Modular Arithmetic II

Hanna Chen and Mahith Gottipati

August 22, 2021

Contents

1 Introduction

In the previous handout, we saw the basics of modular arithmetic, such as basic arithmetic operations in different mods. In this handout, we will take a look at some of the more complicated identities and theorems, which we can now better understand with our modular arithmetic tools.

2 Bezout's Identity

2.1 Theorem and Proof

An important theorem in our study of modular arithmetic is Bezout's Identity, which states the following:

Theorem 2.1 (Bezout's Identity)
For two integers $a \neq b$, if $\gcd(a, b) = d$, then there exists integers x, y such that $ax + by = d$.

Proof. Let set S consist of all integers of the form $ax + by$, where x and y are integers and $ax + by > 0$. Since $|a| + |b|$ and $|a + b|$ must be in this set, we know that it is not empty.

Note, there must be an element $p \in S$ less than all other elements in S (this is formally known as the Well Ordering Principle). Let that least element be $p = ax_p + by_p$. By the Division Algorithm, there must exist integers q and $r < p$ such that $a = pq + r$. Since $r < p$ and p is the smallest element in S, r is not in S.

However, we have $r = a - pq = a - (ax_p + by_p)q = a(1 - x_p q) + b(-y_p q)$, which is in S unless $r = 0$. Substituting $r = 0$ we have $pq = a$, implying $p|a$ and for similar reasoning we have $p|b$. To finish, note that d is the greatest integer which divides a and b, so $p \leq d$ as p also divides both a and b. However, $ax_p + by_p \equiv 0x_p + 0y_p \equiv 0 \pmod{d}$ because $a \equiv b \equiv 0 \pmod{d}$, so $d|p \implies d \leq p$. Therefore, $d = p$ and we are done. □

Before we look at some examples, here are two notes that could come in handy when using Bezout's Identity to solve problems.

Remark 2.2. $d = \gcd(a, b)$ is the smallest integer in the form $ax + by$.

Remark 2.3. Every other number in the form $ax + by$ is an integer multiple of d.

2.2 Examples

Example 2.4 (2006 AMC 10A Problem 22)
Two farmers agree that pigs are worth 300 dollars and that goats are worth 210 dollars. When one farmer owes the other money, he pays the debt in pigs or goats, with "change" received in the form of goats or pigs as necessary. (For example, a 390 dollar debt could be paid with two pigs, with one goat received in change.) What is the amount of the smallest positive debt that can be resolved in this way?

Solution. Let p be the number of pigs and let g be the number goats that the farmers involve in their transaction (note that, while both have to be integers, they do not need to both be positive). Furthermore, let the amount of debt be x.

Then, we have that $300p + 210g = x$, and wish to find the minimum value of x.

Directly applying Bezout's Identity gives that there exists integers p and g such that $300p + 210g = \gcd(300, 210) = 30$, so the maximum value of the minimum value of x is 30.

To prove that 30 is the desired answer, we write the equation as $30(10p + 7g) = x$, which forces x to be divisible by 30. Therefore, our answer is $\boxed{30}$. □

Example 2.5
For integers a, b, c, prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Solution. Since $a \mid bc$, we can write $bc = ak$ for some integer k. Furthermore, since $\gcd(a, b) = 1$, we have by Bezout's Identity that there exist integers m, n such that $am + bn = \gcd(a, b) = 1$. Multiplying both sides by c gives $acm + bcn = c$. Plugging in $bc = ak$ gives $acm + akn = c$, so $c = a(cm + kn)$. Since c, m, k, n are integers, this means that $a \mid c$, as desired. □

2.3 Exercises

Exercise 2.6. Prove, without using the Euclidean Algorithm, that $6x + 7$ and $7x + 8$ are relatively prime for all integers x.

Exercise 2.7. For integers a and b, if $ax + by = 24$ for integer x and y, find the sum of all distinct values of $\gcd(a, b)$.

Exercise 2.8. Prove that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ for all positive integers a, m, and n.

3 Multiplicative Inverse

3.1 Definition

In typical arithmetic, the inverse of real number k is the real number k^{-1} such that $k \cdot k^{-1} = 1$. In modular arithmetic, the definition is similar:

Multiplicative Inverse
For positive integer $n \geq 1$, the multiplicative inverse of positive integer a modulo n is the unique positive integer $1 \leq b < n$ such that $ab \equiv 1 \pmod{n}$.

