6 Primitive Roots and the Discrete Logarithm

For further reading on the material in this subsection, consult **Rosen 9.1**.

In section 3.2 we studied the problem of extending division to modular arithmetic. We noted that trying to find b/a is equivalent to solving the equation $ax = b$, and so we worked on the congruence $ax \equiv b \mod m$.

In this section we will be applying a similar analysis to the logarithm. The real number logarithm $\log_a(b)$ is the solution to the equation $a^x = b$; we wish to study the congruence equation $a^x \equiv b \mod m$.

6.1 The order of an integer

We're going to start with the very simplest case: computing the logarithm of 1. In particular we want to consider the equation $a^x \equiv 1 \mod n$ and see if it has any solutions at all, and if so, how many.

It is of course true that $x = 0$ solves this congruence. But we can find more solutions! Recall that Euler's theorem tells us that if n is a natural number and $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$. Thus $x = \phi(n)$ is also a solution to this congruence. That means there is at least one *positive* solution, and so (by the well-ordering principle) we can ask for the *least* positive solution.

Definition 6.1. Let a, n be relatively prime integers with $a \neq 0$ and n positive. Then the least positive integer x such that $a^x \equiv 1 \mod n$ is called the *order of a modulo n*, written $\operatorname{ord}_n a$.

Example 6.2. Let's compute the orders of 2 and 3 modulo 7. We see

$$2^1 \equiv 2 \mod 7 \qquad 3^1 \equiv 3 \mod 7$$
$$2^2 \equiv 4 \mod 7 \qquad 3^2 \equiv 9 \equiv 2 \mod 7$$
$$2^3 \equiv 1 \mod 7 \qquad 3^3 \equiv 27 \equiv 6 \mod 7$$
$$3^4 \equiv 81 \equiv 4 \mod 7$$
$$3^5 \equiv 4 \cdot 3 \equiv 12 \equiv 5 \mod 7$$
$$3^6 \equiv 5 \cdot 3 \equiv 15 \equiv 1 \mod 7.$$

Thus $\operatorname{ord}_7 2 = 3$ and $\operatorname{ord}_7 3 = 6$.

Lemma 6.3. *If a, n are relatively prime integers with $a \neq 0$ and $n > 0$, then a positive integer x is a solution to the congruence $a^x \equiv 1 \mod n$ if and ony if $\operatorname{ord}_n a | x$.*

Proof. First suppose $\operatorname{ord}_n a | x$. Then we can write $x = m \cdot \operatorname{ord}_n a$ for some integer m, and we have

$$a^x \equiv a^{m \cdot \operatorname{ord}_n a} \equiv \left(a^{\operatorname{ord}_n a}\right)^m \equiv 1^m \equiv 1 \mod n.$$

Conversely, suppose $a^x \equiv 1 \mod n$, we can use the division algorithm divide x by $\operatorname{ord}_n a$ and write

$$x = q \cdot \operatorname{ord}_n a + r, \qquad 0 \rightrightarrows r < \operatorname{ord}_n a.$$

Then we compute

$$1 \equiv a^x \equiv a^{q \cdot \operatorname{ord}_n a + r} \equiv a^{q \cdot \operatorname{ord}_n a} \cdot a^r \equiv a^r \mod n$$

so we have $a^r \equiv 1 \mod n$ but $0 \leq r < \operatorname{ord}_n a$. But $\operatorname{ord}_n a$ is by definition the least positive integer with this property, so r cannot be positive and must be 0. Thus $x = q \cdot \operatorname{ord}_n a$ as desired. □

Remark 6.4. This should remind you of the proof that since (a, b) is the least linear combination of a and b, we know that m is a linear combination of a and b if and only if $(a, b) | m$.

Example 6.5. Let's see if 10, 20, or 30 are solutions to $3^x \equiv 1 \mod 7$. We saw that $\operatorname{ord}_7 3 = 6$, so $3^{30} \equiv 1 \mod 7$ since $6|30$. But $3^{20} \not\equiv 1 \mod 7$ and $3^{10} \not\equiv 1 \mod 7$ since $6 \not| 10, 20$.

Corollary 6.6. *If* $(a, n) = 1$ *with* $n > 0$*, then* $\operatorname{ord}_n a | \phi(n)$.

Proof. Since $(a, n) = 1$ we know that $a^{\phi(n)} \equiv 1 \mod n$, thus $\operatorname{ord}_n a | \phi(n)$. □

We can use this to make it easier to compute orders: we only need to check numbers that divide $\phi(n)$.

Example 6.7. Let's find the order of 7 modulo 9. We can compute that $\phi(9) = 3(3-1) = 6$, so we just need to check 1, 2, 3, 6. We see

$$7^1 \equiv 7 \not\equiv 1 \mod 9$$
$$7^2 \equiv 49 \equiv 4 \not\equiv 1 \mod 9$$
$$7^3 \equiv 4 \cdot 7 \equiv 28 \equiv 1 \mod 9$$

We don't need to check 6.

