CS30 (Discrete Math in CS), Summer 2021 : Lecture 28

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. **When is "dividing out" OK.** Recall in a previous lecture, I gave a caveat that if $ab \equiv_n ac$, then one cannot "cancel" or "divide out" a to get $b \equiv_n c$. We saw the example, $3 \cdot 2 \equiv_6 3 \cdot 4$, but $2 \not\equiv_6 4$.

   However, if a and n are *relatively prime* then one can indeed "divide out." We will use this fact multiple times. However, every time you use it, be careful to see the premise holds. We start with the case when the RHS is 0.

   Theorem 1. Let a and n be two relatively prime numbers. That is, $\gcd(a, n) = 1$. Then,

   $$ab \equiv_n 0 \quad \Rightarrow \quad b \equiv_n 0$$

   That is, if n divides ab, then n must divide b.

   Proof. It is an almost-one-liner from Bezout's identity. $\gcd(a, n) = 1$ implies there exists integers x and y such that

   $$xa + yn = 1 \quad \text{which, multiplying both sides by } b \text{ gives} \quad xab + ynb = b$$

   Now take modulo n. $ab \equiv_n 0 \Rightarrow xab \equiv_n 0$. We also have $yan \equiv_n 0$ since n is a factor. So, $b = xab + ynb \equiv_n 0$ □

   As a corollary, we get the "dividing out" theorem.

   Theorem 2 (Dividing out with relatively prime numbers)**.**

   Let a and n be two relatively prime numbers. That is, $\gcd(a, n) = 1$. Then,

   $$ab \equiv_n ac \quad \Rightarrow \quad b \equiv_n c$$

   That is, if we can "divide/cancel out" a from both sides.

   Proof. $ab \equiv_n ac \Rightarrow a(b - c) \equiv_n 0$. Above theorem implies $(b - c) \equiv_n 0 \Rightarrow b \equiv_n c$. □

   Another corollary is the following fact when n is prime.

   Theorem 3. Let p be a prime number. If p divides the number ab, then p must divide a or p must divide b or both.

   Proof. p divides ab implies $ab \equiv_p 0$. If p divides a, we are done. If p doesn't divide a, then $\gcd(a, p) = 1$ because p is a prime. Theorem 1 implies $b \equiv_p 0$. That is, p divides b. □

Remark: *The above fact indeed is the first step to* unique factorization *which states that any number n can be written as a product of primes in one and only one way. We already saw the "one way" via strong induction (remember?). To see a glimpse of the "only one" way, suppose n can be written as pq and rs where these are all 4 distinct primes. Well, then $pq = rs$. That is, p divides rs. And so, by the above theorem, p divides r or p divides s. But r and s are primes distinct from p. Contradiction. I leave the general proof of the unique factorization (which we were asked to believe in grade school) to the interested reader.*

2. **Multiplicative Inverse.** Next, we see a very important concept of the *multipicative inverse* or the reciprocal.

Theorem 4. For any positive integer n and $a \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$, there exists **one and only one** integer $b \in \mathbb{Z}_n$ such that $ab \equiv_n 1$. This number is called the ***multiplicative inverse*** of a modulo n, and denoted as a^{-1}.

Proof. First we show there is at least one such b. 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 $b = x \bmod n$.

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* $10 \cdot 12 \equiv_{17} 1$.

Next, we show *uniqueness*. We prove this via contradiction. Suppose there exist *two* unequal numbers b and c in $\mathbb{Z}_n$ such that both $ab \equiv_n 1$ and $ac \equiv_n 1$. But then, we would have $ab \equiv_n ac$, and since $\gcd(a, n) = 1$, by Theorem 2 we would have $b \equiv_n c$. This contradicts that they were unequal. Contradiction. □

The next theorem shows that if a has an inverse modulo n, then a and n *must* be relatively prime.

Theorem 5. If there exists a number $b \in \mathbb{Z}_n$ such that $ab \equiv_n 1$, then $\gcd(a, n) = 1$.

