CS 30: Discrete Math in CS (Winter 2019): Lecture 9

Date: 17th January, 2019 (Thursday)
Topic: 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. **Recap regarding GCDs.**

   - If $\gcd(a, b) = g$ then there exists integers (x, y) such that $xa + yb = g$.
   - The EXTGCD algorithm returns one such pair (x, y).

   In this lecture we will also use the following fact which *you* will prove in PSet 3, 1(d):

   Fact 1. If $\gcd(a, n) = 1$ and b be an integer such that $ab \equiv_n 0$, then $b \equiv_n 0$.

2. **A useful corollary.**

   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. We give a direct constructive proof. Since $\gcd(a, n) = 1$, there exists integers x, y such that $xa + yn = 1$. Therefore, $xa \equiv_n 1$, and in particular, $(x \bmod n) \cdot a \equiv_n 1$. Thus, the answer we are looking for is $(x \mod n)$. □

   Remark: *The* EXTGCD *algorithm can be used to find such a number b.*

3. **Unique Mappings.** Here is another fun fact about coprime numbers. For any positive number n, and any $a \in \mathbb{Z}_n$ with $\gcd(a, n) = 1$, consider the following numbers $(a \cdot 0) \bmod n$, $(a \cdot 1) \bmod n, \cdots, (a \cdot (n-1)) \bmod n$ In other words we are looking at the set

$$S_{a,n} := \{(a \cdot x) \bmod n : \ x \in \mathbb{Z}_n\}$$

   To take an example, consider $n = 7$ and $a = 3$. We get that the set

$$S_{3,7} = \{0, 3, 6, 2, 5, 1, 4\}$$

   As you can see, the set $S_{3,7}$ is the *same* as $\mathbb{Z}_7$. We next show this is not a coincidence.

   Theorem 2. Given any positive integer n and $a \in \mathbb{Z}_n$ with $\gcd(a, n) = 1$, the set $S_{a,n} = \mathbb{Z}_n$.

Proof. Every element of $S_{a,n}$, that is, $(a \cdot x) \bmod n$ is an element of $\mathbb{Z}_n$ by definition. Therefore, $S_a \subseteq \mathbb{Z}_n$. To show that these are the same, we in fact show that the map $\phi_a : \mathbb{Z}_n \to S_{a,n}$

$$\phi_a : x \mapsto (a \cdot x) \bmod n$$

is *injective*. An injection from a *finite* set to its subset can exist only if the subset is the whole set (and therefore the injection is a bijection). To see this, the injective property implies $|\mathbb{Z}_n| \leq |S_{a,n}|$ (this makes sense since we have finite set), and the only subset whose cardinality is at least as large as the set is the set itself.

To show the injective property, we need to show that for any $x \neq y$ in $\mathbb{Z}_n$, we have $(a \cdot x) \bmod n \neq (a \cdot y) \bmod n$. For the sake of contradiction, suppose there does exist such x and y. Without loss of generality, assume $x > y$.

Since $a \cdot x \equiv_n a \cdot y$, we get $a \cdot (x - y) \equiv_n 0$. Call the number $(x - y)$ as b. Note $1 \leq b \leq n - 1$; the first inequality follows since $x > y$, and the second follows since both $x, y \in \mathbb{Z}_n$. By Fact 1, we get $b \equiv_n 0$ which is a contradiction since $1 \leq b \leq n - 1$. □

4. **Multiplicative Inverse.** Using the above theorems, we see that for any positive number n and any $a \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$, there is an *unique* number $b \in \mathbb{Z}_n$ such that $ab \equiv_n 1$. This number is called the *multiplicative inverse* of a in $\mathbb{Z}_n$, and is denoted as a^{-1}. ✍

   Exercise: *Find the multiplicative inverse of* 2 *in* $\mathbb{Z}_3$, 3 *in* $\mathbb{Z}_5$, 8 *in* $\mathbb{Z}_{21}$.