Example 6.8. Let's find $\operatorname{ord}_{11} 3$. We know that $\phi(11) = 10$ so we just need to check $1, 2, 5, 10$. We have

$$\begin{aligned} 3^1 &\equiv 3 \not\equiv 1 \mod 11 \\ 3^2 &\equiv 9 \not\equiv 1 \mod 11 \\ 3^5 &\equiv 243 = 11(22) + 1 \equiv 1 \mod 11 \end{aligned}$$

so $\operatorname{ord}_{11} 3 = 5$. This saves us from checking 3 or 4 since we know they can't be the answer.

Remark 6.9. Note that sometimes $\operatorname{ord}_n a = \phi(n)$. For instance, you can check that $\operatorname{ord}_{11} 2 = 10$.

Lemma 6.10. *If $(a, n) = 1$, then $a^i \equiv a^j \mod n$ if and only if $i \equiv j \mod \operatorname{ord}_n a$.*

Proof. First, let's suppose $i \equiv j \mod \operatorname{ord}_n a$, and assume that $i \geq j$. Then there is some k such that $i = j + k \cdot \operatorname{ord}_n a$, and we have

$$\begin{aligned} a^i &\equiv a^{j + k \cdot \operatorname{ord}_n a} \equiv a^j \cdot a^{k \cdot \operatorname{ord}_n a} \\ &\equiv a^j \cdot (a^{\operatorname{ord}_n a})^k \equiv a^j \cdot 1^k \equiv a^j \mod n. \end{aligned}$$

Conversely, suppose $a^i \equiv a^j \mod n$, and again without loss of generality assume $i \geq j$. Then we have

$$\begin{aligned} a^i &\equiv a^j \mod n \\ a^j \cdot a^{i-j} &\equiv a^j \mod n \\ a^{i-j} &\equiv 1 \mod n \end{aligned}$$

since $(a, n) = 1$ and thus $(a^j, n) = 1$ so we can use the cancellation lemma. But if $a^{i-j} \equiv 1 \mod n$ then by lemma 6.3 we know that $\operatorname{ord}_n a | i - j$, and so by defnition $i \equiv j \mod \operatorname{ord}_n a$. □

6.2 Primitive Roots

For further reading on the material in this subsection, consult **Rosen 9.1**.

We've shown that the order of any integer modulo n will divide $\phi(n)$. In this subsection we're interested in elements whose order is exactly $\phi(n)$.

Definition 6.11. If $(a, n) = 1$, and $\operatorname{ord}_n a = \phi(n)$, we say that a is a *primitive root* modulo n, and we say that n has a primitive root.

Example 6.12. We showed that $\operatorname{ord}_7 3 = 6 = \phi(7)$ so 3 is a primitive root modulo 7. However, $\operatorname{ord}_7 2 = 3 \neq \phi(7)$, so 2 is not a primitive root modulo 7.

Example 6.13. The number 8 does not have a primitive root. The integers relatively prime to 8 are 1,3,5,7. We can compute $\operatorname{ord}_8 1 = 1$ and $\operatorname{ord}_8 3 = \operatorname{ord}_8 5 = \operatorname{ord}_8 7 = 2$, but $\phi(8) = 4$.

Every prime number has a primitive root; we will prove this in subsection 6.3. Not every composite number has a primitive root, but some, like 6 and 10, do.

Theorem 6.14. *If $(r, n) = 1$ and $n > 0$, and r is a primitive root modulo n, then the set $\{r^1, r^2, \ldots, r^{\phi(n)}\}$ is a reduced residue system modulo n.*

Proof. This set clearly has the correct size, so we need to prove that these numbers are all relatively prime to n and that no two are congruent modulo n.

Because $(r, n) = 1$ we know that $(r^k, n) = 1$ for any natural number k. This satisfies the first requirement.

Suppose $r^i \equiv r^j \mod n$. Then by lemma 6.10 we know that $i \equiv j \mod \operatorname{ord}_n r$. But r is a primitive root, which means that $\operatorname{ord}_n r = \phi(n)$. Thus $\phi(n) | i - j$ but $1 \leq i, j \leq \phi(n)$ and thus $i = j$. □

Example 6.15. We showed that $\operatorname{ord}_7 3 = 6$ so 3 is a primitive root modulo 7. Thus the set

$$\{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3, 9, 27, 81, 243, 729\}$$

is a reduced residue system modulo 7.

We can check that $\operatorname{ord}_9 2 = 6 = \phi(9)$. Thus the set

$$\{2, 2^2, 2^3, 2^4, 2^5, 2^6\} = \{2, 4, 8, 16, 32, 64\}$$

is a reduced residue system modulo 9.

We already noted that not every integer has a primitive root. But if an integer has a primitive root it usually has several more. We will spend the rest of this subsection making that statement more precise.

