Primitive Roots Modulo Prime Powers

Ryan C. Daileda

Trinity University

Number Theory

Recall

Given $n \in \mathbb{N}$, a *primitive root modulo* n is an integer a so that

$$(\mathbb{Z}/n\mathbb{Z})^\times = \langle a + n\mathbb{Z} \rangle.$$

Equivalently, for any $b \in \mathbb{Z}$ with $(b, n) = 1$, there exists a $k \in \mathbb{N}$ so that $a^k \equiv b \pmod{n}$.

Last time we used a counting argument to prove that primitive roots modulo primes exist.

Theorem 1

Let $p \in \mathbb{N}$ be prime. Then there are exactly $\varphi(p-1)$ (incongruent modulo p) primitive roots modulo p.

Order Lifting

Today we will treat the case of primitive roots modulo p^n, where p is an *odd* prime.

(Remember that there are *no* primitive roots modulo 2^n for $n \geq 3$).

We will produce primitive roots modulo p^n by "lifting" primitive roots modulo p.

Recall that if $m|n$, then there is a well-defined map

$$\begin{aligned} r : (\mathbb{Z}/n\mathbb{Z})^\times &\to (\mathbb{Z}/m\mathbb{Z})^\times \\ a + n\mathbb{Z} &\mapsto a + m\mathbb{Z}. \end{aligned}$$

Lemma 1

If $m|n$ and $(a, n) = 1$, then the order of $a + m\mathbb{Z}$ divides the order of $a + n\mathbb{Z}$.

Proof. Let d denote the order of $a + n\mathbb{Z}$. Then $a^d \equiv 1 \pmod{n}$.

Since $m|n$, this implies $a^d \equiv 1 \pmod{m}$. Thus, $(a + m\mathbb{Z})^d = 1 + m\mathbb{Z}$.

This implies that the order of $a + m\mathbb{Z}$ divides d. ∎

Corollary 1

Let p be a prime. If a is a primitive root modulo p,then $a + p^2\mathbb{Z}$ has order $p - 1$ or $p(p - 1)$.

Proof. Let d be the order of $a + p^2\mathbb{Z}$. Since

$$\left|(\mathbb{Z}/p^2\mathbb{Z})^\times\right| = \varphi(p^2) = p(p-1),$$

we have $d|p(p - 1)$.

Since $a + p\mathbb{Z}$ has order $p - 1$, by Lemma 1 $p - 1|d$.

Primitive Roots Modulo p^2

So we have $p-1|d|p(p-1)$, which implies $\frac{d}{p-1}$ divides p.

Since p is prime, this means $\frac{d}{p-1}$ is either 1 or p.

That is, $d = p-1$ or $d = p(p-1)$. □

Theorem 2

Let p be an odd prime. If $a \in \mathbb{Z}$ is a primitive root modulo p, then either a or $a+p$ is a primitive root modulo p^2.

Proof. By Corollary 1, $a + p^2\mathbb{Z}$ has either order $p-1$ or $p(p-1)$.

In the second case we are finished.

So we may assume that $a + p^2\mathbb{Z}$ has order $p - 1$.

That is, $a^{p-1} \equiv 1 \pmod{p^2}$.

Since $a \equiv a + p \pmod{p}$, $(a + p) + p\mathbb{Z}$ also has order $p - 1$.

So $(a + p) + p^2\mathbb{Z}$ has order $p - 1$ or $p(p - 1)$, by Corollary 1.

Thus, if we can show that $(a + p)^{p-1} \not\equiv 1 \pmod{p^2}$, we will be finished.

By the Binomial Theorem and our assumption on a we have

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

If this is $\equiv 1 \pmod{p^2}$, then $a^{p-2}p \equiv 0 \pmod{p^2}$ iff $a^{p-2} \equiv 0 \pmod{p}$ iff $a \equiv 0 \pmod{p}$ (by Euclid's lemma), which contradicts the fact that $(a, p) = 1$.

Thus $(a+p)^{p-1} \not\equiv 1 \pmod{p^2}$, and the result is proven. □

Theorem 2 gives us an explicit algorithm for constructing primitive roots modulo p^2 from primitive roots modulo p.

Examples

2 is a primitive root modulo 3, which means that 2 or $2 + 3 = 5$ is a primitive root modulo $3^2 = 9$.

Since $2^{3-1} = 4 \not\equiv 1 \pmod{9}$, it must be that 2 is a primitive root modulo 9.

The smallest "exception" occurs when $p = 29$. In this case 14 is a primitive root modulo 29.

But $14^{28} \equiv 1 \pmod{29^2}$, so that 14 is *not* a primitive root modulo 29^2.

Instead, $14 + 29 = 43$ is a primitive root modulo 29^2.

Primitive Roots Modulo p^n

For $n \geq 3$, we have the following result concerning primitive roots modulo p^n.

Theorem 3

Let p be an odd prime and $n \geq 3$. If $a \in \mathbb{Z}$ is a primitive root modulo p^{n-1}, then a is a primitive root modulo p^n.

Proof. Let d be the multiplicative order of $a + p^n\mathbb{Z}$. Then $d|\varphi(p^n) = p^{n-1}(p-1)$.

By Lemma 1, the order of $a + p^{n-1}\mathbb{Z}$ divides d as well. Thus

$$\varphi(p^{n-1}) = p^{n-2}(p-1)|d|p^{n-1}(p-1) \;\Rightarrow\; \left.\frac{d}{p^{n-2}(p-1)}\right| p.$$

Since p is prime, this implies that $\frac{d}{p^{n-2}(p-1)} \in \{1, p\}$ or

$$d = p^{n-2}(p-1) \text{ or } p^{n-1}(p-1).$$

It therefore suffices to show that $a^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$.

