Introduction to number theory-9

May 29, 2017

Theorem 3.3 *Let G be a finite subgroup of the multiplicative group of a field. Then G is cyclic.*

Proof. Let $|G| = m$. By Theorem 2.15, if $a \in G$, then the order of a is a divisor of m. For every divisor d of m, let $\psi(d)$ denote the number of elements of G of order d. If $\psi(d) \neq 0$, then there exists an element a of order d, and every element of the cyclic subgroup $\langle a \rangle$ generated by a satisfies $a^d = 1$. By Theorem 3.2, the polynomial $f(x) = x^d - 1 \in F[x]$ has at most d zeros, and so every zero of $f(x)$ belongs to the cyclic subgroup $\langle a \rangle$. In particular, every element of G of order d must belong to $\langle a \rangle$. By Theorem 2.18, a cyclic group of order d has exactly $\varphi(d)$ generators, where $\varphi(d)$ is the Euler phi function. Therefore, $\psi(d) = 0$ or $\psi(d) = \varphi(d)$ for every divisor d of m. Since every element of G has order d for some divisor d of m, it follows that

$$\sum_{d|m} \psi(d) = m.$$

By Theorem 2.8,

$$\sum_{d|m} \varphi(d) = m,$$

and so $\psi(d) = \varphi(d)$ for every divisor d of m. In particular, $\psi(m) = \varphi(m) \geq 1$, and so G is a cyclic group of order m. □

Theorem 3.4 *For every prime p, the multiplicative group of the finite field $\mathbf{Z}/p\mathbf{Z}$ is cyclic. This group has $\varphi(p-1)$ generators. Equivalently, for every prime p, there exist $\varphi(p-1)$ pairwise incongruent primitive roots modulo p.*

Proof. This follows immediately from Theorem 3.3, since $|(\mathbf{Z}/p\mathbf{Z})^\times| = p-1$. □

The following table lists the primitive roots for the first six primes.

p	$\varphi(p-1)$	primitive roots
2	1	1
3	1	2
5	2	2, 3
7	2	3, 5
11	4	2, 6, 7, 8
13	4	2, 6, 7, 11

Let p be a prime, and let g be a primitive root modulo p. If a is an integer not divisible by p, then there exists a unique integer k such that

$$a \equiv g^k \pmod{p}$$

and

$$k \in \{0, 1, \ldots, p-2\}.$$

This integer k is called the *index* of a with respect to the primitive root g, and is denoted by

$$k = \mathrm{ind}_g(a).$$

If k_1 and k_2 are any integers such that $k_1 \leq k_2$ and

$$a \equiv g^{k_1} \equiv g^{k_2} \pmod{p},$$

then

$$g^{k_2-k_1} \equiv 1 \pmod{p},$$

and so

$$k_1 \equiv k_2 \pmod{p-1}.$$

If $a \equiv g^k \pmod{p}$ and $b \equiv g^\ell \pmod{p}$, then $ab \equiv g^k g^\ell = g^{k+\ell} \pmod{p}$, and so

$$\mathrm{ind}_g(ab) \equiv k + \ell \equiv \mathrm{ind}_g(a) + \mathrm{ind}_g(b) \pmod{p-1}.$$

The index map ind_g is also called the *discrete logarithm* to the base g modulo p.

If $a \equiv g^k \pmod{p}$ and $b \equiv g^\ell \pmod{p}$, then $ab \equiv g^k g^\ell = g^{k+\ell} \pmod{p}$, and so

$$\mathrm{ind}_g(ab) \equiv k + \ell \equiv \mathrm{ind}_g(a) + \mathrm{ind}_g(b) \pmod{p-1}.$$

The index map ind_g is also called the *discrete logarithm* to the base g modulo p.