Lemma 6.16. *Let n be a natural number, and $(a, n) = 1$, and set $\operatorname{ord}_n a = t$. Then for any $u \in \mathbb{N}$ we have*

$$\operatorname{ord}_n a^u = \frac{t}{(u, t)}.$$

Proof. First set $t_1 = t/(u,t)$ and $u_1 = u/(u,t)$, and set $s = \operatorname{ord}_n a^u$. We know that $(t_1, u_1) = 1$. Now we want to show that $s = t_1$.

First we want to show that $(a^u)^{t_1} \equiv 1 \mod n$. But

$$(a^u)^{t_1} = a^{ut_1} = a^{ut/(u,t)} = (a^t)^{u_1} \equiv 1^{u_1} \equiv 1 \mod n.$$

Thus we know that $s = \operatorname{ord}_n a^u | t_1$ by lemma 6.3.

Conversely, we know that $(a^u)^s \equiv 1 \mod n$, and thus $a^{us} \equiv 1 \mod n$, which implies that $t|us$, again by lemma 6.3. Dividing on both sides by (u,t) gives $t_1|u_1 s$, but $(t_1, u_1) = 1$, so by Euclid's lemma this gives us $t_1|s$.

Since $t_1|s$ and $s|t_1$, we know that $s = t_1$, which gives us $\operatorname{ord}_n(a^u) = \frac{\operatorname{ord}_n a}{(\operatorname{ord}_n a, u)}$, or $s = t/(u,t)$, as desired. □

Corollary 6.17. *Let r be a primitive root modulo n. Then r^u is a primitive root modulo n if and only if $(u, \phi(n)) = 1$.*

Proof. We know that

$$\operatorname{ord}_n r^u = \frac{\operatorname{ord}_n r}{(u, \operatorname{ord}_n r)} = \frac{\phi(n)}{(u, \phi(n))}.$$

Thus r^u is a primitive root if and only if $\operatorname{ord}_n r^u = \phi(n)$ if and only if $(u, \phi(n)) = 1$. □

So if a number n has a primitive root, how many does it have? It must have one for every exponent that's relatively prime to $\phi(n)$.

Corollary 6.18. *If a positive integer n has a primitive root, it has exactly $\phi(\phi(n))$ primitive roots.*

Proof. Let r be a primitive root modulo n. Then r^u is a primitive root if and only if $(u, \phi(n)) = 1$; there are $\phi(\phi(n))$ numbers relatively prime to $\phi(n)$.

(Every primitive root must have the form r^u for some u, since these are all the numbers relatively prime to n). □

Example 6.19. We claimed earlier that $\operatorname{ord}_{11} 2 = 10$, and thus 2 is a primitive root modulo 11. This tells us that 11 has $\phi(\phi(11)) = \phi(10) = 4$ incongruent primitive roots. In particular, these roots are $2, 2^3 = 8, 2^7 = 128 \equiv 7, 2^9 = 512 \equiv 6$. Thus $\{2, 6, 7, 8\}$ is a complete set of incongruent primitive roots modulo 11.

This result does have one weakness: it tells us what happens if there are *any* primitive roots modulo n, but doesn't tell us which integers n have any primitive roots at all.

6.3 Primitive Roots for Primes

In this section we'd like to prove that every prime number has a primitive root. The basic idea is that for a fixed prime p, there are a lot of numbers relatively prime to p. In fact, there are so many that we run out of "room" for non-primitive roots, so some of them have to be primitive roots.

In order to do this, we have to return to looking at polynomial congruences.

Definition 6.20. Let $f(x)$ be a polynomial with integer coefficients. We say c is a *root of f modulo m* if $f(c) \equiv 0 \mod m$. (This is the same idea as a root in the integers, except we're thinking about everything as belonging to the integers modulo m).

Example 6.21. The polynomial $f(x) = x^2 + 1$ has no roots in the integers, but it has two roots modulo 5: $f(2) = 5 \equiv 0 \mod 5$, and $f(3) = 10 \equiv 0 \mod 5$.

Example 6.22. Let $f(x) = x^{p-1} - 1$ for a fixed prime p. Then by Fermat's little theorem, f has $p-1$ incongruent roots modulo p: $1, 2, 3, \ldots, p-1$.

It's a famous result in the real numbers that a polynomial of degree n has at most n distinct roots. A similar result holds modulo p.

Theorem 6.23 (Lagrange's Theorem)**.** *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, and $p \not| a_n$. Then $f(x)$ has at most n incongruent roots modulo p.*

Proof. We prove this by induction. (Yay!) When $n = 1$, we have $f(x) = a_1 x + a_0$ with $p \not| a_1$. By our results on linear congruences, we know that $a_1 x \equiv -a_0 \mod p$ has exactly one solution modulo p, since $(a_1, p) = 1$. Thus f has exactly one root, and thus at most one root.

