MSCM Number Theory

Alan Zhou

2024-25

Contents

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 the integer x that comes from Bézout's lemma is an inverse of a modulo m.

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 Complete residue sets

A *complete residue set modulo m* is a set of integers S with the property that for every integer a, there is exactly one $x \in S$ for which $x \equiv a \pmod{m}$. We often use the set of remainders, $\{0, 1, 2, \ldots, m - 1\}$, as a complete residue set, but there are other ones we can use at times. Numerically, another convenient choice is to take values centered at 0, e.g. $\{-3, -2, -1, 0, 1, 2, 3\}$ when working modulo 7.

Closely related is the notion of a *complete multiplicative residue set modulo m*, which is a set of integers S with the properties (i) every $x \in S$ satisfies $\gcd(x, m) = 1$, and (ii) for every integer a satisfying $\gcd(a, m) = 1$, there is exactly one $x \in S$ for which $x \equiv a \pmod{m}$.

1. How many elements are there in a complete residue set modulo m?
2. Let S be a complete residue set modulo 24. Is it possible for the sum of the elements of S to be 2024?

2.3 Division in modular arithmetic

In class, we saw an example which shows that $ab \equiv ac \pmod{m}$ does not necessarily imply that $b \equiv c \pmod{m}$ (even when we require $a \not\equiv 0 \pmod{m}$). To derive a variant which does work, we generalize Proposition 1.3 to cover non-prime divisors.

Lemma 2.3. *If m divides ab, then $m' = \frac{m}{\gcd(a,m)}$ divides b.*

Proof. Let $d = \gcd(a, m)$, so that $m = dm'$. By Bézout's lemma, there exist integers x and y such that $xa + ym = d$. Multiplying through by b/m,

$$\frac{bd}{m} = \frac{xab}{m} + yb = x \cdot \frac{ab}{m} + yb$$

is an integer. Therefore, $bd/m = b/m'$ is an integer and b is divisible by m'. □

Proposition 2.4 (Division in modular arithmetic)**.** *If $ab \equiv ac \pmod{m}$, then*

$$b \equiv c \pmod{m'}, \qquad m' = \frac{m}{\gcd(a, m)}.$$

Proof. If $ab \equiv ac \pmod{m}$, then m divides $ab - ac = a(b-c)$. By Lemma 2.3, m' divides $b - c$, so $b \equiv c \pmod{m'}$ as required. □

As an example, to solve $9x \equiv 6 \pmod{15}$, we can divide both sides by 3, making sure to divide the modulus by $\gcd(3, 15) = 3$ as well, to get $3x \equiv 2 \pmod{5}$. Then, we can repeatedly add 5 to the right hand side until we get something divisible by 3. In this case, we successfully find $3x \equiv 12 \pmod{5}$. Dividing by 3 again, this time dividing the modulus by $\gcd(3, 5) = 1$, we get $x \equiv 4 \pmod{5}$. Alternatively, we could have subtracted 5 once to get $3x \equiv -3 \pmod{5}$, so then $x \equiv -1 \pmod{5}$. Since $4 \equiv -1 \pmod{5}$, we found the same solution.

Exercises

1. What is the second smallest positive integer satisfying $12n \equiv 30 \pmod{126}$?
2. The last two digits of $15n$ are 25. If $100 \leq n < 200$, what are the possible values of n?

2.4 Multiplicative inverses

A particularly important case of Proposition 2.4 is that when $\gcd(a, m) = 1$, we can safely cancel a from $ab \equiv ac \pmod{m}$ to get $b \equiv c \pmod{m}$.

Theorem 2.5. *If $\gcd(a, m) = 1$, then the multiples*

$$0, \quad a, \quad 2a, \quad 3a, \quad \ldots, \quad (m-1)a$$

form a complete residue set modulo m, meaning that for every integer N, we can find some multiple ka such that $ka \equiv N \pmod{m}$, and the choice of $k \in \{0, 1, \ldots, m-1\}$ is unique.