For example, the multiplicative inverse of 3 in mod 5 is 2 since $3 \cdot 2 = 6 \equiv 1 \pmod{5}$.

However, the multiplicative inverse does not always exist. For example, 2 does not have a multiplicative inverse in mod 6.

In fact, for positive integers a and n, if $\gcd(a, n) \neq 1$, a will not have a multiplicative inverse in mod n. On the other hand, as long as $\gcd(a, n) = 1$, a has a multiplicative inverse in mod n. We will prove this in the following section:

3.2 Proof of Existence

Theorem 3.1
For positive integers a and n, a has a multiplicative inverse mod n if and only if $\gcd(a, n) = 1$.

Proof. As with all theorems including "if and only if", we must prove both directions.

Let us first prove that if a has a multiplicative inverse mod n, then $\gcd(a, n)$ must be 1. We proceed by contradiction. Suppose $\gcd(a, n) = d \neq 1$. We assumed that a has a multiplicative inverse modulo n, so there must exist an integer b such that $ab \equiv 1 \pmod{n} \implies ab = nq + 1$ for an integer q. Taking this modulo d, we have $0 \equiv 1 \pmod{d}$ as $d|a$ and $d|n$. However, this implies $d = 1$ which contradicts $d \neq 1$.

Now, let's prove that if $\gcd(a, n) = 1$, a has a multiplicative inverse in mod n. By Bezout's Identity, this implies that there exist integers x and y such that $ax + ny = \gcd(a, n) = 1$. Since $ny \equiv 0$ in mod n, we have that $ax \equiv 1 \pmod{n}$, meaning that x is our multiplicative inverse. □

3.3 Examples

Example 3.2
Find the number of positive integers less than 16 that have a multiplicative inverse in mod 16.

Proof. Note that, for x to have a multiplicative inverse in mod 16, we must have $\gcd(x, 16) = 1$. This is true for all odd numbers less than 16, and none of the even numbers less than 16. Therefore, our answer is $\boxed{8}$. □

Example 3.3
Find the value of $1^{-1} + 3^{-1} + 5^{-1} + \cdots + 63^{-1} \pmod{8}$.

Proof. Note that the residues of the bases mod 8 repeat in cycles of $1, 3, 5, 7, 1, 3, \ldots$. The multiplicative inverses of $1, 3, 5, 7$ are $1, 3, 5, 7$ respectively. There are 15 repeats of the cycle of $1, 3, 5, 7$, so the final result will be $15 \cdot (1 + 3 + 5 + 7) = 15 \cdot 16 \equiv \boxed{0} \pmod{8}$. □

3.4 Exercises

Exercise 3.4. Find the multiplicative inverse of 29 in mod 113.

Exercise 3.5. Find the sum of the multiplicative inverses, if they exist, of all mod 24 residues.

4 Chinese Remainder Theorem

4.1 Theorem

The Chinese Remainder Theorem can be useful in many modular arithmetic problems, whose problem statements include a system of linear congruences.

Linear Congruence

A *linear congruence* is an equation of the form $ax \equiv b \pmod{n}$, where we wish to solve for x for given constants a, b, and n.

The theorem states the following:

Theorem 4.1 (Chinese Remainder Theorem)

Let there be a set of k pairwise relatively prime positive integers, $n_1, n_2, \dots n_k$, and let their product be $N = n_1 \cdot n_2 \cdots n_k$. For each set of $x_1, x_2, \dots x_k$ such that $0 \le x_i \le n_i$ for all $1 \le i \le k$, there exists a unique $0 \le x \le N$ such that $x \equiv x_1 \pmod{n_1}$, $x \equiv x_2 \pmod{n_2}$, $\dots x \equiv x_k \pmod{n_k}$. In other words, all solutions to this set of n linear congruences will have the same remainder in mod N.

4.2 Examples

Example 4.2

Find all positive integers x such that $x \equiv 1 \pmod{3}$ and $x \equiv 3 \pmod{7}$.