For example, 2 is a primitive root modulo 13. Here is a table of $\mathrm{ind}_2(a)$ for $a = 1, \ldots, 12$:

a	$\mathrm{ind}_2(a)$	a	$\mathrm{ind}_2(a)$
1	0	7	11
2	1	8	3
3	4	9	8
4	2	10	10
5	9	11	7
6	5	12	6

By Theorem 2.18, if g is a primitive root modulo p, then g^k is a primitive root if and only if $(k, p-1) = 1$. For example, for $p = 13$ there are $\varphi(12) = 4$ integers k such that $0 \leq k \leq 11$ and $(k, 12) = 1$, namely, $k = 1, 5, 7, 11$, and so the four pairwise incongruent primitive roots modulo 13 are

$$\begin{aligned}
2^1 &\equiv 2 \pmod{13}, \\
2^5 &\equiv 6 \pmod{13}, \\
2^7 &\equiv 11 \pmod{13}, \\
2^{11} &\equiv 7 \pmod{13}.
\end{aligned}$$

Primitive Roots to Composite Moduli

In the previous section we proved that primitive roots exist for every prime number. We also observed that primitive roots do not exist for every modulus. For example, congruence (3.1) shows that there is no primitive root modulo 8. The goal of this section is to prove that an integer $m \geq 2$ has a primitive root if and only if $m = 2, 4, p^k$, or $2p^k$, where p is an odd prime and k is a positive integer.

Theorem 3.5 *Let m be a positive integer that is not a power of 2. If m has a primitive root, then $m = p^k$ or $2p^k$, where p is an odd prime and k is a positive integer.*

Proof. Let a and m be integers such that $(a, m) = 1$ and $m \geq 3$. Suppose that

$$m = m_1 m_2, \qquad \text{where } (m_1, m_2) = 1 \text{ and } m_1 \geq 3,\ m_2 \geq 3. \tag{3.2}$$

Then $(a, m_1) = (a, m_2) = 1$. The Euler phi function $\varphi(m)$ is even for $m \geq 3$ (Exercise 4 in Section 2.2). Let

$$n = \frac{\varphi(m)}{2} = \frac{\varphi(m_1)\varphi(m_2)}{2}.$$

By Euler's theorem,

$$a^{\varphi(m_1)} \equiv 1 \pmod{m_1},$$

and so

$$a^n = \left(a^{\varphi(m_1)}\right)^{\varphi(m_2)/2} \equiv 1 \pmod{m_1}.$$

Similarly,

$$a^n = \left(a^{\varphi(m_2)}\right)^{\varphi(m_1)/2} \equiv 1 \pmod{m_2}.$$

Since $(m_1, m_2) = 1$ and $m = m_1 m_2$, we have

$$a^n \equiv 1 \pmod{m},$$

and so the order of a modulo m is strictly smaller than $\varphi(m)$. Consequently, if we can factor m in the form (3.2), then there does not exist a primitive root modulo m. In particular, if m is divisible by two distinct odd primes, then m does not have a primitive root. Similarly, if $m = 2^\ell p^k$, where $\ell \geq 2$, then m does not have a primitive root. Therefore, the only moduli $m \neq 2^\ell$ for which primitive roots can exist are of the form $m = p^k$ or $m = 2p^k$ for some odd prime p. □

To prove the converse of Theorem 3.5, we use the following result about the exponential increase in the order of an integer modulo prime powers.

Theorem 3.6 *Let p be an odd prime, and let $a \neq \pm 1$ be an integer not divisible by p. Let d be the order of a modulo p. Let k_0 be the largest integer such that $a^d \equiv 1 \pmod{p^{k_0}}$. Then the order of a modulo p^k is d for $k = 1, \ldots, k_0$ and dp^{k-k_0} for $k \geq k_0$.*

Proof. There exists an integer u_0 such that

$$a^d = 1 + p^{k_0} u_0 \qquad \text{and} \qquad (u_0, p) = 1. \tag{3.3}$$

Let $1 \le k \le k_0$, and let e be the order of a modulo p^k. If $a^e \equiv 1 \pmod{p^k}$, then $a^e \equiv 1 \pmod{p}$, and so d divides e. By (3.3), we have $a^d \equiv 1 \pmod{p^k}$, and so e divides d. It follows that $e = d$.

Let $j \geq 0$. We shall show that there exists an integer u_j such that

$$a^{dp^j} = 1 + p^{j+k_0} u_j \qquad \text{and} \qquad (u_j, p) = 1. \tag{3.4}$$

The proof is by induction on j. The assertion is true for $j = 0$ by (3.3). Suppose we have (3.4) for some integer $j \geq 0$. By the binomial theorem, there exists an integer v_j such that

$$\begin{aligned} a^{dp^{j+1}} &= \left(1 + p^{j+k_0} u_j\right)^p \\ &= 1 + p^{j+1+k_0} u_j + \sum_{i=2}^{p} \binom{p}{i} p^{i(j+k_0)} u_j^i \\ &= 1 + p^{j+1+k_0} u_j + p^{j+2+k_0} v_j \\ &= 1 + p^{j+1+k_0} (u_j + p v_j) \\ &= 1 + p^{j+1+k_0} u_{j+1}, \end{aligned}$$

and the integer $u_{j+1} = u_j + p v_j$ is relatively prime to p. Thus, (3.4) holds for all $j \geq 0$.

