Introduction to number theory-8

May 22, 2017

Pseudoprimes and Carmichael Numbers

Suppose we are given an odd integer $n \geq 3$, and we want to determine whether n is prime or composite. If n is "small," we can simply divide n by all odd integers d such that $3 \leq d \leq \sqrt{n}$. If some d divides n, then n is composite; otherwise, n is prime. If n is "big," however, this method is time-consuming and impractical.

Fermat's theorem can be applied to this problem. By Fermat's theorem, if n is an odd prime, then $2^{n-1} \equiv 1 \pmod{n}$. Therefore, if n is odd and $2^{n-1} \not\equiv 1 \pmod{n}$, then n must be composite. In general, we can choose any integer b that is relatively prime to n. By Fermat's theorem, if n is prime, then $b^{n-1} \equiv 1 \pmod{n}$. It follows that if $b^{n-1} \not\equiv 1 \pmod{n}$, then n must be composite. Thus, for every base b, Fermat's theorem gives a *primality test*, that is, a necessary condition for an integer n to be prime.

Suppose we want to know whether $n = 851$ is prime or composite. We shall compute $2^{850} \pmod{851}$. An efficient method is to use the 2-adic representation of 850:

$$850 = 2 + 2^4 + 2^6 + 2^8 + 2^9.$$

Since $2^{2^n} = \left(2^{2^{n-1}}\right)^2$, we have

$$
\begin{aligned}
2^2 &\equiv 4 \pmod{851},\\
2^{2^2} &\equiv 16 \pmod{851},\\
2^{2^3} &\equiv 256 \pmod{851},\\
2^{2^4} &\equiv 9 \pmod{851},\\
2^{2^5} &\equiv 81 \pmod{851},\\
2^{2^6} &\equiv 604 \pmod{851},\\
2^{2^7} &\equiv 588 \pmod{851},\\
2^{2^8} &\equiv 238 \pmod{851},\\
2^{2^9} &\equiv 478 \pmod{851}.
\end{aligned}
$$

Then

$$\begin{aligned} 2^{850} &\equiv 2^{2}2^{2^4}2^{2^6}2^{2^8}2^{2^9} \pmod{851} \\ &\equiv 4 \cdot 9 \cdot 604 \cdot 238 \cdot 478 \pmod{851} \\ &\equiv 169 \not\equiv 1 \pmod{581}, \end{aligned}$$

This test can prove that an integer is composite, but it cannot prove that an integer is prime. For example, consider the composite number $n = 341 = 11 \cdot 31$, Choosing base $b = 2$, we have

$$2^{10} \equiv 1 \pmod{11},$$

and so

$$2^{340} \equiv \left(2^{10}\right)^{34} \equiv 1 \pmod{11}.$$

Similarly,

$$2^{5} \equiv 1 \pmod{31},$$

and so

$$2^{340} \equiv \left(2^{5}\right)^{68} \equiv 1 \pmod{31}.$$

Since $2^{340} - 1$ is divisible by both 11 and 31, it is divisible by their product, that is,

$$2^{340} \equiv 1 \pmod{341}.$$

A composite number n is called a *pseudoprime to the base* b if $(b, n) = 1$ and $b^{n-1} \equiv 1 \pmod{n}$.

Can every composite number be *proved* composite by some primality test based on Fermat's theorem? It is a surprising fact that the answer is "no." There exist composite numbers n that cannot be proved composite by any congruence of the form $b^{n-1} \pmod{n}$ with $(b, n) = 1$.

For example, $561 = 3 \cdot 11 \cdot 17$ is composite.
Let b be an integer relatively prime to 561.
Then

$$b^2 \equiv 1 \pmod{3},$$

and so

$$b^{560} = \left(b^2\right)^{280} \equiv 1 \pmod{3}.$$

Similarly,

$$b^{10} \equiv 1 \pmod{11},$$

and so

$$b^{560} = \left(b^{10}\right)^{56} \equiv 1 \pmod{11}.$$

Finally,

$$b^{16} \equiv 1 \pmod{17},$$

and so

$$b^{560} = \left(b^{16}\right)^{35} \equiv 1 \pmod{17}.$$

Since $b^{560} - 1$ is divisible by 3, 11, and 17, it is also divisible by their product, hence

$$b^{560} \equiv 1 \pmod{561}.$$

This proves that 561 is a pseudoprime to base b for every b such that $(b, n) = 1$.

