1 Elementary number theory

The goal of this lecture is to prove Fermat's little theorem.

Theorem 1.1. *Let p be a prime, and let a be any integer. Then $a^p - a$ is divisible by p.*

1.1 Modular arithmetic [2.7, 2.9]

An *equivalence relation* on a set S is a relation $\sim$ between certain pairs of elements of S. We write $a \sim b$ if a and b are *equivalent*. An equivalence relation is required to be

- *transitive*: if $a \sim b$ and $b \sim c$, then $a \sim c$.
- *symmetric*: if $a \sim b$, then $b \sim a$.
- *reflexive*: for all a, $a \sim a$.

An equivalence relation $\sim$ partitions S into *equivalence classes*.

Definition 1.2. Let n be a positive integer. For integers a, b, we write

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

if $a - b$ is divisible by n, i.e., $a - b = nk$ for some integer k.

Lemma 1.3 (Addition and multiplication modulo n)**.** *If $a' \equiv a \pmod{n}$ and $b' \equiv b \pmod{n}$, then $a' + b' \equiv a + b \pmod{n}$ and $a'b' \equiv ab \pmod{n}$.*

Proof. Suppose $a' = a + nk$ and $b' = b + n\ell$. Then

$$a' + b' = (a + b) + n(k + \ell),$$

and

$$a'b' = ab + n(a\ell + bk + k\ell). \qquad \square$$

Definition 1.4. Let $\mathbb{Z}/n\mathbb{Z}$ denote the set of equivalence classes of $\mathbb{Z}$ with respect to the equivalence relation $\equiv$. These equivalence classes are also referred to as *congruence classes* modulo n.

By the lemma above, addition and multiplication of congruence classes modulo n is well-defined. If we write $\overline{a}$ to denote the congruence class of a, then

$$\overline{a} + \overline{b} = \overline{a + b},$$

and similarly

$$\overline{a}\overline{b} = \overline{ab}.$$

The associative, commutative, and distributive laws carry over for addition and multiplication of elements of $\mathbb{Z}/n\mathbb{Z}$.

Example 1.5. $\mathbb{Z}/6\mathbb{Z}$ has 6 elements. The elements $\overline{2}$ and $\overline{8}$ are the same element since $2 \equiv 8 \pmod{6}$.

We have $\overline{2} \cdot \overline{5} = \overline{10}$, and $\overline{8} \cdot \overline{5} = \overline{40}$. Fortunately, $\overline{10} = \overline{40}$ since $10 \equiv 40 \pmod{6}$. We usually take the remainder when divided by 6 and say $\overline{2} \cdot \overline{5} = \overline{4}$.

1.2 Bezout's lemma [2.3]

We recall division with remainder: let n be an integer, and let a be a positive integer. Then there exists an integer q and an integer $0 \leq r < a$ such that

$$n = aq + r.$$

Definition 1.6. Let a and b be integers, not both zero. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the largest integer which divides both a and b. If $\gcd(a, b) = 1$, we say that a and b are *coprime* or *relatively prime.*

The GCD satisfies the property that

$$\gcd(a, b) = \gcd(a + bk, b)$$

for any integer k. Indeed, if d divides both a and b, then d divides both $a + bk$ and b, and conversely.

As such, we can compute GCD's using the *Euclidean algorithm*, which works by repeated division with remainder.

Example 1.7. For example, for $a = 314$, $b = 136$, since

$$314 = 2 \cdot 136 + 42, \quad 136 = 3 \cdot 42 + 10, \quad 42 = 4 \cdot 10 + 2,$$

we have

$$\gcd(314, 136) = \gcd(42, 136) = \gcd(42, 10) = \gcd(2, 10) = 2.$$

Proposition 1.8 (Bezout's lemma)**.** *For any integers a and b, not both zero, there exist integers r and s such that*

$$\gcd(a, b) = ra + sb.$$

Proof. Let $d = \gcd(a, b)$ Let ℓ be the smallest positive integer that can be expressed as

$$\ell = ra + sb$$

for some r and s.

We claim that $\ell | a$. Use division with remainder to write

$$a = \ell q + m$$

for $0 \leq m < \ell$. Then m can also be expressed in the form $ra + sb$:

$$m = a - \ell q = a - q(ra + sb) = (1 - qr)a - (qs)b.$$

Since ℓ was assumed to be minimal, $m = 0$, so $\ell | a$.