Proof. By the Chinese Remainder Theorem, since $\gcd(3, 7) = 1$, all solutions will have the same residue in mod $3 \cdot 7 = 21$.
We can write $x = 3a + 1 = 7b + 3$ for positive integers a, b. This gives that $3a \equiv 2 \pmod{7}$. Using the multiplicative inverse of 3 in mod 7, which is 5, we get that $a \equiv 2 \cdot 5 = 10 \equiv 3$ mod 7.
Our smallest solution is $3 \cdot 3 + 1 = 10$, but that is not the only solution. By the Chinese Remainder Theorem, all solutions will be 10 in mod 21, so all of our solutions are of the form $\boxed{21y + 10 \text{ for nonnegative integers } y}$. □

Example 4.3

Find all positive integers x such that $x \equiv 2 \pmod{4}$ and $x \equiv 3 \pmod{8}$.

Proof. Note that here we cannot apply the Chinese Remainder Theorem, because $\gcd(4, 8) = 4 \neq 1$.
By letting $x = 4a + 2 = 8b + 3$, we note that $x = 4a + 2$ means that x is even, while $x = 8b + 3$ means that x is odd, which is a contradiction. Therefore there are $\boxed{\text{no solutions}}$. □

In some cases with systems of linear congruences, however, we don't need to use the Chinese Remainder Theorem. See the following example:

Example 4.4

Find all positive integers x such that $x \equiv 3 \pmod{4}$ and $x \equiv 8 \pmod{9}$.

Proof. Here, we don't need to use the Chinese Remainder Theorem.
Note that $x \equiv 3 \pmod 4$ means that $x \equiv -1 \pmod 4$, and $x \equiv 8 \pmod 9$ means that $x \equiv -1 \pmod 9$. So, our solutions will be of the form $\boxed{36n - 1 \text{ for all positive integers } n}$, since $\operatorname{lcm}(4, 9) = 36$. □

From Example 4.4, we have a formula to solve this special case of linear congruences:

Theorem 4.5
If positive integer x satisfies $x \equiv a \pmod{m_1}$, $x \equiv a \pmod{m_2}$, $\ldots x \equiv a \pmod{m_k}$ for positive integer k, integer a, and positive integers m_i, then $x \equiv a \pmod{\operatorname{lcm}(m_1, m_2, \ldots m_k)}$.

4.3 Exercises

Exercise 4.6 (2017 AMC 10B). Let $N = 123456789101112\ldots4344$ be the 79-digit number that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45?

Exercise 4.7. Find the sum of the 3 smallest positive values of x such that $x \equiv 3 \pmod 7$, $x \equiv 5 \pmod 9$, and $x \equiv 12 \pmod{17}$.

5 Exponential Congruences

5.1 Examples

Example 5.1
If one wanted to find the value of 2^3 in mod 3, they could just calculate 2^3 and divide it by 3. But, what if the question were to find 2^{100} in mod 3?

Proof. Note that $2 \equiv -1 \pmod 3$. Since 100 is even, $2^{100} \equiv (-1)^{100} \equiv 1 \pmod 3$. □

Example 5.2 (2009 AMC 10B Problem 21)
What is the remainder when $3^0 + 3^1 + 3^2 + \cdots + 3^{2009}$ is divided by 8?

Proof. Note that 3^{2k} for integer $k \equiv 1 \pmod 8$ and 3^{2k+1} for integer $k \equiv 3 \pmod 8$. Therefore, we can rewrite the expression as $(1 + 3) + (1 + 3) + ... + (1 + 3)$. The total number of pairs in the expression is $2010/2 = 1005$, which is odd. Therefore, the answer is $\boxed{4}$. □

5.2 Techniques, Tips, and Tricks

Here are some common techniques when working with exponents in modular arithmetic:

1. Try to find powers of the base such that the whole expression is 1, −1, or another small number in the given mod.
2. When there are many powers in a sum, try to group the terms together in a way that cancels most/all of them.

3. Look for cyclic residues–in other words, after the first few terms, the residues of the powers start to repeat in a cycle of a certain length.

Another key thing to note is the following theorem:

Theorem 5.3
For real a and b and positive integer n, if $a \equiv b \pmod{n}$, then $a^c \equiv b^c$ for all integer values of c.

5.3 Exercises

Exercise 5.4 (2003 AMC 10A). What is the units digit of 13^{2003}?

Exercise 5.5. Find the last two digits of $27^0 + 27^1 + \cdots + 27^{100}$.

6 Fermat's, Wilson's, and Euler's

As we saw previously, exponents in modular arithmetic can be simplified using various techniques. In this section, we will explore three of the most important theorems which will come in handy in simplifying and/or solving many modular arithmetic problems.

6.1 Fermat's Little Theorem

Theorem 6.1
$a^p \equiv a \pmod{p}$ for all positive primes p and integers a.