Suppose the theorem is true for $n-1$, that is, *any* polynomial of degree $n-1$ has at most $n-1$ incongruent solutions. Now let $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Suppose $f(x)$ has $n+1$ incongruent solutions modulo p, which we can call $c_0, c_1, \ldots, c_n$. Then $f(c_i) \equiv 0 \mod p$ for $0 \leq i \leq n$. Then

$$f(x) - f(c_0) = a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0).$$

We see that we can factor $(x - c_0)$ out of each term, so we can write

$$f(x) - f(c_0) = (x - c_0)g(x)$$

for some polynomial $g(x)$ with degree $\leq n - 1$.

We claim that $g(c_i) \equiv 0 \mod p$ for any $1 \leq i \leq n$. For we have

$$(c_i - c_0)g(c_i) = f(c_i) - f(c_0) \equiv 0 - 0 \equiv 0 \mod p.$$

Thus since p is prime, either $p|g(c_i)$ or $p|(c_i - c_0)$. But by hypothesis we know that $c_i \neq c_0 \mod p$ so $p \not| c_i - c_0$, and thus we have $p|g(c_i)$ and $g(c_i) \equiv 0 \mod p$. Thus c_i is a root of g modulo p for $1 \leq i \leq n$.

Thus g is a polynomial of degree $\leq n-1$ with n incongruent solutions, which contradicts the inductive hypothesis. □

Remark 6.24. This theorem does *not* hold for composite moduli. For instance, if we take $g(x) = x^2 - 3x + 2$, then modulo 6 we see that $g(1) = 0 \equiv 0 \mod 6$, and $g(2) = 0 \equiv 0 \mod 6$, and $g(4) = 6 \equiv 0 \mod 6$.

We want to use Lagrange's Theorem to put limits on how many elements can have a given order modulo p.

Proposition 6.25. *Let p be a prime and let d be a divisor of $p-1$. Then the polynomial $f(x) = x^d - 1$ has exactly d incongruent roots modulo p.*

Proof. We know that $d|p-1$, so by the difference of nth powers formula we have $(x^d - 1)|x^{p-1} - 1$. In particular

$$x^{p-1} - 1 = (x^d - 1)(1 + x^d + x^{2d} + \cdots + x^{p-1-d}).$$

Set $g(x) = 1 + x^d + \cdots + x^{p-1-d}$; this is a polynomial of degree $p - 1 - d$.

By Fermat's Little Theorem, we know that $x^{p-1} - 1$ has exactly $p-1$ incongruent roots. We can see that every root of $x^{p-1} - 1$ that is not a root of g must be a root of $x^d - 1$ (since if $p|x^{p-1} - 1$ then either $p|g(x)$ or $p|x^d - 1$).

But by Lagrange's theorem we know that g has at most $p - 1 - d$ incongruent roots, so $x^d - 1$ must have at least $p - 1 - (p - 1 - d) = d$ incongruent roots. But again we know that $x^d - 1$ has at most d incongruent roots, so it has exactly d incongruent roots. □

Lemma 6.26. *Let p be a prime and let $d|p-1$. Then there are fewer than $\phi(d)$ positive integers less than p that have order d modulo p.*

Proof. Let $F(d)$ be the number of positive integers of order d modulo p that are less than p. We wish to prove that $F(d) \leq \phi(d)$.

If there are no roots of order d modulo p then it's clear that $F(d) = 0 \leq \phi(d)$. So suppose there is an integer a of order d modulo p. Then the integers $a, a^2, \ldots, a^d$ are all incongruent modulo p.

Further, we see that for any $k \in \mathbb{N}$, we compute that $(a^k)^d = (a^d)^k \equiv 1^k \equiv 1 \mod p$, so a^k is a root of $x^d - 1$ modulo p for any k. Thus we have d incongruent roots of $x^d - 1$ on this list. Since we know $x^d - 1$ has exactly d incongruent roots modulo p, we know that the set of roots is exactly the set $a, a^2, \dots, a^d$.

By lemma 6.16, we see that $\operatorname{ord}_p a^k = \frac{\operatorname{ord}_p a}{(k, \operatorname{ord}_p a)} = \frac{d}{(k,d)}$, and thus a^k has order d if and only if $(k, d) = 1$. There are exactly $\phi(d)$ such integers k with $1 \leq k \leq d$, and thus if there is one element of order d modulo p, there are exactly $\phi(d)$ positive integers less than p of order d modulo p. Thus $F(d) \leq \phi(d)$. □

Remark 6.27. This theorem proves that for a given $d|p-1$, either there are $\phi(d)$ elements of order d or there are 0. But we didn't state it that way because we are about to leverage it into an even better result.