Let $k \geq k_0 + 1$ and $j = k - k_0 \geq 1$. Suppose that the order of a modulo p^{k-1} is dp^{j-1}. Let e_k denote the order of a modulo p^k. The congruence

$$a^{e_k} \equiv 1 \pmod{p^k}$$

implies that

$$a^{e_k} \equiv 1 \pmod{p^{k-1}},$$

and so dp^{j-1} divides e_k. Since

$$a^{dp^{j-1}} = 1 + p^{k-1}u_{j-1} \not\equiv 1 \pmod{p^k},$$

it follows that dp^{j-1} is a proper divisor of e_k. On the other hand,

$$a^{dp^j} = 1 + p^k u_j \equiv 1 \pmod{p^k},$$

and so e_k divides dp^j. It follows that the order of a modulo p^k is exactly $e_k = dp^j = dp^{k-k_0}$. This completes the proof. □

Theorem 3.7 *Let p be an odd prime. If g is a primitive root modulo p, then either g or $g+p$ is a primitive root modulo p^k for all $k \geq 2$. If g is a primitive root modulo p^k and $g_1 \in \{g, g+p^k\}$ is odd, then g_1 is a primitive root modulo $2p^k$.*

Theorem 3.6, if $k_0 = 1$, then the order of g modulo p^k is $(p-1)p^{k-1} = \varphi(p^k)$, and g is a primitive root modulo p^k for all $k \geq 1$.

If $k_0 \geq 2$, then

$$g^{p-1} = 1 + p^2 v$$

for some integer v. By the binomial theorem,

$$\begin{aligned} (g+p)^{p-1} &= \sum_{i=0}^{p-1} \binom{p-1}{i} g^{p-1-i} p^i \\ &\equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2} \\ &\equiv 1 + p^2 v + g^{p-2}p^2 - g^{p-2}p \pmod{p^2} \\ &\equiv 1 - g^{p-2}p \pmod{p^2} \\ &\not\equiv 1 \pmod{p^2}. \end{aligned}$$

Then $g + p$ is a primitive root modulo p such that

$$(g+p)^{p-1} = 1 + pu_0 \qquad \text{and} \qquad (u_0, p) = 1.$$

Therefore, $g + p$ is a primitive root modulo p^k for all $k \geq 1$.

Next we prove that primitive roots exist for all moduli of the form $2p^k$. If g is a primitive root modulo p^k, then $g+p^k$ is also a primitive root modulo p^k. Since p^k is odd, it follows that one of the two integers g and $g+p^k$ is odd, and the other is even. Let g_1 be the odd integer in the set $\{g, g+p^k\}$. Since $(g+p^k, p^k) = (g, p^k) = 1$, it follows that $(g_1, 2p^k) = 1$. The order of g_1 modulo $2p^k$ is not less than $\varphi(p^k)$, which is the order of g_1 modulo p^k, and not greater than $\varphi(2p^k)$. However, since p is an odd prime, we have

$$\varphi(2p^k) = \varphi(p^k),$$

and so g_1 has order $\varphi(2p^k)$ modulo $2p^k$, that is, g_1 is a primitive root modulo $2p^k$. This completes the proof. □

For example, 2 is a primitive root modulo 3. Since 3 is the greatest power of 3 that divides $2^2 - 1$, it follows that 2 is a primitive root modulo 3^k for all $k \geq 1$, and $2 + 3^k$ is a primitive root modulo $2 \cdot 3^k$ for all $k \geq 1$.

Finally, we consider primitive roots modulo powers of 2.

Theorem 3.8 *There exists a primitive root modulo* $m = 2^k$ *if and only if* $m = 2$ *or* 4.