Proof. The above note shows that these m multiples of a lie in distinct residue classes. As there are only m residue classes in total, all of the residue classes are represented exactly once. □

Corollary 2.6. *If $\gcd(a, m) = 1$, then there is an integer b for which $ab \equiv 1 \pmod{m}$, and this b is unique modulo m. Conversely, if $ab \equiv 1 \pmod{m}$, then $\gcd(a, m) = 1$.*

Proof. For the forward direction, let $N = 1$ in Theorem 2.5. For the converse, let $d = \gcd(a, m)$. If $ab \equiv 1 \pmod{m}$, then $ab - 1 = km$ for some integer k. Both ab and km are divisible by d, so d divides 1 and hence $d = 1$. □

Since the integer b above is unique modulo m, we denote any such value by a^{-1} and call it a *multiplicative inverse of a modulo* 10. For instance, when working modulo 10, we have $3^{-1} \equiv 7$ because $3 \cdot 7 \equiv 1 \pmod{10}$. Multiplicative inverses have the same role for modular arithmetic that reciprocals do for real numbers: if we want to divide by a number in modular arithmetic, we can multiply by a multiplicative inverse (if it exists).

Exercises

1. Given that 17 is a multiplicative inverse of 13 modulo 22, solve $13x \equiv 18 \pmod{22}$.
2. Compute multiplicative inverses of 1, 2, 3, 4, 5, and 6 modulo 7.

2.5 Systems of linear congruences

In this section, we consider systems of congruences of the form

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

For example, suppose we have the system

$$\begin{aligned} x &\equiv 4 \pmod{8}, \\ x &\equiv 2 \pmod{21}. \end{aligned}$$

To solve this, we can rewrite one of the congruences as an equation using an extra integer-valued variable. The second congruence states that $x = 21k + 2$ for some integer k. Substituting into the first congruence,

$$21k + 2 \equiv 4 \pmod{8} \implies 5k \equiv 2 \pmod{8}.$$

Either by finding a multiplicative inverse of 5 modulo 8, which is doable since $\gcd(5, 8) = 1$, or by adding or subtracting a multiple of 8 to the right hand side to get something divisible by 5, we find that $k \equiv 2 \pmod{8}$. In turn writing this as $k = 8\ell + 2$ for some integer ℓ,

$$x = 21(8\ell + 2) + 2 = 168\ell + 44.$$

This shows that $\boxed{x \equiv 44 \pmod{168}}$. Conversely, $x \equiv 44 \pmod{168}$ satisfies the two original congruences, as can be seen by simplify $168\ell + 44$ modulo 8 and 21, so we have found the exact solution set. The process generalizes.

Theorem 2.7 (Chinese remainder theorem)**.** *If* $\gcd(m, n) = 1$*, then for any integers* a *and* b*, the solution set to the system of congruences*

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

is a residue class modulo mn*.*

Exercises

1. (Week 4 slides) There are several cookies in a jar. Sharing the cookies evenly among 3 children leaves 2 cookies left. Sharing the cookies among 7 children leaves 3 cookies left. Find all the possible amounts of cookies in the jar.

2. (Week 4 extensions) The eighth graders are taking buses to visit Sea World today. Each large bus can take 56 students and each small bus can take 36 students. If we try to let all students take a large bus, then all will be full except for one bus with only 9 students. If we try to let all students take a small bus, then all will be full except for one bus with 21 students. What are the possible amounts of eighth graders?

2.6 Euler's Totient Theorem

By Corollary 2.6, the integers relatively prime to m are precisely those that have multiplicative inverses modulo m. As we can compute $(xy)^{-1} \equiv x^{-1}y^{-1} \pmod{m}$ whenever x and y are invertible modulo m, this tells us (with an admittedly roundabout proof) that the product of any two integers relatively prime to m is also relatively prime to m.

Now consider the complete multiplicative residue set modulo m

$$\Phi_m = \{a \mid 1 \leq a \leq m \text{ and } \gcd(a, m) = 1\}.$$

(Here Φ is the capital Greek letter Phi. The notation is non-standard.) The number of elements of Φ_m is the *Euler totient function* evaluated at m, and this function is denoted ϕ or φ (the lowercase Greek letter phi).

Analogously to Theorem 2.5, we have

Theorem 2.8. *If* $\gcd(a, m) = 1$*, then*

$$a \cdot \Phi_m = \{ab \mid b \in \Phi_m\}$$

is also a complete multiplicative residue set modulo m*.*