Proof. Note that $a^p \equiv a \pmod{p} \implies p|(a^p - a)$ since rearranging gives that $a^p - a \equiv 0$.

We proceed by induction. Assume that, for positive integer $k > 1$, p divides $k^p - k$. Now, consider $(k+1)^p - (k+1)$. By the binomial theorem, $(k+1)^p = k^p + \binom{p}{1}k^{(p-1)} + \cdots + \binom{p}{p-1}k + 1$, which means that $(k+1)^p - k^p - 1 = \binom{p}{1}k^{(p-1)} + \cdots + \binom{p}{p-1}k$ is a multiple of p. Adding $k^p - k$ to both sides gives $((k+1)^p - k^p - 1) + (k^p - k) = (k+1)^p - (k+1)$. Since both of $((k+1)^p - k^p - 1)$ and $(k^p - k)$ are multiples of p, the whole expression is a multiple of p, which means that p divides $(k+1)^p - (k+1)$. Since k was chosen arbitrarily, this means that p divides all integers of the form $a^p - a$ for integers a. Rearranging gives Fermat's Little Theorem. □

Example 6.2
Find the value of 2^{100} in mod 7.

Proof. By Fermat's Little Theorem, we have that $2^7 \equiv 2 \pmod{7}$ since 7 is prime. Using our exponential congruence techniques, we have $2^{100} = (2^7)^{14} \cdot 2^2 \equiv 2^{14} \cdot 2^2$. We can apply Fermat's Little Theorem again to get $2^{14} \cdot 2^2 = (2^7)^2 \cdot 2^2 \equiv 2^2 \cdot 2^2 = 2^4 = 16 \equiv \boxed{2} \pmod{7}$. □

6.2 Wilson's Theorem

Theorem 6.3
For all primes p, $(p-1)! \equiv -1 \pmod{p}$.

Proof. By Theorem 3.1, every integer in the set $\{1, 2, \dots p-1\}$ has a multiplicative inverse in mod p (which is in the set), since each of those integers is relatively prime to p. Note that here, p is a prime that's greater than 2, and is thus an odd number.

For any a in the set, we have $a \cdot a^{-1} \equiv 1 \pmod{p}$, where a^{-1} denotes the modulo p multiplicative inverse of a. Note that $a = a^{-1} \implies a^2 \equiv 1 \pmod{p} \implies a \equiv \pm 1 \pmod{p} \implies a = 1$ or $a = (p-1)$. So, for all $a \neq 1$ or $p-1$, we can pair a with its inverse, $a^{-1} \neq a$, and together, their product is 1 mod p. This product gets cancelled in the expression for $(p-1)!$. Therefore, $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$.

Note that we overlooked $p = 2$, which we can prove directly–$(p-1)! = (2-1)! = 1 \equiv -1 \pmod{2}$. □

Here's an example in which Wilson's Theorem can be applied:

Example 6.4 (Well-Known)
Let a be an integer such that $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{23} = \frac{a}{23!}$. Find the remainder when a is divided by 13.

Proof. Multiplying both sides by 23! gives $a = \frac{23!}{1} + \frac{23!}{2} + \cdots + \frac{23!}{23}$. Since 13 is prime, the only term on the Left Hand Side that isn't a multiple of 13 is $\frac{23!}{13}$, so $a \equiv \frac{23!}{13} \pmod{13}$.

So, $a \equiv 23 \cdot 22 \cdots 14 \cdot 12!$. By Wilson's Theorem, $12! \equiv -1 \pmod{13}$, so $a \equiv (-1) \cdot 23 \cdot 22 \cdots 14 \equiv 10! = 3628800 \equiv \boxed{7} \pmod{13}$. □

6.3 Euler's Totient Theorem

Before we state Euler's Theorem, we must first define the totient function:

Totient Function
The totient function of positive integer n, denoted as $\varphi(n)$, is the number of positive integers less than or equal to n that are relatively prime to n.

For example, $\varphi(12) = 4$ because the only integers less than 12 that are relatively prime to it are $1, 5, 7$, and 11. To quickly compute $\varphi(n)$ for large values of n, all you need is, is its prime factorization.