Similarly, $\ell | b$, so ℓ divides both a and b. Since d is the greatest common divisor,

$$\ell \leq d.$$

On the other hand, d divides both ra and sb, so d also divides ℓ, so

$$d \leq \ell.$$

Thus, $\ell = d$. $\square$

Corollary 1.9. *Let e be an integer which divides both a and b. Then e divides $\gcd(a,b)$.*

Proof. Let

$$\gcd(a,b) = ra + sb.$$

Since e divides both terms on the right hand side, it also divides $\gcd(a,b)$. $\square$

Corollary 1.10. *Let p be a prime, and let a and b be integers. If $p|ab$, then $p|a$ or $p|b$.*

Proof. Suppose that p divides ab, but p does not divide a.

Since p is prime, $\gcd(a,p) = 1$, so by Bezout's lemma there exist $r, s \in \mathbb{Z}$ such that

$$1 = ra + sp.$$

Multiplying both sides by b,

$$b = rab + spb.$$

Both terms on the right are multiples of p by the assumption $p|ab$, so $p|b$. $\square$

Corollary 1.11 ($\mathbb{Z}/p\mathbb{Z}$ has inverses)**.** *Let p be a prime, and let a be an integer which is not divisible by p. There exists an integer b such that $ab \equiv 1 \pmod{p}$.*

Proof. As in the proof above, there exist $r, s \in \mathbb{Z}$ such that

$$1 = ra + sp.$$

So $ra \equiv 1 \pmod{p}$. Clearly, we can take $b = r$. $\square$

1.3 Proof of Fermat's little theorem

Proof. If a is divisible by p, then it is apparent that $a^p - a$ is divisible by p. Assume $p \nmid a$.

1. Consider the set
$$\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$
of nonzero congruence classes modulo p. Then consider the set
$$\{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$$
of congruence classes modulo p.

2. We claim that they're the same set. Indeed, since both sets have $p-1$ elements, we just need to show that $\overline{j}$ appears in the second set for every $j \in \{1, \ldots, p-1\}$.

   In other words, we want $ka \equiv j \pmod{p}$ for some $k \not\equiv 0 \pmod{p}$. Let b be such that $ab \equiv 1 \pmod{p}$, and let $k = jb$. Then
$$ka \equiv jba \equiv j \pmod{p}.$$
   Obviously $k \not\equiv 0 \pmod{p}$ since $j \not\equiv 0 \pmod{p}$.

3. Then

$$\begin{aligned} 1 \cdot 2 \cdots (p-1) &\equiv a \cdot (2a) \cdots (p-1)a \\ &\equiv 1 \cdot 2 \cdots (p-1) \cdot a^{p-1} \pmod{p}. \end{aligned}$$

   Multiplying both sides by an inverse of $(p-1)!$ gives

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

1.4 $(\mathbb{Z}/n\mathbb{Z})^\times$

Corollaries 1.10 and 1.11 are not true if p is not prime. For example, $4|2 \cdot 2$ but 4 does not divide 2, and there is no integer b such that $2b \equiv 1 \pmod{4}$, because $2b$ cannot be odd.

Here are some generalizations of them to general n.

Lemma 1.12. *Suppose n be a positive integer. If $n|ab$, then b is a multiple of $n/\gcd(a,n)$.*

Proof. Let $d = \gcd(a, n)$. Suppose

$$d = ra + sn.$$

Then $db = rab + snb$ is a multiple of n, so b is a multiple of n/d. □

Lemma 1.13. *Let n be a positive integer, and a be an integer such that $\gcd(a,n) = 1$. There exists an integer b such that $ab \equiv 1 \pmod{n}$.*

Proof. Since $\gcd(a, n) = 1$, there exist $r, s \in \mathbb{Z}$ such that

$$1 = ra + sn.$$

So $ra \equiv 1 \pmod{p}$, and we can take $b = r$. □

Definition 1.14. Let $(\mathbb{Z}/n\mathbb{Z})^\times$ denote the set of congruence classes $\overline{a}$ modulo n such that $\gcd(a, n) = 1$. Note that this does not depend on the choice of a, only on $a \pmod{n}$, since $\gcd(a + nk, n) = \gcd(a, n)$ as mentioned previously.

Definition 1.15. In the special case when $n = p$ is a prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ is just all of the elements of $\mathbb{Z}/p\mathbb{Z}$ other than $\overline{0}$.

1.5 Least common multiple

Definition 1.16. Let a and b be integers, both not zero. The *least common multiple* of a and b, denoted $\text{lcm}(a, b)$ is the smallest positive integer which is a multiple of both a and b.

Proposition 1.17. *Let a and b be positive integers. If $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$, then $ab = dm$.*

Proof. Suppose $m = ak$. Since $b|m$, by Lemma 1.12, $k \geq b/d$, so $m \geq ab/d$. On the other hand, it is clear that ab/d is a multiple of both a and b, so $m \leq ab/d$. $\square$