

## Day 2

See DF Section 2.3.

### Euclid's Algorithm

1. Well-ordering of the integers. Every nonempty set of positive integers has a least element.
2. Let  $a$  and  $b$  be nonzero integers. Consider the set

$$X = \{ax + by : x, y \in \mathbb{Z}\}$$

1.  $X$  contains positive elements.
2.  $X$  contains a smallest positive element, call it  $d$ . So  $ax + by = d$ .
3. Note that  $X$  contains every (positive and negative) multiple of  $d$ .
4. Take any other positive element  $z$  of  $X$ . Then  $z = qd + r$  but also  $z = ax' + by'$ . Suppose  $r > 0$ . So  $qd + r = ax' + by'$  and therefore  $r = a(x' - qx) + b(y' - qy)$ . This means that  $r$  is in  $X$ ; but since  $r$  is less than  $d$ , this cannot happen. It follows that  $r = 0$  and every element of  $X$  is a multiple of  $d$ .
5. We conclude that  $X = d\mathbb{Z}$ .
6. Since  $X$  contains both  $a$  and  $b$ , we see that  $d$  is a common divisor of  $a$  and  $b$ .
7. If  $g$  is any other common divisor of  $a$  and  $b$ , then  $g$  divides  $d$  since  $d = ax + by$ .
8. Therefore  $d$  is the *greatest* common divisor of  $a$  and  $b$ , and any other common divisor of  $a$  and  $b$  is a divisor of  $d$ .
9.  $a$  and  $b$  are called *relatively prime* if their greatest common divisor is 1.

**Theorem:** Given nonzero integers  $x$  and  $y$ , the equation  $ax + by = z$  has a solution if and only if  $z$  is a multiple of the greatest common divisor of  $a$  and  $b$ .

**Corollary 1:** If  $a$  and  $n$  are relatively prime, and  $a \mid nb$ , then  $a \mid b$ .

**Proof:** Write  $ax + ny = 1$ . Multiply by  $b$  to get  $abx + nby = b$ . Since  $a$  divides both terms on the left, it divides  $b$ .

**Corollary 2:** Given integers  $a$  and  $b$  with greatest common divisor  $d$ , the integers  $a/d$  and  $b/d$  are relatively prime (i.e. have gcd equal to one).

**Proof:** Divide  $ax + by = d$  by  $d$ .

**Corollary 3:** The least common multiple of  $m$  and  $n$  is  $mn/d$  where  $d = \gcd(m, n)$ .

**Proof:** Suppose  $x$  is a common multiple of  $m$  and  $n$ . Write  $x = am$ . Then  $n \mid x$  so  $n \mid am$  and therefore  $\frac{n}{d} \mid a\frac{m}{d}$ . By Corollaries 1 and 2 this means  $\frac{n}{d}$  divides  $a$ , so  $mn/d$  divides  $x$ . Thus  $mn/d$  is the least common multiple and any common multiple is a multiple of  $mn/d$ .

## Congruences

**Theorem:** The congruence equation

$$ax \equiv b \pmod{n}$$

has solutions if and only if  $d = \gcd(a, n)$  divides  $b$ . In that case it has  $n/d$  solutions modulo  $n$ .

**Proof:** Solving the congruence equation

$$ax \equiv b \pmod{n}$$

is equivalent to solving the equation

$$ax + ny = b.$$

Euclid's algorithm tells us this equation has a solution if and only if  $d = \gcd(a, n)$  divides  $b$ . When this holds, we have a solution to our congruence  $x$  to our congruence. Notice that  $x + k\frac{n}{d}$  is *also* a solution to this equation for  $k = 0, \dots, d-1$ , so we actually have  $d$  solutions. If  $x$  and  $x'$  are any two solutions to this equation, then subtracting  $ax + ny = b$  from  $ax' + ny' = b$  yields

$$a(x - x') + n(y - y') = 0$$

and so, since  $n/d$  and  $a/d$  have gcd equal to one we conclude that  $x - x'$  is divisible by  $n/d$ . Therefore we have found all solutions.

## Cyclic Groups

### *Key Facts about Cyclic Groups*

1. Any cyclic group of infinite order is isomorphic to  $\mathbb{Z}$ . Any cyclic group of finite order  $n$  is isomorphic to  $\mathbb{Z}/n\mathbb{Z}$ . A group  $G$  is cyclic if and only if there is a surjective homomorphism from  $\mathbb{Z}$  to  $G$ .
2. An infinite cyclic group has two generators.
3. If  $g$  is a generator of a finite cyclic group  $G$  of order  $n$ , then  $g^a$  has order  $n/\gcd(n, a)$ . Thus  $g^a$  generates  $G$  if and only if  $\gcd(n, a) = 1$ .
4. Every subgroup of  $\mathbb{Z}/n\mathbb{Z}$  is cyclic, and there is a unique such subgroup for every  $d \mid n$ .
5. If  $H$  is the cyclic subgroup of  $\mathbb{Z}/n\mathbb{Z}$  of order  $d$  where  $d \mid n$ , then the elements of  $H$  are the multiples of  $n/d$ . The generators of  $H$  are the multiples  $kn/d$  where  $\gcd(k, d) = 1$ .

6. If  $\gcd(n, m) = 1$  then  $\mathbb{Z}/nm\mathbb{Z}$  is isomorphic to  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ .
7. If  $n$  and  $m$  are relatively prime, then a pair  $(a, b)$  generates  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  if and only if  $a$  and  $b$  generate  $\mathbb{Z}/n\mathbb{Z}$  and  $\mathbb{Z}/m\mathbb{Z}$  respectively. Therefore  $\phi(nm) = \phi(n)\phi(m)$  when  $n$  and  $m$  are relatively prime.
8. If  $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$  where the  $p_i$  are distinct primes then

$$\phi(n) = \prod_{i=1}^k (p^{e_i} - p^{e_i-1}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

***For discussion***

1. We know that  $\mathbb{Z}/6\mathbb{Z}$  is a subgroup of  $\mathbb{Z}/24\mathbb{Z}$ . Find all injective maps  $\mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/12\mathbb{Z}$ .
2. “Reduction mod 6” gives a surjective homomorphism  $\mathbb{Z}/24\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ . Find the inverse image of 5 under this map.
3. Find all surjective homomorphisms  $\mathbb{Z}/24\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$ .
4. Prove that  $(\mathbb{Z}/11\mathbb{Z})^\times$  is cyclic. In fact  $(\mathbb{Z}/p\mathbb{Z})^\times$  is always cyclic, we’ll prove this later.