

CS 30: Discrete Math in CS (Winter 2020): Lecture 26

Date: 26th February, 2020 (Wednesday)

Topic: Numbers: Application of Bezout's, Multiplicative Inverses

Disclaimer: These notes have not gone through scrutiny and in all probability contain errors.

Please discuss in Piazza/email errors to deeparnab@dartmouth.edu

1. **Arithmetic modulo n .** Recall the set $\mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}$, that is, the set of possible remainders. Given any number $a \in \mathbb{N}$, we know that $a \bmod n$ lies in this set \mathbb{Z}_n .

Furthermore, we can do addition, subtraction, and multiplication which takes two numbers in \mathbb{Z}_n and lands in \mathbb{Z}_n . Indeed, the definitions are as follows:

$$a +_n b = (a + b) \bmod n \quad a -_n b = (a - b) \bmod n \quad a \times_n b = (a \cdot b) \bmod n$$

One arithmetic operation is missing : *division*. It turns out that when n is a prime, we can define a form of division as well. And this is going to be a super-powerful thing.

2. **Multiplicative Inverse.**

Theorem 1. For any positive integer n and $a \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$, there exists an integer $b \in \mathbb{Z}_n$ such that $ab \equiv_n 1$.


Proof. Since $\gcd(a, n) = 1$, Bezout's identity tells us there exists integers x and y (caution: these may not lie in \mathbb{Z}_n ...indeed, they may not even be positive) such that

$$xa + yn = 1$$

Taking both sides modulo n , we get

$$(xa + yn) \bmod n = (xa) \bmod n + \underbrace{(yn) \bmod n}_{=0} = (x \bmod n) \cdot a \equiv_n 1$$

where we have used that $a \in \mathbb{Z}_n$ to begin with and thus $a \bmod n = a$. Therefore, the answer is $b = x \bmod n$. \square

Example. Suppose $a = 12$ and $n = 17$. By applying the Extended Euclid Algorithm (we did it last time), we get $(-7) \cdot a + 5 \cdot n = 1$. Then, the $b \in \mathbb{Z}_{17}$ such that $ab \equiv_{17} 1$ should be given by $b = x \bmod n = (-7) \bmod 17 = 10$. Check: $10 \times 12 = 120 = 17 \cdot 7 + 1$, and so $10 \cdot 12 \equiv_{17} 1$. 

Exercise: Repeat the same calculations for $a = 17$ and $b = 12$.

The next theorem shows that the b above is unique.

Theorem 2. For any positive integer n and $a \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$, there exists a **unique** integer $b \in \mathbb{Z}_n$ such that $ab \equiv_n 1$.

Proof. Theorem 1 shows there is at least one such b . This theorem is asking for uniqueness. We prove this via contradiction.

Suppose there exist *two* unequal numbers b_1 and b_2 in \mathbb{Z}_n such that both $ab_1 \equiv_n 1$ and $ab_2 \equiv_n 1$. Since $b_1 \neq b_2$, we get that $(b_1 - b_2) \bmod n \neq 0$. Subtracting, we get that $(a(b_1 - b_2)) \bmod n = 0$. Since $\gcd(a, n) = 1$, Bezout tells us there exists x, y such that $xa + yn = 1$. Multiplying both sides by $(b_1 - b_2)$, we get

$$xa(b_1 - b_2) + yn(b_1 - b_2) = (b_1 - b_2)$$

Taking modulo n , we get

$$(x \bmod n) \cdot \underbrace{(a(b_1 - b_2)) \bmod n}_{=0} + \underbrace{(yn(b_1 - b_2)) \bmod n}_{=0} = \underbrace{(b_1 - b_2) \bmod n}_{\neq 0}$$

We get a contradiction. □

The above two theorems establish the following: for any number n , and any number $a \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$, there exists one and only number $b \in \mathbb{Z}_n$, such that $ab \equiv_n 1$. This number b is called the **multiplicative inverse** of a in \mathbb{Z}_n . This is denoted as a^{-1} . ✎

Exercise: Given an n and $a \in \mathbb{Z}_n$ with $\gcd(a, n) = 1$, prove that the multiplicative inverse a^{-1} of a modulo n satisfies $\gcd(a^{-1}, n) = 1$. ✎

Exercise: Given an n and $a \in \mathbb{Z}_n$ with $\gcd(a, n) = 1$, show that the multiplicative inverse of a^{-1} is a itself. (This is easy)

3. **Division in \mathbb{Z}_p .** Let p be a prime number. Since p is prime, every non-zero number $a \in \mathbb{Z}_p$ satisfies $\gcd(a, p) = 1$. The fact that non-zero number in \mathbb{Z}_p has an inverse allows to define division in \mathbb{Z}_p as follows. Given any $a \in \mathbb{Z}_p$ and $b \in \mathbb{Z}_p \setminus \{0\}$, we define

$$a \div_p b = (a \cdot b^{-1}) \bmod p$$

Why is this useful? Well, it makes \mathbb{Z}_p behave like rational/real numbers (technically, \mathbb{Z}_p is a “field”). Here is an application

Theorem 3. Let p be a prime, and let $a \in \mathbb{Z}_p \setminus \{0\}, b, r \in \mathbb{Z}_p$. Then the following linear equation has exactly one solution in \mathbb{Z}_p

$$a \cdot x + b \equiv_p r$$

Proof. The solution is as in the reals case. If a was a non-zero real, and b, r were arbitrary reals, then the unique solution would be $x = (r - b)/a$ (where we are talking about real division).

In this case, it is precisely $x := a^{-1} \cdot (r - b) \bmod p$. Check: $ax \equiv_p (aa^{-1})(r - b) \equiv_p (r - b)$, and so $ax + b \equiv_p r$.