Theorem 6.28. *Let p be a prime, and let d be a positive divisor of $p-1$. Then the number of incongruent ingeters of order d modulo p is exactly $\phi(d)$.*

Proof. This is essentially a counting argument. For any $d|p-1$, let $F(d)$ be the number of positive integers of order d modulo p that are less than p. Because every integer from 1 to $p-1$ has an order dividing $p-1$, we see that

$$p - 1 = \sum_{d|p-1} F(d).$$

But we also know that

$$p - 1 = \sum_{d|p-1} \phi(d),$$

so

$$\sum_{d|p-1} F(d) = \sum_{d|p-1} \phi(d).$$

From lemma 6.26 we know that $F(d) \leq \phi(d)$, but their sums are equal; the only way this is possible is if $F(d) = \phi(d)$ for each $d|p-1$. Thus there are exactly $\phi(d)$ incongruent integers of order d modulo p. □

Corollary 6.29. *Every prime has a primitive root.*

Proof. Let p be a prime. Then there are exactly $\phi(p-1)$ incongruent integers of order $p-1$ modulo p by theorem 6.28. But these are all primitive roots by definition. Since $\phi(p-1) \geq 1$, this completes the proof. □

This proves that every prime has a primitive root, but doesn't give us a way to find them. In fact locating primitive roots is not trivial; on the other hand, 2 appears to be a primitive root quite often. But we don't know whether it is a primitive root infinitely often.

Conjecture 6.30 (Artin)**.** *Any integer a such that $a \neq \pm 1$ and a is not a perfect square is a primitive root of infinitely many primes.*

Proposition 6.31 (Hooley 1967)**.** *The Generalized Riemann Hypothesis implies Artin's conjecture.*

Proposition 6.32 (Heath-Brown 1985)**.** *There are at most three positive square-free integers a such that a is a primitive root of only finitely many primes. Thus at least one of 2, 3, 5 is a primitive root for infinitely many primes.*

6.4 Primitive Roots for Composites

We now understand exactly when a prime number has a primitive root (always), and how many it has ($\phi(p-1)$). What about composite numbers?

We start with the simplest kind of composite numbers: the prime powers.

Lemma 6.33. *Let p be an odd prime, with primitieve root r. Then either r or $r+p$ is a primitive root modulo p^2.*

Remark 6.34. This means that there is some integer that is a primitive root modulo p and also modulo p^2, since $p+r$ is a primitive root modulo p.

Proof. We know that $\operatorname{ord}_p r = \phi(p) = p-1$. Let $n = \operatorname{ord}_{p^2} r$. By definition $r^n \equiv 1 \mod p^2$, and thus $r^n \equiv 1 \mod p$. This implies that $p-1 = \operatorname{ord}_p r | n$.

But we know that $\operatorname{ord}_{p^2} r | \phi(p^2) = p(p-1)$, so we have $p-1 | n | p(p-1)$. Thus either $n = p-1$ or $n = p(p-1)$. If $n = p(p-1)$ then r is a primitive root modulo p^2; so suppose $n = p-1$.

Let $s = r+p$. Then since s is also a primitive root modulo p, by the same logic we know that $\operatorname{ord}_{p^2} s$ is either $p-1$ or $p(p-1)$. We wish to show that $\operatorname{ord}_{p^2} s \neq p-1$.

By the binomial theorem, we compute

$$\begin{aligned} s^{p-1} = (r+p)^{p-1} &= \sum_{i=0}^{p-1} \binom{p-1}{i} p^i r^{p-1-i} \\ &= r^{p-1} + (p-1)pr^{p-2} + \cdots + (p-1)p^{p-2}r + p^{p-1} \\ &\equiv r^{p-1} + (p-1)pr^{p-2} \mod p^2 \\ &\equiv 1 + (p-1)pr^{p-2} \mod p^2. \end{aligned}$$

But since $p \not| r$ we see that $(p-1)pr^{p-2} \not\equiv 0 \mod p^2$ so $s^{p-1} \not\equiv 1 \mod p^2$ as desired.

Thus $\text{ord}_{p^2} s \neq p-1$, and the only remaining possibility is that $\text{ord}_{p^2} s = p(p-1) = \phi(p^2)$. □

Example 6.35. We have seen that 2 is a primitive root modulo 11. But $2^{10} = 1024 \equiv 56 \mod 121$ so $\text{ord}_{121} 2 \neq 10$. Thus we must have $\text{ord}_{121} 2 = 110 = \phi(121)$ so 2 is a primitive root modulo 121.

We hve seen that 3 is a primitive root modulo 7. But $3^6 = 729 \equiv 43 \not\equiv 1 \mod 49$. Thus $\text{ord}_{49} 3 \neq 6$ so $\text{ord}_{49} 3 = 42 = \phi(49)$ and 3 is a primitive root modulo 49.

Example 6.36. Let $p = 487$ be prime, and we compute that $\text{ord}_{487} 10 = 486$. (We do not do this by hand). But $10^{486} \equiv 1 \mod 487^2$ so 10 is not a primitive root modulo 487^2. Thus we know that $497 = 10 + 487$ is a primitive root modulo 487^2.