Proof. We note that 1 is a primitive root modulo 2, and 3 is a primitive root modulo 4. We shall prove that if $k \geq 3$, then there is no primitive root modulo 2^k. Since $\varphi(2^k) = 2^{k-1}$, it suffices to show that

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \tag{3.5}$$

for a odd and $k \geq 3$. We do this by induction on k. The case $k = 3$ is congruence (3.1). Let $k \geq 3$, and suppose that (3.5) is true. Then

$$a^{2^{k-2}} - 1$$

is divisible by 2^k. Since a is odd, it follows that

$$a^{2^{k-2}} + 1$$

is even. Therefore,

$$a^{2^{k-1}} - 1 = \left(a^{2^{k-2}} - 1\right)\left(a^{2^{k-2}} + 1\right)$$

is divisible by 2^{k+1}, and so

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}.$$

This completes the induction and the proof of theorem. □

Let $k \geq 3$. By Theorem 3.8, there is no primitive root modulo 2^k, that is, there does not exist an odd integer whose order modulo 2^k is 2^{k-1}. However, there do exist odd integers of order 2^{k-2} modulo 2^k.

Theorem 3.9 *For every positive integer k,*

$$5^{2^k} \equiv 1 + 3 \cdot 2^{k+2} \pmod{2^{k+4}}.$$

Proof. The proof is by induction on k. For $k = 1$ we have

$$5^{2^1} = 25 \equiv 1 + 3 \cdot 2^3 \pmod{2^5}.$$

Similarly, for $k = 2$ we have

$$5^{2^2} = 625 = 1 + 48 + 576 \equiv 1 + 3 \cdot 2^4 \pmod{2^6}.$$

If the theorem holds for $k \geq 1$, then there exists an integer u such that

$$5^{2^k} = 1 + 3 \cdot 2^{k+2} + 2^{k+4}u = 1 + 2^{k+2}(3 + 4u).$$

Since $2k + 4 \geq k + 5$, we have

$$\begin{aligned} 5^{2^{k+1}} &= \left(5^{2^k}\right)^2 \\ &= \left(1 + 2^{k+2}(3 + 4u)\right)^2 \\ &\equiv 1 + 2^{k+3}(3 + 4u) \pmod{2^{2k+4}} \\ &\equiv 1 + 3 \cdot 2^{k+3} \pmod{2^{k+5}}. \end{aligned}$$

This completes the proof. □

Theorem 3.10 *If $k \geq 3$, then 5 has order 2^{k-2} modulo 2^k. If $a \equiv 1 \pmod 4$, then there exists a unique integer $i \in \{0, 1, \ldots, 2^{k-2} - 1\}$ such that*

$$a \equiv 5^i \pmod{2^k}.$$

If $a \equiv 3 \pmod 4$, then there exists a unique integer $i \in \{0, 1, \ldots, 2^{k-2} - 1\}$ such that

$$a \equiv -5^i \pmod{2^k}.$$

Proof. In the case $k = 3$, we observe that 5 has order 2 modulo 8, and

$$\begin{aligned} 1 &\equiv 5^0 \pmod 8, \\ 3 &\equiv -5^1 \pmod 8, \\ 5 &\equiv 5^1 \pmod 8, \\ 7 &\equiv -5^0 \pmod 8. \end{aligned}$$

Let $k \geq 4$. By Theorem 3.9, we have

$$\begin{aligned} 5^{2^{k-2}} &\equiv 1 + 3 \cdot 2^k \pmod{2^{k+2}} \\ &\equiv 1 \pmod{2^k} \end{aligned}$$

and

$$\begin{aligned} 5^{2^{k-3}} &\equiv 1 + 3 \cdot 2^{k-1} \pmod{2^{k+1}} \\ &\equiv 1 + 3 \cdot 2^{k-1} \pmod{2^k} \\ &\not\equiv 1 \pmod{2^k}. \end{aligned}$$

Therefore, 5 has order exactly 2^{k-2} modulo 2^k, and so the integers 5^i are pairwise incongruent modulo 2^k for $i = 0, 1, \ldots, 2^{k-2} - 1$. Since $5^i \equiv 1 \pmod{4}$ for all i, and since exactly half, that is, 2^{k-2}, of the 2^{k-1} odd numbers between 0 and 2^k are congruent to 1 modulo 4, it follows that the congruence

$$5^i \equiv a \pmod{2^k}$$

is solvable for every $a \equiv 1 \pmod{4}$. If $a \equiv 3 \pmod{4}$, then $-a \equiv 1 \pmod{4}$ and so the congruence

$$-a \equiv 5^i \pmod{2^k},$$

or, equivalently,

$$a \equiv -5^i \pmod{2^k},$$

is solvable. This completes the proof. □

thank you