Now Euler's Theorem implies

$$a^{p^{n-3}(p-1)} \equiv 1 \pmod{p^{n-2}} \;\Rightarrow\; a^{p^{n-3}(p-1)} = 1 + kp^{n-2}.$$

However, since a is a primitive root modulo p^{n-1}, $a^{p^{n-3}(p-1)} \not\equiv 1 \pmod{p^{n-1}}$.

It follows that $p \nmid k$.

By the Binomial Theorem we therefore have

$$\begin{aligned} a^{p^{n-2}(p-1)} &= \left(a^{p^{n-3}(p-1)}\right)^p = (1+kp^{n-2})^p \\ &= 1 + \binom{p}{1}kp^{n-2} + \binom{p}{2}k^2p^{2(n-2)} + \cdots \\ &\qquad \cdots + \binom{p}{p-1}k^{p-1}p^{(p-1)(n-2)} + k^p p^{p(n-2)} \\ &\equiv 1 + kp^{n-1} \not\equiv 1 \pmod{p^n} \end{aligned}$$

since $\binom{p}{m} \equiv 0 \pmod{p}$ for $1 \le m \le p-1$, $p, n \ge 3$ and $p \nmid k$.

This is what we needed to show. □

Corollary 2

Let p an odd prime and let $a \in \mathbb{Z}$ be a primitive root modulo p. Then either a or $a + p$ is a primitive modulo p^n for all $n \geq 2$.

Proof. By Theorem 2, either a or $a + p$ is a primitive root modulo p^2. The result follows from Theorem 3 and a quick induction. □

Examples.

- Since 2 is a primitive root modulo 3 and 9, it is a primitive root modulo 3^n for all $n \geq 1$.
- Since 14 is a primitive root modulo 29 and $14 + 29 = 43$ is a primitive root modulo 29^2, 43 is a primitive root modulo 29^n for all $n \geq 2$.

Primitive Roots Modulo Composite Integers in General

We are almost ready completely classify the natural numbers n for which there exist primitive roots.

Lemma 2

Let $m, n \in \mathbb{N}$. Suppose that $(m, n) = 1$ and $m, n \geq 3$. Then there is no primitive root modulo mn.

Proof. Suppose that $(a, mn) = 1$. Then $(a, m) = (a, n) = 1$.

Since $\varphi(m)$ and $\varphi(n)$ are both even, Euler's Theorem implies

$$a^{\frac{\varphi(m)\varphi(n)}{2}} = \left(a^{\varphi(m)}\right)^{\frac{\varphi(n)}{2}} \equiv 1^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{m},$$
$$a^{\frac{\varphi(m)\varphi(n)}{2}} = \left(a^{\varphi(n)}\right)^{\frac{\varphi(m)}{2}} \equiv 1^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{n}.$$

Thus $a^{\frac{\varphi(m)\varphi(n)}{2}} \equiv 1 \pmod{mn}$, by the CRT.

So the order of a modulo mn cannot exceed $\frac{\varphi(m)\varphi(n)}{2}$.

But $\frac{\varphi(m)\varphi(n)}{2} = \frac{\varphi(mn)}{2} < \varphi(mn)$.

So a cannot be a primitive root modulo mn. □

We can now eliminate "most" composite numbers from consideration.

Corollary 3

Let $n \in \mathbb{N}$. Then n fails to have a primitive root if either:

1. *n is divisible by two odd primes.*
2. *$n = 2^k p^\ell$, where $k \geq 2$ and p is an odd prime.*

Proof (Sketch). In both cases we can write $n = ab$ with $(a, b) = 1$ and $a, b \geq 3$. □

We now find that the only candidates for moduli for which primitive roots exist are 2, 4, p^k and $2p^k$, where p is an odd prime.

We've seen that primitive roots do, indeed, exist in the first three cases.

It remains to address integers of the form $2p^k$, where p is an odd prime.

Lemma 3

Let p be an odd prime. For any $k \in \mathbb{N}$, there is a primitive root modulo $2p^k$.

Proof. Let a be a primitive root modulo p^k.

Since $a \equiv a + p^k \pmod{p^k}$, $a + p^k$ is also a primitive root modulo p^k.

Since either a or $a + p^k$ is even, we can assume WLOG that a is odd.

Since $(a, p^k) = 1$ by assumption, it follows that $(a, 2p^k) = 1$.

We will show that a is a primitive root modulo $2p^k$.

Let $r = |a + 2p^k\mathbb{Z}|$. By Lemma 1, $\varphi(p^k) = |a + p^k\mathbb{Z}|$ must divide r.

But then we have $\varphi(p^k)|r|\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$.

Hence $r = \varphi(p^k) = \varphi(2p^k)$, and we're finished. $\square$

We have achieved our complete classification!

Theorem 4

Let $n \in \mathbb{N}$. There is a primitive root modulo n if and only if

$$n = 2, 4, p^k, \text{ or } 2p^k,$$

where p is an odd prime.

Remark. Euler, Lagarange, Legendre and Gauss all had a hand in originally proving Theorem 4.

Legendre gave the first complete proof of the existence of primitive roots modulo primes in 1785, and Gauss first proved Theorem 4 in 1801.

Example

Let's find a primitive root modulo $338 = 2 \cdot 13^2$.

Since $\varphi(13) = 12$ and

$$2^2 = 4, 2^3 = 8, 2^4 \equiv 3 \pmod{13}, 2^6 \equiv -1 \pmod{13}$$

2 must be a primitive root modulo 13. And since

$$2^{12} \equiv 40 \not\equiv 1 \pmod{169},$$

2 must also be a primitive root modulo 169.

Since 2 is even, the proof of Lemma 3 tells us that $2 + 169 = 171$ must be a primitive root modulo 338 (or modulo $2 \cdot 13^k$).