# Notes on Primitive Roots

*Dan Klain*

*last updated March 22, 2013*
*Comments and corrections are welcome*

These supplementary notes summarize the presentation on primitive roots given in class, which differed slightly from the approach in the textbook.

❧

Denote by $U_n$ the group of units mod $n$.

The *order* of a unit $u \in U_n$ is the smallest positive integer $k$ such that $u^k \equiv 1 \mod n$. This value is denoted $\text{ord}_n(u)$.

For example, if we compute the powers of 2 mod 7 we have

$$2^1 \equiv 2, \qquad 2^2 \equiv 4, \qquad 2^3 \equiv 1 \mod 7,$$

so that $\text{ord}_7(2) = 3$.

**Proposition 1.** *If $\alpha = \text{ord}_n(u)$, then $u^m \equiv 1 \mod n$ if and only if $\alpha | m$.*

*Proof.* If $\alpha | m$ then $m = \alpha k$ for some integer $k$, so that

$$u^m \equiv u^{\alpha k} \equiv (u^\alpha)^k \equiv 1^k \equiv 1 \mod n.$$

To prove the converse, suppose that $u^m \equiv 1$. Write $m = \alpha q + r$, where $0 \leq r < \alpha$. Since $u^\alpha \equiv 1$, we have

$$1 \equiv u^m \equiv u^{\alpha q + r} \equiv (u^\alpha)^q u^r \equiv u^r \mod n.$$

Since $r < \alpha$, this violates the minimality of the order $\alpha$, unless $r = 0$. ❑

By Euler's Theorem, $u^{\phi(n)} \equiv 1 \mod n$ for every $u \in U_n$. It follows from the previous proposition that

$$\text{ord}_n(u) | \phi(n)$$

for all $u \in U_n$.

In the discussion that follows we will often focus the order properties of units modulo a prime $p$. In this case we know that $\text{ord}_p(u) | (p-1)$ for all units $u \in U_p$.

❧

If we take the powers of 2 mod 5 we have

$$2^1 \equiv 2 \qquad 2^2 \equiv 4 \qquad 2^3 \equiv 3 \qquad 2^4 \equiv 1 \mod 5$$

exhausting the units mod 5, so that $\text{ord}_5(2) = 4$. In other words, 2 generates the entire multiplicative group $U_5$, which turns out to be a cyclic group. A similar computation reveals that 3 generates the group $U_7$; that is $\text{ord}_7(3) = 6 = \phi(7)$.

We say that $r$ is a *primitive root* mod $n$ if

$$U_n = \{1, r, r^2, \ldots, r^{\phi(n)-1}\}.$$

In other words, $r$ is a primitive root for $n$ iff $\text{ord}_n(r) = \phi(n)$. In this case, the group $U_n$ is *cyclic*, with $r$ as a *generator*.

*Exercise:* Show that there is *no* primitive root mod 8.

Some moduli have primitive roots, and some do not. We will show (eventually) that every prime modulus $p$ has at least one primitive root.

❧

It is not always easy to find a primitive root, when they exist at all. However, once we have found a primitive root $r$ mod $n$, it is easy to find the others.

**Proposition 2.** *If $u \in U_n$ has order $\alpha$, then $u^k$ is has order $\alpha$ if and only if* $\gcd(k, \alpha) = 1$.

*Proof.* Let $d = \gcd(k, \alpha)$, and let $\beta = \text{ord}_n(u^k)$. We need to show that $\beta = \alpha$ if and only if $d = 1$.

If $d > 1$ then $k = dx$ and $\alpha = dy$, where $x, y \in \mathbb{Z}$, and where $1 \leq y < \alpha$. In this case,

$$(u^k)^y \equiv u^{ky} \equiv u^{dxy} \equiv u^{\alpha x} \equiv (u^\alpha)^x \equiv 1^x \equiv 1 \mod p.$$

The minimality of the order $\beta$ now implies that $\beta \leq y < \alpha$.

Suppose instead that $d = 1$. Since $\beta = \text{ord}_n(u^k)$, we have

$$u^{k\beta} = (u^k)^\beta = 1.$$

It follows from Proposition 1 that $\alpha | k\beta$. Since $d = 1$, the values $\alpha$ and $k$ are co-prime, so that $\alpha | \beta$.

