Lecture 3.2

Last time:

- If $\gcd(a,b) = d$ then solutions to

$$ax + by = d$$

are all of the form

$$(x,y) = \left(x_0 + \frac{bk}{d}, y_0 - \frac{ak}{d}\right)$$

where (x_0, y_0) can be found using the gcd algorithm.

- Every $n \in \mathbb{N}$ has a unique factorization into powers of primes:

$$n = p_1^{k_1} \cdots p_r^{k_r}.$$

To prove the uniqueness portion of the

FTA, we need:

Lemma (a) If p is prime and $p \mid ab$ for some $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

(b) If p and $q_1, \ldots, q_r$ are primes and $p \mid q_1 \cdots q_r$ then $p = q_i$ for some $1 \leq i \leq r$.

Pf: (a) Suppose $p \nmid a$. Then $\gcd(p, a) = 1$ so there are $x, y \in \mathbb{Z}$ solving

$$px + ay = 1.$$

Multiplying by b gives

$$pbx + aby = b$$

but $p \mid ab$ so p divides the entire expression $pbx + aby$, hence also b.

(b) If $r = 1$, we must have $p = q_1$.

If $r > 1$, apply (a) to the product $q_1 (q_2 \cdots q_r)$ to see that $p = q_1$ or $p \mid q_2 \cdots q_r$.

In the latter case, repeat until we find $p = q_i$. □

Pf of Uniqueness in FTA: Suppose n has two prime factorizations:

$$n = p_1^{k_1} \cdots p_r^{k_r} = q_1^{l_1} \cdots q_s^{l_s}.$$

Then $p_1 \mid q_1^{l_1} \cdots q_s^{l_s}$ so by (b) of the Lemma, $p_1 = q_j$ for some $1 \leq j \leq s$.

By changing the order of the q_j, we can assume $p_1 = q_1$.

Cancelling out factors of p_1 and q_1 leaves us with

$$p_2^{k_2} \cdots p_r^{k_r} = q_1^{l_1 - k_1} q_2^{l_2} \cdots q_s^{l_s}$$

or $$p_1^{k_1 - l_1} p_2^{k_2} \cdots p_r^{k_r} = q_2^{l_2} \cdots q_s^{l_s},$$

let's say it's the first option.

If $\ell_1 - k_1 > 0$, then q_1 divides the product $p_2^{k_2} \cdots p_r^{k_r}$, hence by (b) of the Lemma again, $q_1 = p_i$ for some $2 \leq i \leq r$.

But this is impossible since $q_1 \neq p_1$.

Therefore $\ell_1 - k_1 = 0$ and we are left with $p_2^{k_2} \cdots p_r^{k_r} = q_2^{\ell_2} \cdots q_s^{\ell_s}$.

Now repeat until all p_i and q_j are identified. □

The upshot of this theorem is that we can learn almost everything there

is to know about $\mathbb{N}$ by studying the prime numbers $2, 3, 5, 7, 11, \ldots$

The bad news is primes are notoriously hard to study.

Even "is this number prime?" can be difficult to answer, though in theory one needs only test all primes $p \leq \sqrt{n}$ as we showed earlier.

More on primes in a few lectures...

Modular Arithmetic

Recall that $a \equiv b \pmod{n}$ if n divides $b - a$, or equivalently if $a = nq + b$ for some $q \in \mathbb{Z}$.

By Exercise 3 in Lecture 2.1, $\equiv$ is an equivalence relation on $\mathbb{Z}$, meaning the integers can be partitioned into congruence classes mod n.

Ex 1 For $n = 2$, the congruence classes are exactly the even and odd numbers:

$$2\mathbb{Z} = \{a \in \mathbb{Z} \mid a = 2q,\ q \in \mathbb{Z}\}$$

$$2\mathbb{Z}+1 = \{a \in \mathbb{Z} \mid a = 2q+1,\ q \in \mathbb{Z}\}.$$

(2) For $n = 3$, the congruence classes are:

$$3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$$

$$3\mathbb{Z}+1 = \{3k+1 \mid k \in \mathbb{Z}\}$$

$$3\mathbb{Z}+2 = \{3k+2 \mid k \in \mathbb{Z}\}.$$

In general, modulo n, there are n distinct congruence classes, written $[0], [1], \ldots, [n-1]$, where

$$[r] = \{nk + r \mid k \in \mathbb{Z}\}.$$

Prop Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$.

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

then:

(a) $a + c \equiv b + d \pmod{n}$.

(b) $a - c \equiv b - d \pmod{n}$.