Lemma 6.37. *Let p be an odd prime. Then p^k has a primitive root for any $k \in \mathbb{N}$. Moreover, if r is a primitive root modulo p^2, then r is a primitive root modulo p^k for any $k \in \mathbb{N}$.*

Proof. By lemma 6.33 we know that p has a primitive root r that is also a primitive root modulo p^2, and thus $r^{p-1} \not\equiv 1 \mod p^2$.

First we will prove by induction that $r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k$ for any $k \geq 2$. The base case when $k = 2$ follows from Lemma 6.33. Suppose the assertion is true for k, and we will prove it for $k+1$.

By inductive hypothesis, we know that

$$r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k.$$

But also $(r, p) = 1$ since r is a primitive root, and thus $(r, p^{k-1}) = 1$. Thus $\phi(p^{k-1}) = p^{k-2}(p-1)$ and thus

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \mod p^{k-1}.$$

Thus we can find some integer such that

$$r^{p^{k-2}(p-1)} = 1 + dp^{k-1}$$

where $p \not| d$ since otherwise the congruence would hold moduldo p^k. We can raise both sides

of this to the pth power, which gives

$$\begin{aligned} r^{p^{k-2}(p-1)(p)} &= \sum_{i=0}^{p} \binom{p}{i} (dp)^{(k-1)i} \\ r^{p^{k-1}(p-1)} &= 1 + dp^k + p^{k+1} \text{ (stuff)} \\ r^{p^{k-1}(p-1)} &\equiv 1 + dp^k \mod p^{k+1} \\ &\not\equiv 1 \mod p^{k+1} \end{aligned}$$

since $p \not| d$. Thus by induction, for any $k \geq 2$ we have

$$r^{p^{k-1}(p-1)} \not\equiv 1 \mod p^{k+1}.$$

Now we wish to show that r is a primtiive root modulo p^k. Let $n = \text{ord}_{p^k} r$. We know that $n|\phi(p^k) = p^{k-1}(p-1)$. Further, we know that $\text{ord}_p r = p-1$ so we must have $p-1|n$. So $n = p^t(p-1)$ for some $0 \leq t \leq k-1$.

But we know that

$$r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k,$$

so we must have $t < k-2$. Thus $t = k-1$ and so $\text{ord}_r = p^{k-1}(p-1) = \phi(p^k)$, and r is a primitive root modulo p^k. □

Example 6.38. We saw that 2 is a primitive root modulo 11 and also modulo 121. Thus 2 is a primitive root modulo 11^k for any $k \in \mathbb{N}$.

Now we turn our attention to powers of even primes.

Lemma 6.39. *If a is an odd integer and k is an integer with $k \geq 3$, then*

$$a^{\phi(2^k)/2} = a^{2^{k-2}} \equiv 1 \mod 2^k.$$

Thus there are no primitive roots modulo 2^k for $k \geq 3$.

Proof. We prove this by induction, again.

Our base case is $k = 3$, which you checked for homework: we saw that $\phi(2^3) = \phi(8) = 4$, but $a^2 \equiv 1 \mod 8$ for any odd a.

Now suppose $a^{2^{k-2}} \equiv 2^k$. Then there is an integer d with $a^{2^{k-2}} = 1 + d2^k$. Squaring both sides gives

$$\begin{aligned} a^{2^{k-2} \cdot 2} &= (1 + d2^k)^2 \\ a^{2^{k-1}} &= 1 + 2^{k+1}d + d^2 2^{2k} \\ a^{2^{k-1}} &\equiv 1 \mod 2^{k+1} \end{aligned}$$

as desried.

□

This shows that there is never a primitive root modulo 2^k if $k \geq 3$. However, there is always an "almost primitive root"–a number whose order is as big as possible without being a primitive root. In fact, 5 is always such a number. The proof is very similar to the last two proofs we did.

Exercise 6.40. *Let $k \geq 3$ be an integer. Then*

$$\operatorname{ord}_{2^k} 5 = \phi(2^k)/2 = 2^{k-2}.$$

6.4.1 Primitive roots modulo not prime powers

We now have a pretty thorough understanding of when a prime power has a primitive root. What about other composite numbers? *Mostly* they don't have primitive roots.

Lemma 6.41. *If n is a positive integer that is not a prime power or twice a prime power, then n does not have a primitive root.*

Proof. Let $n = p_1^{t_1} \dots p_m^{t_m}$, and suppose r is a primitive root modulo n. Then $(r, n) = 1$ and $\operatorname{ord}_n r = \phi(n)$.

We know that $(r, p^t) = 1$ for any p in the prime factorization of n, and for any $t \in \mathbb{N}$. Thus $r^{p^{t-1}(p-1)} = r^{\phi(p^t)} \equiv 1 \mod p^t$.