   ✍

   Exercise: *Write code to find the multiplicative inverse of any* a *modulo* n *such that* a *and* n *are coprime.*

5. **Fermat's Little Theorem.** We now use multiplicative inverses to prove the following beautiful theorem: it says that for any prime p and any integer a such that $\gcd(a, p) = 1$, p must divide $a^{p-1} - 1$.

   Theorem 3. For any $a \in \{1, 2, 3, \ldots, p - 1\}$, $a^{p-1} \equiv_p 1$.

   Remark: *Note that the above theorem is for* $a \in \mathbb{Z}_p \setminus \{0\}$. *For any (larger)* a *with* $\gcd(a, p)$, *we can simply map* $a \mapsto a \bmod p$, *and use that* $a^{p-1} \equiv_p (a \bmod p)^{p-1}$.

   Remark: *The above allows us to do must "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: *What is the remainder of* 5^{1234} *when divided by* 11*?*

Proof. (Fermat's Little Theorem)

Let us write the proof elaborately.

- The key is to look at a slightly different set than $S_{a,p}$. Define $S'_{a,p} = S_{a,p} \setminus \{0\}$. Since $S_{a,p} = \mathbb{Z}_p$, this set is simply $\{1, 2, \ldots, p-1\}$. To write it explicitly,

$$\{(a \cdot x) \bmod p : x \in \{1, 2, \ldots, p-1\}\} = \{1, 2, \ldots, p-1\} \tag{1}$$

  It's the same set, so taking the product of the elements gives the same numbers.

- Just for brevity's sake, lets call the set in the LHS of (1) A and the set in the RHS of (1) B. Now we write an almost trivial statement

$$\prod_{z \in A} z = \prod_{y \in B} y \tag{2}$$

- If two numbers are same, then surely their remainders when divided by p is same. So,

$$\left(\prod_{z \in A} z\right) \bmod p = \left(\prod_{y \in B} y\right) \bmod p = Q \bmod p \tag{3}$$

  Now, $\prod_{y \in B} y$ is nothing but $(p-1)!$. Again, for brevity's sake, I am going to call $Q := (p-1)!$, which is what I have shown above in the second equality.

- Now comes the main observation. Consider the expression in the LHS of (3). The set A is $\{(a \cdot x) \bmod p : x \in \{1, 2, \ldots, p-1\}\}$, and so

$$\left(\prod_{z \in A} z\right) \bmod p = \Big((a \cdot 1) \bmod p \cdot (a \cdot 2) \bmod p \cdots (a \cdot (p-1)) \bmod p\Big) \bmod p$$

  Recall that $(u \mod n) \cdot (v \mod n) \equiv_n u \cdot v$. Therefore, we can take all the $\bmod p$ outside to get

$$\left(\prod_{z \in A} z\right) \bmod p = \Big(\prod_{x \in \{1,2,\ldots,p-1\}} (a \cdot x)\Big) \bmod p = \left(a^{p-1} Q\right) \bmod p \tag{4}$$

  The last equality follows since there are exactly $(p-1)$ a's in the product and the rest product up to give $(p-1)! = Q$. Substituting (4) in (3), we get

$$a^{p-1} Q \equiv_p Q \quad \Rightarrow \left(a^{p-1} - 1\right) Q \equiv_p 0 \tag{5}$$

- Finally, what is $\gcd(Q, p)$? Well, $Q = (p-1)!$. Now a corollary of Fact 1 gives us that if a *prime* p doesn't divide a, and doesn't divide b, then it doesn't divide ab (do you see this? It uses the fact that if a number a doesn't divide p then $\gcd(a, p) = 1$)

Remark: *This requires primeness – 6 doesn't divide 9, 6 doesn't divide 4, but it sure divides* $9 \times 4 = 36$.

So, since p doesn't divide $2, 3, 4, \ldots, (p-1)$, p doesn't divide $(p-1)!$, and therefore (since p is a prime) $\gcd(p, Q) = 1$.

- But if $\gcd(p, Q) = 1$ and $Q \cdot (a^{p-1} - 1) \equiv_p 0$, again using Fact 1 we get that $a^{p-1} - 1 \equiv_p 0$. We have proved Fermat's Little Theorem.

□

✍

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 in PSet 3 explores this.*