(c) $ac \equiv bd \pmod{n}$.

That is, we can do arithmetic with congruence classes:

$$[a] + [c] = [a + c]$$

$$[a] - [c] = [a - c]$$

$$[a][c] = [ac]$$

since each of these is "well-defined

mod n".

WARNING: Divisibility doesn't work the same way, i.e. it is <u>not</u> true that if $[a][c] = [b][c]$ and $[b] \neq [0]$ then $[a] = [c]$.

Ex For $n = 6$,

$$2 \cdot 3 \equiv 4 \cdot 3 \pmod{6}$$

but $2 \not\equiv 4 \pmod{6}$.

Exercise 1: Prove that if p is

prime, then "cancellation mod p" does work: if $ac \equiv bc \pmod{p}$ and $c \not\equiv 0 \pmod{p}$ then $a \equiv b \pmod{p}$.

Can you find any composite modulus with this property?

Now that we can do arithmetic modulo n, we can try to solve basic equations modulo n.

Ex Find all solutions to

$$x + 12 \equiv 5 \pmod{8}.$$

We can "subtract mod 8" to get

$$x + 12 - 12 \equiv 5 - 12 \pmod{8}$$

$$x \equiv -7 \pmod 8$$

whose solutions are

$$[-7] = \{a \in \mathbb{Z} \mid a \equiv -7 \pmod 8\}$$

$$= \{-7 + 8k \mid k \in \mathbb{Z}\}$$

$$= \{\ldots, -15, -7, 1, 9, 17, \ldots\}.$$

Since $\equiv$ is an equivalence relation, we could write the solution as $[n]$ for any $n \in [-7]$, such as $[1]$.

Ex Let's solve

$$4x \equiv 3 \pmod{19}.$$

Here's a clever trick: multiply both sides by 5!

$$20x \equiv 15 \pmod{19}.$$

Since $20 \equiv 1 \pmod{19}$, this becomes

$$x \equiv 15 \pmod{19}.$$

Thus $[15] = \{15 + 19k \mid k \in \mathbb{Z}\}$ is the set of solutions.

In general, we may ask for solutions to linear equations:

$$ax \equiv c \pmod{n}.$$

Theorem Let $a, c \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $\gcd(a,n) = d$. Then

(1) If $d \nmid c$, there are no solutions to

$$ax \equiv c \pmod{n},$$

(2) If $d \mid c$, there are exactly d solutions to $ax \equiv c \pmod{n}$ which are not congruent mod n. One is

$$x_0 = \frac{cu}{d}$$

where $au + nv = d$ and all solutions are parametrized by

$$x \equiv x_0 + \frac{nk}{d} \pmod{n}$$

for $0 \leq k < n$.

Pf: (1) We are looking for $x \in \mathbb{Z}$ such that n divides $ax - c$, i.e. $ax - c = ny$ for some $y \in \mathbb{Z}$. This can be rewritten

$$ax - ny = c$$

which we know has a solution if and only if $d \mid c$.

(2) Now assuming $d \mid c$, let $u, v \in \mathbb{Z}$ satisfy $au - nv = d$.

Multiplying through by $\frac{c}{d}$ yields

$$a\left(\frac{cu}{d}\right) - n\left(\frac{cv}{d}\right) = c$$

$$\Rightarrow \quad n \mid a\left(\frac{cu}{d}\right) - c.$$

So $x_0 = \frac{cu}{d}$ satisfies $ax \equiv c \pmod{n}$.

Exercise 2: Show that all solutions are of the form

$$x \equiv x_0 + \frac{nk}{d} \pmod{n}$$

for $0 \leq k < d$.

This exercise finishes the proof. □

Let's solve

$$8x \equiv 12 \pmod{20}.$$

Here, $\gcd(8, 20) = 4$ which divides 12, so we will have 4 solutions.

To start,

$$20 = 8 \cdot 2 + 4$$

($\gcd(8, 20)$)

$$\Longrightarrow 4 = 8(-2) + 20(1).$$

So $x_0 = \frac{12 \cdot -2}{4} = -6$ is a solution to $8x \equiv 12 \pmod{20}$:

$$8x_0 = 8(-6) = -48$$

and $-48 - 12 = 60 = 20 \cdot 3$.

All 4 solutions are given by

$$x \equiv x_0 + \frac{20k}{4} \equiv -6 + 5k \pmod{20}.$$

Explicitly, they are the congruence classes

$$[-6],\ [-1],\ [4],\ [9].$$

$$\| \qquad \|$$

$$[14] \qquad [19]$$

Next time: nonlinear congruences.