Let U be the least common multiple of $\phi(p_i^{t_i})$ i.e.

$$U = \operatorname{lcm}\left(\phi(p_1^{t_1}), \dots, \phi(p_m^{t_m})\right).$$

Then since $\phi(p_i^{t_i}) | U$ we know that $r^U \equiv 1 \mod p_i^{t_i}$ for every i. Thus, by the Chinese Remainder Theorem, $r^U \equiv 1 \mod n$.

Then we must have $\phi(n) = \operatorname{ord}_n r \leq U$. But since ϕ is multiplicative, this must imply that

$$\phi(p_1^{t_i}) \dots \phi(p_m^{t_m}) \leq U = \operatorname{lcm}\left(\phi(p_1^{t_1}), \dots, \phi(p_m^{t_m})\right).$$

But the product of a set of integers is always at least their least common multiple, with equality only when all the numbers are relatively prime. So we must have the $\phi(p_i^{t_i})$ all pairwise relatively prime.

But recall that $\phi(\ell)$ is even unless ℓ is 1 or 2. Thus in order for the $\phi(p_i^{t_i})$ to all be pairwise relatively prime, there can be at most one $p_i^{t_i}$ that is not equal to 2. Thus either $n = p_1^{t_i}$ and is a prime power, or $n = 2p_1^{t_1}$ and is two times a prime power, as desired. □

This lemma limits which numbers can have primitive roots. We've shown that many of the possibilities do in fact have primitive roots: we know that prime powers have primitive roots as long as the prime is not 2. But we haven't checked this case of "twice a prime power," so we do that now.

Lemma 6.42. *If p is an odd prime and t is a positive integer, then $2p^t$ has a primitive root.*

In particular, if r is an odd primitive root modulo p^t then it is also a primitive root modulo $2p^t$. If r is an even primitive root modulo p^t then $r + p^t$ is a primitive root modulo $2p^t$.

Proof. If r is a primitive root modulo p^t, then $\operatorname{ord}_{p^t} r = \phi(p^t) = p^{t-1}(p-1)$. We observe that $\phi(2p^t) = \phi(2)\phi(p^t) = \phi(p^t)$, so $\operatorname{ord}_{p^t} r = \phi(2p^t)$ as well.

If r is odd, then $r \equiv 1 \mod 2$ so $r^{\phi(2p^t)} \equiv 1 \mod 2$. Since $r^{\phi(2p^t)} \equiv 1 \mod p^t$, by the Chinese Remainder Theorem we have $r^{\phi(2p^t)} \equiv 1 \mod 2p^t$. But if $r^n \equiv 1 \mod 2p^t$ then $r^n \equiv 1 \mod p^t$, and we know $\operatorname{ord}_{p^t} r = \phi(2p^t)$ so $n \geq 2p^t$. Thus $\operatorname{ord}_{2p^t} r = \phi(2p^t)$ and thus r is a primitive root modulo $2p^t$.

If r is even, then $r + p^t$ is odd and a primitive root modulo p^t, and by the same argument we see that $r + p^t$ is a primitive root modulo $2p^t$. □

Example 6.43. We showed that 2 is a primitive root modulo 11^k for any $k \in \mathbb{N}$. Since 2 is even, we know that $2 + 11^k$ is a primitive root modulo $2 \cdot 11^k$ for any $k \in \mathbb{N}$.

Combining everything we have shown, we can state the following theorem:

Theorem 6.44. *Let n be a positive integer greater than 1. Then n possesses a primitive root if and only if $n = 2, 4, p^t$, or $2p^t$ for some odd prime p and natural number t.*

6.5 Discrete Logarithms

For further reading on the material in this subsection, consult **Rosen 9.4, Shoup 11.1-11.2**.

Recall from theorem 6.14 that if r is a primitive root modulo m, then $\{r^k : 1 \leq k \leq \phi(m)\}$ is a reduced residue system modulo m. Thus the equation $r^x \equiv a \mod m$ has a solution whenever $(a, m) = 1$, and this solution is unique modulo $\phi(m)$.

Definition 6.45. Let m be a natural number with primitive root r, and let a be a positive integer with $(a, m) = 1$. the unique integer x with $1 \leq x \leq \phi(m)$ and $r^x \equiv a \mod m$ is called the *index* or *discrete logarithm* of a to the base r modulo m, and is denoted $\operatorname{ind}_r a$ or $\log_r a$.

Clearly $r^{\operatorname{ind}_r a} \equiv a \mod m$. Further, by lemma 6.10 we see that $a \equiv b \mod m$ if and only if $\operatorname{ind}_r a \equiv \operatorname{ind}_r b \mod \phi(m)$, indeed if and only if $\operatorname{ind}_r a = \operatorname{ind}_r b$ since the index is always between 1 and $\phi(m)$.

