv 4 \pmod 8$. Solving this congruence for b gives us $b \equiv 4 \pmod 8$, so $b = 8k + 4$ for some integer k. Substituting this back in,

$$x = 13(8k + 4) + 9 = 104k + 61.$$

Thus every solution must have this form. Conversely, any integer of the form $104k + 61$ satisfies both congruences, so the solution set is the set of all $x \equiv 61 \pmod{104}$.

Theorem 2.4 (Chinese remainder theorem)**.** *If* $\gcd(m, n) = 1$*, the solution to the system of linear congruences*

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

is of the form $x \equiv c \pmod{mn}$ *for some integer* c *(depending on* a, b, m, n*).*

For an example where $\gcd(m, n) > 1$, consider Problem 6 from the Week 4 extensions, which amounts to solving the system of congruences

$$\begin{aligned} x &\equiv 9 \pmod{56}, \\ x &\equiv 21 \pmod{36}. \end{aligned}$$

If x is a solution, there are integers a and b for which

$$x = 56a + 9 = 36b + 21.$$

Before reducing the equation $56a + 9 = 36b + 21$ with a suitable modulus, we rearrange to get $56a = 36b + 12$, then divide out by the common factor of 4 to get $14a = 9b + 3$. Now, we reduce this equation modulo 9 to find $5a \equiv 3 \pmod 9$, or $a \equiv 6 \pmod 9$. Writing $a = 9k + 6$,

$$x = 56(9k + 6) + 9 = 504k + 345,$$

and the solution to the system is $x \equiv 345 \pmod{504}$. In this case, we got a similar form of solution, but with the final congruence modulo $\operatorname{lcm}(56, 36)$ instead of $56 \cdot 36$.

However, unlike the case where $\gcd(m, n) = 1$, it is possible that a solution does not exist when $\gcd(m, n) > 1$. Suppose we change the numbers in the previous example slightly, to

$$\begin{aligned} x &\equiv 9 \pmod{56}, \\ x &\equiv 22 \pmod{36}. \end{aligned}$$

From the resulting equation $56a + 9 = 36b + 22$, the left hand side is odd while the right hand side is even, so there cannot be any solutions. This means that any extension of the Chinese remainder theorem to cover moduli which are not relatively prime should include a condition for when a solution exists.

Proposition 2.5. *The system of linear congruences*

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

has a solution if and only if $a \equiv b \pmod{\gcd(m, n)}$*. In this case, the solution is of the form* $x \equiv c \pmod{\operatorname{lcm}(m, n)}$ *for some integer* c*.*

2.4 Euler's totient theorem

Let m be a positive integer, and consider the set

$$\Phi_m = \{0 \leq n < m \mid \gcd(n, m) = 1\}$$

of all non-negative integers less than m which are relatively prime to m. Every element of Φ_m is invertible modulo m, and for any integer which is invertible modulo m, there is exactly one element of Φ_m which is congruent to it modulo m.

Given two integers a and b which are invertible modulo m, their product ab is also invertible modulo m. The most direct way to see this is to identify that if we pick inverses a^{-1} and b^{-1} of a and b, then

$$(ab)(a^{-1}b^{-1}) \equiv aa^{-1} \cdot bb^{-1} \equiv 1 \cdot 1 \equiv 1 \pmod{m}.$$

This shows that $a^{-1}b^{-1}$ is an inverse to ab. Also, if a, b, c are invertible and $ab \equiv ac \pmod{m}$, then $b \equiv c \pmod{m}$. (This only requires a to be invertible.)

Putting the above observations together gives us

Lemma 2.6. *Suppose* $\gcd(a, m) = 1$. *The set*

$$a \cdot \Phi_m = \{ab \mid 0 \leq b < m \text{ and } \gcd(b, m) = 1\}$$

has the property that each element is congruent modulo m *to exactly one element of* Φ_m.

As a consequence of this lemma, when we multiply the elements of $a \cdot \Phi_m$ together, we get the same result modulo m as if we multiplied the elements of Φ_m together. That is, if P is the product of the elements of Φ_m, then

$$a^{\#(\Phi_m)} P \equiv P \pmod{m}.$$

Each element of Φ_m is invertible, so P is invertible, and we get $a^{\#(\Phi_m)} \equiv 1 \pmod{m}$.

Definition 2.7 (Euler totient function)**.** The number of elements of Φ_m, meaning the number of non-negative integers less than m which are relatively prime to m, is the *Euler totient function* evaluated at m, denoted $\phi(m)$ or $\varphi(m)$

With this notation, we have

Theorem 2.8 (Euler totient theorem)**.** *If* $\gcd(a, m) = 1$,

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

A particularly important example is that when p is a prime number, $\phi(p) = p - 1$ because every positive integer less than p is relatively prime to p. This gives us

Theorem 2.9 (Fermat's little theorem)**.** *If* p *is prime and* $\gcd(a, p) = 1$, *then* $a^{p-1} \equiv 1 \pmod{p}$.

2.5 Computing the Euler totient function

In order for the theorem to be effective, we need a way to compute $\phi(m)$. As an example, consider $\phi(100)$. In order to be relatively prime to 100, an integer must not be divisible by 2 or 5. Of the non-negative integers less than 100, there are $100/2 = 50$ multiples of 2 and $100/5 = 20$ multiples of 5. However, the multiples of 10 were counted twice, so we need to subtract $100/10 = 10$ from our count to make sure they are only counted once. This gives $50 + 20 - 10 = 60$ non-negative integers less than 100 which are not relatively prime to 100, which leaves $\phi(100) = 40$.

In general, doing this counting argument (an example of inclusion-exclusion) gives us

Theorem 2.10. *Let N be a positive integer and let $p_1, p_2, \ldots, p_k$ be the list of (distinct) primes dividing N. Then*

$$\phi(N) = N\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

2.6 A preview of further number theory

For odd primes p, consider the congruence $x^2 \equiv -1 \pmod{p}$.

p	smallest positive solution to $x^2 \equiv -1 \pmod{p}$
3	none
5	2
7	none
11	none
13	5
17	4
19	none
23	none
29	12
31	none

We may observe that when $p \equiv 3 \pmod{4}$, we get no solution. To prove this, suppose $p = 4k+3$ for an integer k. If $x^2 \equiv -1 \pmod{p}$, then

$$x^{p-1} \equiv x^{4k+2} \equiv (x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p},$$

contradicting Fermat's little theorem.

What remains is to investigate $p \equiv 1 \pmod{4}$, for which the examples computed above all have solutions. It turns out we can even write down a solution fairly compactly.

Lemma 2.11 (Wilson's theorem)**.** *If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. For $p = 2$, we just get $1 \equiv -1 \pmod{2}$, which is true. For odd primes p, the factorial $(p-1)!$ is the product of all invertible residues modulo p, and we can pair each residue with its inverse modulo p. Aside from 1 and $p-1 \equiv -1$, which are their own inverses, each pair gives us a product of 1, so the overall product is -1 modulo p. □

Now, we can take the factorial in Wilson's theorem and pair each factor k with $p - k \equiv -k$. For odd p, this gives us

$$(-1)^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}.$$

When $p \equiv 1 \pmod{4}$, the sign factor is just 1, so $x = (\frac{p-1}{2})!$ is a solution to $x^2 \equiv -1 \pmod{p}$. We have thus shown

Theorem 2.12. *For odd primes p, the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.*

This is part of the *law of quadratic reciprocity*, one of the major results of number theory. (A full discussion is beyond the scope of this course.)