Theorem 6.5 (Totient Function Closed Form)
Let $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$. Then,

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Proof. Consider the set of numbers $\{1, 2, 3, \dots, n\}$. The probability a number randomly selected from this list that contains p_1 as a factor is $\frac{1}{p_1}$, so the probability that a number does not contain p_1 as a factor is the complement of that; $1 - \frac{1}{p_1}$. Similarly, the probability a number does not contain p_2 as a factor is $1 - \frac{1}{p_2}$. For any p_k, the probability that a randomly selected number from this list does not contain p_k as a factor is $1 - \frac{1}{p_k}$. Thus, the probability a randomly selected integer does not have any of $p_1, p_2, \ldots, p_k$ as a factor is

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

So, the number of integers in this list satisfying this property would just be n times this probability, which is exactly what we wanted to prove. □

Now, we state the theorem and its proof:

Theorem 6.6 (Euler's Totient Theorem)
For relatively prime positive integers a and n, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. We consider the set of $\varphi(n)$ elements, set $S = \{s_1, s_2, \ldots s_{\varphi(n)}\}$, where s_i are all relatively prime to n. Note that this set is identical to set $R = \{as_1, as_2, \ldots as_{\varphi(n)}\}$, although not in order, because all elements of R are distinct and also relatively prime to n.

Therefore, $s_1 s_2 \cdots s_{\varphi(n)} \equiv as_1 as_2 \cdots as_{\varphi(n)} \pmod{n} \implies a^{\varphi(n)} s_1 s_2 \cdots s_{\varphi(n)} \equiv s_1 s_2 \cdots s_{\varphi(n)} \pmod{n}$. Since $s_1 s_2 \cdots s_{\varphi(n)}$ is relatively prime to n, we can divide both sides by $s_1 s_2 \cdots s_{\varphi(n)}$ to get that $a^{\varphi(n)} \equiv 1 \pmod{n}$, as desired. □

Example 6.7
Find the last three digits of 3^{807}.

Proof. This is equivalent to finding 3^{807} in mod 1000. By Euler's Totient Theorem, we have $3^{\varphi 1000} \equiv 1 \pmod{1000}$. $\varphi 1000 = 1000 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$. So, $3^{807} = (3^{400})^2 \cdot 3^7 \equiv 3^7 = 2187 \equiv \boxed{187} \pmod{1000}$. □

6.4 Exercises

Exercise 6.8. Find the value of 42! in mod 1763.

Exercise 6.9. Find the last two digits of $2^{50} + 5^{50}$.

7 Problems

Minimum is **[16 ♟]**. Problems denoted with ♖ are required. (They still count towards the point total.)

> "We know that God exists because mathematics is consistent and we know that the devil exists because we cannot prove the consistency."
>
> *Andre Weil*

[2 ♖] Problem 1. Find the value of $3^{-1} + 9^{-1} + 27^{-1} + \cdots + 14348907^{-1}$ in mod 10. Your answer should be an integer between 0 and 9, inclusive.

[2 ♟] Problem 2 (2018 AMC 10B). Let $a_1, a_2, \ldots, a_{2018}$ 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 3 (2017 AMC 10B). An integer N is selected at random in the range $1 \leq N \leq 2020$. What is the probability that the remainder when N^{16} is divided by 5 is 1?

[3 ♖] Problem 4 (2020 BMT Discrete Round). Compute the remainder when 98! is divided by 101.

[5 ♖] Problem 5 (2019 SMT Discrete Round). Let $S = 1 + 2 + 3 + ... + 100$. Find $(100!/4!)$ mod S.

[5 ♟] Problem 6 (1975 IMO). When 4444^{4444} is written in decimal notation, the sum of its digits is A. Let B be the sum of the digits of A. Find the sum of the digits of B. (A and B are written in decimal notation.)

[6 ♟] Problem 7 (2010 AMC 10A). The number obtained from the last two nonzero digits of 90! is equal to n. What is n?

[6 ♖] Problem 8 (2007 HMMT Guts). Find the number of 7-tuples $(n_1, \ldots, n_7)$ of integers such that

$$\sum_{i=1}^{7} n_i^6 = 96957.$$

[7 ♟] Problem 9 (2007 PUMaC Number Theory). How many pairs of integers a and b are there such that a and b are between 1 and 42 and $a^9 = b^7 \mod 43$?

[7 ♟] Problem 10 (2019 AMC 10A). For how many integers n between 1 and 50, inclusive, is

$$\frac{(n^2-1)!}{(n!)^n}$$

an integer? (Recall that $0! = 1$.)