Meanwhile,

$$(u^k)^\alpha \equiv (u^\alpha)^k \equiv 1^k \equiv 1 \mod p,$$

so that $\beta | \alpha$, again by Proposition 1. It now follows that $\beta = \alpha$. ❑

**Corollary 1.** *If $\mathbb{Z}_n$ has a primitive root $r$, then the primitive roots for $\mathbb{Z}_n$ are precisely those units $r^k$ where* $\gcd(k, \phi(n)) = 1$. *In particular, there are $\phi(\phi(n))$ primitive roots mod $n$.*

*Proof.* If $r$ is a primitive root mod $n$, then $\text{ord}_n(r) = \phi(n)$. The previous proposition then implies that $\text{ord}_n(r^k) = \phi(n)$ iff $k$ is relatively prime to $\phi(n)$, giving $\phi(\phi(n))$ distinct cases. Since every $u \in U_n$ has the form $r^k$ for some $k$ (because $r$ is primitive), this exhausts all possibilities for primitive roots mod $n$. ❑

Assuming that there is at least one primitive root modulo a prime $p$ (to be shown below), it follows there are exactly $\phi(p-1) = \phi(\phi(p))$ primitive roots for $p$.

❧

The following lemma is useful for generating elements of higher order, given elements of smaller order.

**Lemma 1** (Multiplicative Lemma)**.** *Suppose that* $\text{ord}_n(\alpha) = a$ *and* $\text{ord}_n(\beta) = b$*. If* $\gcd(a, b) = 1$*, then* $\text{ord}_n(\alpha\beta) = ab$*.*

*Proof.* Let $c = \text{ord}_n(\alpha\beta)$. Evidently

$$(\alpha\beta)^{ab} = \alpha^{ab}\beta^{ab} = (\alpha^a)^b(\beta^b)^a = 1^b 1^a = 1,$$

so that $c|ab$, by Proposition 1. Meanwhile,

$$1 = 1^a = ((\alpha\beta)^c)^a = (\alpha\beta)^{ac} = \alpha^{ac}\beta^{ac} = \beta^{ac},$$

so that $b|ac$, again by Proposition 1. Since $\gcd(a, b) = 1$, it follows that $b|c$. By a similar and symmetrical argument, we also have $a|c$. Again, since $\gcd(a, b) = 1$, we have $ab|c$. It now follows that $c = ab$. ❑

This lemma can be useful for finding primitive roots. For example, it is easy to see that 2 has order 5 mod 31, since $2^5 \equiv 32 \equiv 1 \bmod 31$. And we always know that $-1$ has order 2 modulo an odd prime. If we can find and element $c$ of order 3, the Multiplicative Lemma implies that $-2c$ will have order 30, so it is primitive. Looking at a list of cubes:

$$1, 8, 27, 64, 125, 216, 343, ...$$

we see that $5^3 = 125 \equiv 1 \bmod 31$, so that $-10 \equiv 21$ is a primitive root. The complete list of primitive roots mod 31 will be congruent to some $21^k$ for $k$ relatively prime to 30, that is, the values:

$$21, 21^7, 21^{11}, 21^{13}, 21^{17}, 21^{19}, 21^{23}, 21^{29} \mod 31$$

or (listed in the same order):

$$21,\ 11,\ 12,\ 22,\ 24,\ 13,\ 17,\ 3 \mod 31$$

❧

We now present a series of lemmas leading to a proof that, if $p$ is prime, then $\mathbb{Z}_p$ has a primitive root.

It is a consequence of Fermat's Theorem that the polynomial

$$x^{p-1} - 1$$

has at least $p-1$ roots mod $p$. By Lagrange's Theorem this polynomial has at most $p-1$ roots, so it therefore has *exactly* the $p-1$ roots $1, 2, \ldots, p-1$.

A similar argument yields the following.

**Lemma 2.** *If $x^{p-1} - 1 = g(x)h(x)$, where $\deg(g) = k$ and $\deg(h) = l$, then $g(x)$ has exactly $k$ roots, and $h(x)$ has exactly $l$ roots mod $p$.*

*Proof.* Note that $k + l = p - 1$, since degrees (leading exponents) are added when polynomials are multiplied.

If $r$ is a root of $x^{p-1} - 1$, then $g(r)h(r) \equiv 0 \mod p$, so that either $g(r) \equiv 0$ or $h(r) \equiv 0 \mod p$. If $g$ has fewer than $k$ roots, then there are more than $l = p - 1 - k$ distinct roots of $x^{p-1} - 1$ remaining, all of which must then be roots of $h$. But $h$ cannot have more than $l$ roots. Therefore $g$ must have exactly $k$ roots, and similarly $h$ must have exactly $p - 1 - k = l$ roots. ❑

The following algebraic identity is a variant of the geometric sum formula.

**Lemma 3.** *If $n = kl$, then*

$$x^n - 1 \;=\; (x^k)^l - 1 \;=\; (x^k - 1)(x^{k(l-1)} + x^{k(l-2)} + \cdots + x^k + 1).$$

*Proof.* Begin with the geometric sum identity:

$$u^l - 1 \;=\; (u - 1)(u^{l-1} + u^{l-2} + \cdots + u + 1).$$

The lemma follows after substituting $u = x^k$. ❑

We are now ready to prove the main theorem.