Example 6.46. Earlier we worked out the table

$$3^1 \equiv 3 \mod 7 \qquad 3^2 \equiv 9 \equiv 2 \mod 7$$
$$3^3 \equiv 27 \equiv 6 \mod 7 \qquad 3^4 \equiv 81 \equiv 4 \mod 7$$
$$3^5 \equiv 4 \cdot 3 \equiv 12 \equiv 5 \mod 7 \qquad 3^6 \equiv 5 \cdot 3 \equiv 15 \equiv 1 \mod 7.$$

Thus modulo 7 we have

$$\operatorname{ind}_3 1 = 6 \qquad \operatorname{ind}_3 2 = 2 \qquad \operatorname{ind}_3 3 = 1$$
$$\operatorname{ind}_3 4 = 4 \qquad \operatorname{ind}_3 5 = 5 \qquad \operatorname{ind}_3 6 = 3.$$

If we use a different base we get different indices. For instance, we see that 5 is a primitive root modulo 7, and we have

$$\operatorname{ind}_5 1 = 6 \qquad \operatorname{ind}_5 2 = 4 \qquad \operatorname{ind}_5 3 = 5$$
$$\operatorname{ind}_5 4 = 2 \qquad \operatorname{ind}_5 5 = 1 \qquad \operatorname{ind}_5 6 = 3.$$

We can prove that the "index" operation has most of the properties of logarithms.

Exercise 6.47. *Let m be a natural number with primitive root r, and let a, b be relatively prime to m. Then*

1. $\operatorname{ind}_r 1 \equiv 0 \mod \phi(m)$
2. $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \mod \phi(m)$
3. $\operatorname{ind}_r a^k \equiv k \operatorname{ind}_r a \mod \phi(m)$.

Example 6.48. We know that modulo 7, we have $\operatorname{ind}_5 2 = 4$ and $\operatorname{ind}_5 3 = 5$. We compute that $\operatorname{ind}_5(2 \cdot 3) = \operatorname{ind}_5 2 + \operatorname{ind}_3 = 4 + 5$, and modulo $\phi(7) = 6$ this is indeed equivalent to $\operatorname{ind}_5 6 = 3$.

Example 6.49. We can use this to solve exponential congruences. Suppose we wish to find all solutions of $6x^{12} \equiv 11 \mod 17$. We can compute that 3 is a primitive root modulo 17, and can compute (or look up) a table of indices of integers modulo 17.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Then we have

$$\begin{aligned}
\operatorname{ind}_3(6x^{12}) &\equiv \operatorname{ind}_3(11) \mod \phi(17) \\
\operatorname{ind}_3 6 + \operatorname{ind}_3 x^{12} &\equiv \operatorname{ind}_3 11 \mod 16 \\
\operatorname{ind}_3 6 + 12 \operatorname{ind}_3 x &\equiv \operatorname{ind}_3 11 \mod 16 \\
15 + 12 \operatorname{ind}_3 x &\equiv 7 \mod 16 \\
12 \operatorname{ind}_3 x &\equiv 8 \mod 16 \\
3 \operatorname{ind}_3 x &\equiv 2 \mod 4 \\
\operatorname{ind}_3 x &\equiv 2 \cdot 3 \equiv 2 \mod 4.
\end{aligned}$$

Thus we have $\operatorname{ind}_3 x \in \{2, 6, 10, 14\}$ and thus

$$x \equiv 3^2, 3^6, 3^{10}, 3^{14} \equiv 9, 15, 8, 2 \mod 17.$$

Example 6.50. Find all solutions of $7^x \equiv 6 \mod 17$.

We have

$$\begin{aligned} \operatorname{ind}_3(7^x) &\equiv \operatorname{ind}_3 6 \mod 16 \\ x \cdot \operatorname{ind}_3 7 &\equiv 15 \mod 16 \\ 11x &\equiv 15 \mod 16 \\ x &\equiv 11^{-1} \cdot 15 \equiv 3 \cdot 15 \equiv 13 \mod 16. \end{aligned}$$

Thus $7^x \equiv 6 \mod 17$ if and only if $x \equiv 13 \mod 16$.

Remark 6.51. You might notice that we did a lot of work with the cavalier statement "we can compute a table of indices." In fact, computing indexes or discrete logarithms is quite computationally intensive, and there isn't much of a better way of computing $\operatorname{ind}_3 12$ than just raising 3 to a bunch of powers and seeing which one gives you 12. (Thus if you're computing indices at all you might as well build a table).

The fact that this problem is computationally difficult underlies the security of much cryptography currently in use; it is comparable to the problem of factoring large integers.

Like integer factorization, the discrete logarithm problem can be solved quickly on a quantum computer. We don't currently have useful quantum computers, but researchers are worried that they will be practical in the near-to-medium future, and we are starting to move to "lattice-based" encryption methods that do not depend on the discrete logarithm problem.