Proof. If $ab \equiv_n 1$, then it means there is an integer q (the quotient) such that $ab = qn + 1$. But then, $ab - qn = 1$. That is, we have written 1 as an integer linear combination of a and n. Therefore, $\gcd(a, n) = 1$. To recall why, if $\gcd(a, n) = g$, then g divides both ab (since g divides a), qn (since g divides n), and thus, $ab - qn$, that is, g divides 1. g must be 1. □

The above two theorems thus give an algorithm to obtain the multiplicative inverses.

```
1: procedure MULTINV(a, n) ▷ Assumes a, n are positive integers.
2:     ▷ Returns a^{-1} mod n if gcd(a, n) = 1.
3:     (g, x, y) ← EXTGCD(a, n) ▷ We first run EXTGCD to get combination xa + yn = 1.
4:     if g = 1 then:
5:         return x mod n. ▷ See proof of Theorem 4
6:     else:
7:         return "No Multiplicative Inverse" ▷ See Theorem 5
```

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* basically allows us to "divide" out numbers like we do "usually". (Technically, $\mathbb{Z}_p$ is a "field" in case you have taken an abstract algebra course). This has many applications. Here is one.

Theorem 6. 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 $\mathbb{Z}_p$

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

Remark: *To compare with the case of rationals, if $a \neq 0, b, r$ are all rational numbers, then $ax + b = r$ has a unique solution giveb by $x = \frac{b-r}{a} = a^{-1} \cdot (b - r)$. The above theorem says if we restrict to the ring $\mathbb{Z}_p$ and $a \not\equiv_p 0$, then there is a unique solution here as well.*

Remark: *I stress again we* **need** *p to be prime. For instance, when $n = 6$, there is* **no** *solution to the equation $3x \equiv_6 1$. Check it.*

Proof. Let a^{-1} be the multiplicative inverse of a modulo p. This exists since p is a prime and $a \neq 0$. Then the solution is

$$x := a^{-1}(r - b) \bmod p$$

Indeed check: $ax \equiv_p (aa^{-1})(r - b) \equiv_p (r - b)$, and so $ax + b \equiv_p r$.

Why is it unique? Again, the dividing out rule (Theorem 2). If $ax + b \equiv_p r \equiv_p ay + b$, then we get $ax \equiv_p ay$ which implies $x \equiv_p y$ since $\gcd(a, p) = 1$. Thus, there is exactly one solution in $\mathbb{Z}_p$. □

Example. Let's take $p = 17$ and consider the equation

$$12 \cdot x + 7 \equiv_{17} 4$$

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 a theorem for two variables, and I build this in the UGP. This is also used in the (highly recommended) extra credit problem about hash functions.

Theorem 7. Let p be a prime. Let $a \neq c$ be two elements in $\mathbb{Z}_p$. Let b, d be any two elements in $\mathbb{Z}_p$. Then the following system of equations has a unique solution over $\mathbb{Z}_p$.

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

$$c \cdot x + y \equiv_p d$$

Proof. Again, we proceed as in the case of reals. We subtract, to get

$$(a - c) \cdot x \equiv_p (b - d)$$

Since $a \neq c$, we get $(a - c)$ has an inverse in $\mathbb{Z}_p$ (since p is a prime). Therefore, the unique solution (again, unique for reasons as in the previous theorems) is

$$x = \left((b - d) \cdot (a - c)^{-1}\right) \bmod p$$

And once we solve for x, we can solve for y as

$$y = (b - ax) \bmod p$$

□

Example. Consider the system of equations

$$5x + y \equiv_7 3$$

$$2x + y \equiv_7 6$$

The above formulas suggest

$x \equiv_7 (3 - 6) \cdot (5 - 2)^{-1} \equiv_7 (-3) \cdot (3)^{-1} \equiv_7 (-1)(3) \cdot (3^{-1}) \equiv_7 -1 \equiv_7 6.$

And $y \equiv_7 (3 - 5x) \equiv_7 (3 - (-5)) \equiv_7 8 \equiv_7 1.$

Indeed, check: $5 \cdot 6 + 1 = 31 \equiv_7 3$ and $2 \cdot 6 + 1 = 13 \equiv_7 6$.