**Theorem 1.** *If $p$ is prime, then $\mathbb{Z}_p$ has a primitive root.*

*Proof.* Suppose $p - 1$ has the prime power factorization

$$p - 1 = q_1^{a_1} \cdots q_k^{a_k},$$

where $q_1 < \cdots < q_k$.

By Lemma 3, we have

$$x^{p-1} - 1 \;=\; (x^{q_1^{a_1}} - 1)h(x),$$

where $h(x)$ is a polynomial. By Lemma 2 the factor $x^{q_1^{a_1}} - 1$ has exactly $q_1^{a_1}$ roots mod $p$.

If $s$ is a root of $x^{q_1^{a_1}} - 1$, then $s^{q_1^{a_1}} \equiv 1 \mod p$. It follows from Proposition 1 that $\mathrm{ord}_p(s) | q_1^{a_1}$. Therefore, $\mathrm{ord}_p(s) = q_1^{b_1}$, for some $0 \leq b_1 \leq a_1$.

If every root of $x^{q_1^{a_1}} - 1$ has order strictly less than $q_1^{a_1}$, then every root of $x^{q_1^{a_1}} - 1$ is also a root of of $x^{q_1^{a_1-1}} - 1$. In other words, this polynomial of degree $q_1^{a_1-1}$ would have $q_1^{a_1}$ roots, which is impossible. It follows that at least one of the roots

of $x^{q_1^{a_1}} - 1$ has order $q_1^{a_1}$. In other words, there exists an element $r_1 \in U_p$ having order $q_1^{a_1}$.

Repeating this argument for each $q_i$, we find, for each $i$, an element $r_i \in U_p$ of order $q_i^{a_i}$.

By the Multiplicative Lemma, the unit $r = r_1 \cdots r_k$ has order $q_1^{a_1} \cdots q_k^{a_k} = p - 1$, so that $r$ is a primitive root mod $p$. ❑

❧

*Exercise:*

> Suppose that $\phi(p) = p - 1 = q_1^{a_1} \cdots q_s^{a_s}$, where $q_1 < \cdots < q_s$ are prime, and each $a_i > 0$. Prove that $r$ is a primitive root mod $p$ iff
>
> $$r^{\frac{p-1}{q_i}} \not\equiv 1 \mod p$$
>
> for every $q_i$.

This result in this exercise speeds the process of checking whether a value $r$ is primitive. For example, if $p = 31$ then $p - 1 = 30 = 2 \cdot 3 \cdot 5$. To determine if 3 is primitive mod 31 we need only check that

$$3^6 \not\equiv 1, \quad 3^{10} \not\equiv 1, \quad 3^{15} \not\equiv 1, \qquad \mod 31.$$

First, use repeated squaring to determine that

$$3^2 \equiv 9, \quad 3^4 \equiv -12, \quad 3^8 \equiv 20, \quad 3^{16} \equiv -3 \mod 31.$$

It is then easy to compute

$$3^6 \equiv 16, \quad 3^{10} \equiv 25, \quad 3^{15} \equiv -1 \mod 31$$

so that 3 must be primitive mod 31.

❧

We have shown that if $p$ is prime then $\mathbb{Z}_p$ has a primitive root.

More generally, it can be shown that primitive roots exist for $\mathbb{Z}_n$ if and only if $n = 1, 2, 4, p^e$ or $2p^e$, where $p$ is an odd prime, and $e$ is a positive integer.

Moreover, it is a consequence of Euler's theorem and the Chinese Remainder Theorem that $\mathbb{Z}_n$ has no primitive roots if $n$ is divisible by two distinct odd primes.

Since $\mathbb{Z}_8$ has no primitive roots (by inspection), it follows from an induction argument (with respect to the exponent $e$) that $\mathbb{Z}_{2^e}$ has no primitive roots for $e \geq 3$.

To prove that $\mathbb{Z}_{p^2}$ has a primitive root, find a primitive root $r$ for $\mathbb{Z}_p$. One can show that either $r$ or $r + p$ is primitive for $\mathbb{Z}_{p^2}$.

To prove that $\mathbb{Z}_{p^e}$ has a primitive root for $e > 2$, find a primitive root $r$ for $\mathbb{Z}_{p^2}$. One can show that $r$ is also primitive for $\mathbb{Z}_{p^e}$, using induction on $e$.

To prove that $\mathbb{Z}_{2p^e}$ has a primitive root for $e > 2$, find a primitive root $r$ for $\mathbb{Z}_{p^e}$. Either $r$ or $r + p^e$ is odd. The odd choice is also primitive for $\mathbb{Z}_{2p^e}$.

Details are given in the textbook (Jones & Jones).

❧ ❧ ❧ ❧