

Announcements:

Lecture notes for the second class are online.

Topics for today:

1. More on the Euclid's gcd algorithm
2. The multiplicative group $\mathbf{Z}/n\mathbf{Z}^*$
3. Linear Congruences
4. Subgroups

Lecture:

Henceforth we'll use the notation (a, b) as shorthand for $\gcd(a, b)$. In the last lecture we discussed about how $(a, b) = (b, r)$ where $a = qb + r$, $0 \leq r < b$ was the primary idea in Euclid's gcd algorithm. We also showed that if a and b are n -bit integers then computing gcd with Euclid's method requires $O(n)$ divisions and using naive arithmetic it takes $O(n^3)$ bit operations to calculate the greatest common divisor. As part of HW #1 (which will be announced in the next class) you'll be asked to show that a variant of Euclid's gcd actually takes time $O(n^2)$. Next we'll give some intuition as to why this is the true by looking at a particular case.

Suppose $b > \frac{a}{2}$ then $q = 1$ and so

$$(a, b) = \begin{cases} (b, a - b) & \text{when } b > \frac{a}{2} \\ (a - b, b) & \text{when } b \leq \frac{a}{2} \end{cases}$$

And as atmost 2 subtractions are required to reduce the size of the problem by half, we need atmost $2n$ subtractions. Hence computing gcd in this fashion requires $O(n^2)$ bit operations.

Last time we also introduced the notion of a group. One of the consequences of the group axioms is that the inverse of a group element is unique. Can you prove it?

The multiplicative group $\mathbf{Z}/n\mathbf{Z}^*$

Consider the set $\mathbf{Z}/n\mathbf{Z} = \{[0], [1], \dots, [n-1]\}$. We can think of this set as the set of integers $\{0, 1, \dots, n-1\}$ under modular addition. When $n = 3$ the group table for $(\mathbf{Z}/3\mathbf{Z}, +)$ is as follows:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Does $(\mathbf{Z}/3\mathbf{Z}, *)$ form a group?

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

No. What if we exclude 0?

*	1	2
1	1	2
2	2	1

Yes! It's a group with 2 elements and we'll denote it by $(\mathbf{Z}/3\mathbf{Z} - 0, *)$. So is $\mathbf{Z}/n\mathbf{Z} - 0$ a group under multiplication? Let's take $n = 4$ and look at $(\mathbf{Z}/4\mathbf{Z} - 0, *)$

*	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$2 * 2 = 0$ and hence it's not closed and 2 doesn't seem to have an inverse. But we notice that 3 has an inverse as it is relatively prime to 4. $(3, 4) =$

$1 \Rightarrow 3x + 4y = 1 \Rightarrow 3x \equiv 1 \pmod{4}$ and x is the inverse of 3. More generally, if $(a, n) = 1$ Euclid's algorithm guarantees existence of $x, y \in \mathbf{Z}$ such that $ax + ny = 1$ which implies $n \mid ax - 1 \Rightarrow ax \equiv 1 \pmod{n}$.

If we consider the set of integers which relatively prime to n the above argument assures us of inverses for these integers. For example $\mathbf{Z}/6\mathbf{Z} = \{0, \mathbf{1}, 2, 3, 4, \mathbf{5}\}$

$*$	1	5
1	1	5
5	5	1

Why is such a set closed? $(a, b) = (b, n) = 1 \Rightarrow (ab, n) = 1$. Also if $ax \equiv 1 \pmod{n}$, $(a, n) = 1$ then $(x, n) = 1$. Otherwise $\exists d > 1$ such that $d \mid x, d \mid n$. $ax \equiv 1 \pmod{n} \Rightarrow \exists y, ax - 1 = yn \Rightarrow 1 = ax - yn \Rightarrow d \mid ax - yn = 1$. Contradiction as a number greater than 1 cannot divide 1! So both a and it's inverse are prime to n . Therefore we have a closed set. We introduce a new notation to talk about this interesting set.

$\mathbf{Z}/n\mathbf{Z}^* = \{a \in \mathbf{Z}/n\mathbf{Z} \mid (a, n) = 1\} = \{1 \leq a \leq n - 1 \mid (a, n) = 1\}$. $(\mathbf{Z}/n\mathbf{Z}^*, *)$ is a group and as $*$ is commutative we have an abelian group. The order (= size) of this group plays an important role in classical # Theory and cryptography and is assigned a special symbol ϕ (read as phi). $\phi(n) := |\mathbf{Z}/n\mathbf{Z}^*|$. So $\phi(6) = |\{1, 5\}| = 2$, $\phi(4) = |\{1, 3\}| = 2$. Also $\phi(p) = |\{1, \dots, p - 1\}| = p - 1$

Is there a unique inverse for an element $\in \mathbf{Z}/n\mathbf{Z}^*$? Say $ax \equiv 1 \pmod{n}$ and $ay \equiv 1 \pmod{n} \Rightarrow n \mid ax$ and $n \mid ay \Rightarrow n \mid a(x - y)$. As $(a, n) = 1$, we have $n \mid (x - y) \Rightarrow x \equiv y \pmod{n}$. Hence the inverse is unique modulo n . And we know how to calculate it using Euclid's gcd algorithm. $(a, n) = 1 \Rightarrow \exists x, y \in \mathbf{Z}$, $ax + ny = 1 \Rightarrow ax \equiv 1 \pmod{n}$. Sometimes we'll write the inverse of a as a^{-1} .