Why is it unique? It is the same reason why it was unique for reals. If $ax + b \equiv_p r \equiv_p ay + b$, then we get $a \cdot (x - y) \equiv_p 0$. Since $x, y \in \mathbb{Z}_p$ are unequal, we have $(x - y) \not\equiv_p 0$, and $a \not\equiv_p 0$, which implies $a(x - y) \not\equiv_p 0$. \square

Example. Let's take $p = 17$ and consider the equation $12 \cdot x + 7 = 4 \bmod 17$. We already know $12^{-1} \equiv_{17} 10$ (calculated above). Thus, we get the solution $x = (4 - 7) \cdot 10 \bmod 17 = -30 \bmod 17 = 4$. Indeed check: $12 \cdot 4 + 7 = 55$ which indeed leaves remainder 4 when divided by 17.

There is no reason to stick to one equation in one variable. We can generalize to more variables and more equations. Let me state one theorem that we will use (and then discuss the general case).

Theorem 4. Let p be a prime. Let $u \neq v$ be two elements in $\mathbb{Z}_p \setminus \{0\}$. Let w, r and s be three elements in \mathbb{Z}_p . Then the following system of equations has a unique solution over \mathbb{Z}_p .

$$u \cdot x + w = r \bmod p \quad v \cdot y + w = s \bmod p$$

Proof. Indeed, the solutions are $x = u^{-1} \cdot (r - w) \bmod p$ and $y = v^{-1} \cdot (s - w) \bmod p$. \square

4. **Scramblings.** The above fact that linear equations have unique solutions over \mathbb{Z}_p have a lot of advantages. Let p be prime, and let $a \in \mathbb{Z}_p \setminus \{0\}$. Given a and p , define the map

$$h_a : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \quad h_a : x \mapsto a \cdot x \bmod p \quad (1)$$

Theorem 5. For any $a \in \mathbb{Z}_p \setminus \{0\}$, the function h_a is a bijection.

Proof. The function is clearly well-defined. To prove it is a surjection, given any $b \in \mathbb{Z}_p$, we need to show an $x \in \mathbb{Z}_p$ such that $ax \equiv_p b$. But this is given by $x = a^{-1} \cdot b \bmod p$. To prove this is an injection, given any x and y in \mathbb{Z}_p with $x \neq y$, we need to show $h_a(x) \neq h_a(y)$. Indeed, $h_a(x) - h_a(y) = a \cdot (x - y) \bmod p \neq 0$ (the same reason why linear equations have unique solutions). \square

Example. Let us take $p = 11$ and $a = 6$ and consider the function h_a . We see that it takes $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$ to $(0, 6, 1, 7, 2, 8, 3, 9, 4, 10, 5)$. Thus if we forget the 0 (0's are always mapped to 0's), it *scrambles* us the permutation 1 to 10. If we take a different a , say $a = 3$, we get a different permutation $(0, 3, 6, 9, 1, 4, 7, 10, 2, 5, 8)$. This idea is used heavily in the construction of "random looking functions", that is, *hash functions*.

5. Fermat's Little Theorem.

Theorem 6. For any $a \in \mathbb{Z}_p \setminus \{0\}$, $a^{p-1} = 1 \pmod p$.

Remark: The above allows us to do much “faster” modular exponentiation (at least by hand) when the modulus is prime. For instance, instantiating the above theorem for $a = 3$ and $p = 7$, we get $3^6 \equiv_7 1$. But we also get $3^{60} \equiv_7 1$ by taking the above to power 10 on both sides (note $1^{10} = 1$). And we also get $3^{61} \equiv_7 3 \cdot 3^{60} \equiv_7 3$.

Exercise: Use Fermat’s Little Theorem to find the following (much faster than modular exponentiation):

- (a) $4^{18} \pmod{19}$
- (b) $7^{100} \pmod{11}$
- (c) $13^{100} \pmod{13}$

Proof. The crux of the proof lies in the function $h_a : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ defined in (1). Indeed, consider the following sets

$$A = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \dots, p-1\} \quad \text{and} \quad B = \{h_a(x) : x \in A\}$$

As we established above, the set B is the same as the set A . And therefore,

$$\prod_{z \in A} z = \prod_{z \in B} z = \prod_{x \in A} h_a(x) = \prod_{x \in A} (ax \pmod p)$$

Taking both sides modulo p , we get

$$\left(\prod_{z \in A} z \right) \pmod p = \left(\prod_{x \in A} (ax \pmod p) \right) \pmod p = \left(a^{p-1} \cdot \prod_{x \in A} x \right) \pmod p$$

Let us call $Q := (\prod_{z \in A} z) \pmod p$. Then, we get

$$Q \pmod p = (a^{p-1} Q) \pmod p \quad \Rightarrow \quad Q \cdot (a^{p-1} - 1) = 0 \pmod p$$

That is, p divides $Q \cdot (a^{p-1} - 1)$. Since each of the numbers $x \in A$ has $\gcd(x, p) = 1$, we have $\gcd(Q, p) = 1$. That is, p doesn’t divide Q . Since p is a prime, we must have that p divides $a^{p-1} - 1$. That is, $a^{p-1} = 1 \pmod p$. □

Exercise: Check if the above would be true if p were not a prime but the only restriction was $\gcd(a, n) = 1$. In particular, find a, n such that $\gcd(a, n) = 1$ but $a^{n-1} \not\equiv_n 1$.

Remark: After doing the above exercise you should ask yourself: where all is the property that p is prime used? If you think about it clearly enough, you will indeed prove that if $\gcd(a, n) = 1$, then there is indeed some number ϕ such that $a^\phi \equiv_n 1$. The Extra Credit Problem explores this.

