Lecture 3.1

Last time:

- The Division Algorithm lets us express "quotients with remainder":

$$a = bq + r$$

for unique $q, r \in \mathbb{Z}$ with $0 \leq r < b$.

- For $a, b \in \mathbb{Z}$, $\gcd(a,b)$ can be computed by a finite sequence of DA steps.

- $\gcd(a,b) = 1 \iff ax + by = 1$ for some $x, y \in \mathbb{Z}$.

Linear Equations

We saw that when $\gcd(a,b) = 1$, it is possible to write 1 as a $\mathbb{Z}$-linear combination of a and b.

Moreover, if $ax + by = 1$ has a solution, then so does $ax + by = n$ for any $n \in \mathbb{N}$. (Why?)

What happens if $\gcd(a,b) > 1$?

Theorem Let $a, b \in \mathbb{Z}$, not both 0, and set $d = \gcd(a,b)$. Then there

are $x, y \in \mathbb{Z}$ satisfying

$$ax + by = d$$

and given one such solution (x, y), every other solution is of the form

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

for some $k \in \mathbb{Z}$.

Pf: For existence of x, y, it's possible to just adapt our proof for $d = 1$, but here's a slicker proof.

Since $d|a$ and $d|b$, we can rewrite

$ax + by = d$ as

$$\frac{a}{d}x + \frac{b}{d}y = 1.$$

Now $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ so by the $d=1$ case, there's a solution (x,y).

The other solutions are easy to solve for by reducing to the $d=1$ case and comparing the equations

$$ax + by = 1 \quad \text{and} \quad ax' + by' = 1$$

for two different solutions $(x,y), (x',y')$. □

Exercise 1: (a) Verify that for

any $a, b \in \mathbb{Z}$ with $\gcd(a,b) = d$,

$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$

(b) Show that all solutions to

$$ax + by = d$$

have the form described in the Theorem.

Ex Let's find all integer solutions to

$$60x + 22y = d$$

where $d = \gcd(60, 22)$. The division algorithm produces

$$60 = 22 \cdot 2 + 16$$

$$22 = 16 \cdot 1 + 6$$

$$16 = 6 \cdot 2 + 4$$

$$6 = 4 \cdot 1 + \boxed{2} \quad \leftarrow d = 2$$

$$4 = 2 \cdot 2 + 0$$

and one solution to $60x + 22y = 2$

is found by working backwards:

$$2 = 6 - 4 \cdot 1 = 6 - (16 - 6 \cdot 2)$$

$$= 6 \cdot 3 - 16 = (22 - 16 \cdot 1) \cdot 3 - 16$$

$$= 22 \cdot 3 - 16 \cdot 4 = 22 \cdot 3 - (60 - 22 \cdot 2) \cdot 4$$

$$= 60 \cdot \underbrace{\boxed{-4}}_{x} + 22 \cdot \underbrace{\boxed{11}}_{y}$$

Then every solution is of the form

$$\left(-4+\frac{22k}{2},\ 11+\frac{60k}{2}\right) = (-4+11k,\ 11+30k).$$

Prime Factorization

Recall that $p \in \mathbb{N}$ is prime if its only positive factors are 1 and p.

Proposition Let $n > 1$ be a natural number.

(a) There exists a prime $p \in \mathbb{N}$ dividing n.

(b) n is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divide n.

Pf: (a) If there were some $n > 1$

with no prime divisor, n itself would be composite.

Let n be the smallest natural number > 1 with no prime divisor.

Then there would be some $1 < d < n$ with $d \mid n$.

However, since $d < n$, d has a prime divisor, say $p \mid d$, which also divides n, a contradiction.

Therefore no such n exists.

$(b, \Rightarrow)$ If n is prime, it is not divisible by any primes less than

itself.

($\Leftarrow$) Suppose n is not divisible by any prime $p \leq \sqrt{n}$.

If there is a prime divisor of n between $\sqrt{n}$ and n, let q be the smallest one: $\sqrt{n} < q < n$.

Then $n < q^2$.

However, if r is another prime with $\sqrt{n} < r < n$, then $r \geq q$ so

$$n < q^2 \leq qr$$

This shows that n is not divisible by

any prime $< n$, a contradiction. $\square$

Exercise 2: Prove 101, 103, 107 and 109 are prime.

Theorem (Fundamental Theorem of Arithmetic)

Every $n \in \mathbb{N}$ can be written as a product of powers of primes,

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where $p_1, \ldots, p_r$ are distinct primes and $k_1, \ldots, k_r \in \mathbb{N}$. Moreover, this factorization is unique up to reordering the primes.

Ex $10 = 2 \cdot 5$, $12 = 2^2 \cdot 3$

Ex

$10 = 2 \cdot 5$

$12 = 2^2 \cdot 3$

$15 = 3 \cdot 5$

$26 = 2 \cdot 13$

$27 = 3^3$

$30 = 2 \cdot 3 \cdot 5$

$50 = 2 \cdot 5^2$

$100 = 2^2 \cdot 5^2$

$120 = 2^3 \cdot 3 \cdot 5$

$121 = 11^2$

$122 = 2 \cdot 61$

$1728 = 2^6 \cdot 3^3$

Pf of Existence: If n is prime, it's easy: $n = n^1$.

If n is composite, we prove FTA by induction, starting with the base case $n = 4 = 2^2$.

Now assume that for all $n \in \mathbb{N}$, n has a prime factorization.

Since N is composite, (a) of the Prop says $q \mid N$ for some prime $q < N$.

Write $N = qd$ for $d \in \mathbb{N}$. By the induction hypothesis,

$$d = p_1^{k_1} \cdots p_r^{k_r}$$

for some primes $p_1, \ldots, p_r$ and $k_i \in \mathbb{Z}$.

Then $N = q p_1^{k_1} \cdots p_r^{k_r}$ and if $q \neq p_i$ for any $1 \leq i \leq r$, we're done.

Otherwise, if $q = p_i$ then

$$N = p_1^{k_1} \cdots p_i^{k_i+1} \cdots p_r^{k_r}. \quad \square$$

To prove the uniqueness portion of the FTA we need:

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 $q_1, \dots, q_r$ 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:

$$p_1^{k_1} \cdots p_r^{k_r} \qquad q_1^{l_1} \cdots q_s^{l_s}$$

$n = p_1 \cdots p_r = q_1 \cdots q_s$.

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 $l_1 - k_1 \geq 0$ then q_1 divides the

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 3: 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?

Next time: more modular arithmetic.