Linear Congruences

Next, let's solve linear congruences which are of the form $ax \equiv b \pmod{n}$ with $(a, n) = 1$. Notice that when $b = 1$ this reduces to computing the inverse of a . Now as a is relatively prime to n , $a^{-1} \pmod{n}$ exists. And so multiplying both sides of the linear congruence $ax \equiv b \pmod{n}$ by $a^{-1} \pmod{n}$, we get $a^{-1}(ax) \equiv a^{-1}b \pmod{n}$. Using associativity of $*$ and $a^{-1}.a = 1$, we get $x \equiv a^{-1}b \pmod{n}$. If we plug this x back into the original linear congruence we

see that the congruence is satisfied and that a unique solution exists provided $(a, n) = 1$.

On the other hand say $d = (a, n) > 1$. If $ax \equiv b \pmod n$ then $\exists y, ax - b = yn$. But $d|n, d|a$ implies $d|b$. Therefore $ax \equiv b \pmod n$ has a solution only if $(a, n)|b$. So let's suppose $d|b$ and $a = da_1, b = db_1, n = dn_1$. So $ax \equiv b \pmod n \Leftrightarrow da_1x \equiv db_1 \pmod{dn_1} \Leftrightarrow dn_1|d(a_1x - b_1) \Leftrightarrow n_1|(a_1x - b_1) \Leftrightarrow a_1x \equiv b_1 \pmod{n_1}$. Now as $(a_1, n_1) = 1$ we can solve for x in the last congruence and reconstruct the original solution.

So if $(a, n) = d$ then $ax \equiv b \pmod n$ is solvable $\Leftrightarrow d|b$ in which case we are reduced to solving $a_1x \equiv b_1 \pmod{n_1}$ where $a = da_1, b = db_1, n = dn_1$.

Exercise: How many solutions does $ax \equiv b \pmod n$ have?

So far we've seen two interesting groups $(\mathbf{Z}/n\mathbf{Z}, +), (\mathbf{Z}/n\mathbf{Z}^*, *)$ and the latter plays an important role in cryptography.

Subgroups

Can we construct subsets of $\mathbf{Z}/15\mathbf{Z}$ which form a group under addition?

1 generates the entire group $\mathbf{Z}/15\mathbf{Z}$ as

$$\begin{aligned} 1 \\ 1 + 1 = 2 \\ 1 + 1 + 1 = 3 \\ \dots \\ 1 + 1 + \dots + 1 = 14 \\ 1 + 1 + \dots + 1 + 1 = 0 \end{aligned}$$

And so does 2. But 3 only generates

$$\begin{aligned} 3 \\ 3 + 3 = 6 \\ 3 + 3 + 3 = 9 \\ 3 + 3 + 3 + 3 = 12 \\ 3 + 3 + 3 + 3 + 3 = 0 \end{aligned}$$

$\{3, 6, 9, 12, 0\}$ before starting all over again. The reason why 2 generates $\mathbf{Z}/15\mathbf{Z}$ but not 3 is because 3 and 15 are not relatively prime. On the contrary as $(2, 15) = 1$ we can solve the linear congruence $2x \equiv b \pmod{15}$ for all b . And hence all $b \in \mathbf{Z}/15\mathbf{Z}$ can be generated as multiples of 2.

Definition Suppose (G, \odot) is a group and $H \subset G$, then (H, \odot) is a *subgroup* of (G, \odot) if (H, \odot) is a group. In other words we'll say that H is a

subgroup of G if H inherits group properties from G . Ex. $\{3, 6, 9, 12, 0\}$ is a subgroup of $\mathbf{Z}/15\mathbf{Z}$ under $+$. Check!

Let $x \in G$. Now the idea is to consider the smallest subgroup of G which contains x .

$$\begin{aligned} x^{(2)} &:= x \odot x \in G \\ x^{(3)} &:= x \odot x^{(2)} \in G \\ &\dots \\ x^{(i)} &:= x \odot x^{(i-1)} = x \odot x \odot \dots \odot x \in G \end{aligned}$$

We must also have an identity $e := x^0$ and inverses for the above elements x^{-1}, x^{-2}, \dots . So the subgroup containing x must be atleast as big as (infact it is equal to) $\{x^{(i)} \mid i \in \mathbf{Z}\}$. This subgroup is denoted by $\langle x \rangle$ and is called the subgroup generated by x .

Is this set closed? Yes. $x^{(i)} \odot x^{(j)} = x^{(i+j)}$

Ex. $x^{(2)} \odot x^{(-3)} = x^{(2)} \odot x^{(2)} \odot x^{(-1)} \odot x^{(-1)} \odot x^{(-1)} = x^{(-1)}$

The identity $x^0 \in \langle x \rangle$. Inverses exist and it's associative. Hence $\langle x \rangle$ is a group and is the smallest subgroup of G containing x . The way we've defined $\langle x \rangle$ it looks like we need negative indeces. Here's some food for thought until next time: Suppose G is finite show that for $x \in G$, $\langle x \rangle = \{x^i \mid i \geq 0\}$ and is a finite subgroup.