A *Carmichael number* is a positive integer n such that n is composite but $b^{n-1} \equiv 1 \pmod{n}$ for every integer b relatively prime to n. Thus, 561 is a Carmichael number.

Carmichael conjectured in 1912 that the number of Carmichael numbers is infinite. Alford, Granville, and Pomerance [1] confirmed this in 1994. They proved that if $C(x)$ is the number of Carmichael numbers less than x, then $C(x) > x^{2/7}$ for all sufficiently large x. Erdős has made the stronger conjecture that for every $\varepsilon > 0$ there exists a number $x_0(\varepsilon)$ such that $C(x) > x^{1-\varepsilon}$ for all $x \geq x_0(\varepsilon)$.

Polynomials and Primitive Roots

Let m be a positive integer greater than 1, and a an integer relatively prime to m. The *order of* a *modulo* m, denoted by $\mathrm{ord}_m(a)$, is the smallest positive integer d such that $a^d \equiv 1 \pmod{m}$. By Theorem 2.14, $\mathrm{ord}_m(a)$ is a divisor of the Euler phi function $\varphi(m)$. The order of a modulo m is also called the *exponent* of a modulo m.

We investigate the least nonnegative residues of the powers of a modulo m. For example, if $m = 7$ and $a = 2$, then

$$\begin{aligned} 2^0 &\equiv 1 \pmod{7}, \\ 2^1 &\equiv 2 \pmod{7}, \\ 2^2 &\equiv 4 \pmod{7}, \\ 2^3 &\equiv 1 \pmod{7}, \end{aligned}$$

If $m = 7$ and $a = 3$, then

$$\begin{aligned} 3^0 &\equiv 1 \pmod{7}, \\ 3^1 &\equiv 3 \pmod{7}, \\ 3^2 &\equiv 2 \pmod{7}, \\ 3^3 &\equiv 6 \pmod{7}, \\ 3^4 &\equiv 4 \pmod{7}, \\ 3^5 &\equiv 5 \pmod{7}, \\ 3^6 &\equiv 1 \pmod{7}, \end{aligned}$$

and 3 has order 6 modulo 7. The powers of 3 form a reduced residue system modulo 7.

The integer a is called a *primitive root modulo* m if a has order $\varphi(m)$. In this case, the $\varphi(m)$ integers $1, a, a^2, \ldots, a^{\varphi(m)-1}$ are relatively prime to m and are pairwise incongruent modulo m. Thus, they form a reduced residue system modulo m. For example, 3 is a primitive root modulo 7. Similarly, 3 is a primitive root modulo 10, since $\varphi(10) = 4$ and

$$\begin{aligned}
3^0 &\equiv 1 \pmod{10},\\
3^1 &\equiv 3 \pmod{10},\\
3^2 &\equiv 9 \pmod{10},\\
3^3 &\equiv 7 \pmod{10},\\
3^4 &\equiv 1 \pmod{10}.
\end{aligned}$$

Some moduli do not have primitive roots. There is no primitive root modulo 8, for example, since $\varphi(8) = 4$, but

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8, \tag{3.1}$$

and no integer has order 4 modulo 8.

In this section we prove that every prime p has a primitive root. Next we determine all composite moduli m for which there exist primitive roots.

We begin with some remarks about polynomials. Let R be a commutative ring with identity. A *polynomial with coefficients in* R is an expression of the form

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_m \in R$. The element a_i is called the *coefficient* of the term x^i. The *degree* of the polynomial $f(x)$, denoted by $\deg(f)$, is the greatest integer n such that $a_n \neq 0$, and a_n is called the *leading coefficient*. If $\deg(f) = n$, we define $a_i = 0$ for $i > n$. Nonzero constant polynomials $f(x) = a_0 \neq 0$ have degree 0. The zero polynomial $f(x) = 0$ has no degree. A *monic polynomial* is a polynomial whose leading coefficient is 1.

We define addition and multiplication of polynomials in the usual way: If $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$, then

$$(f+g)(x) = \sum_{k=0}^{\max(m,n)} (a_k + b_k) x^k$$

and

$$fg(x) = \sum_{k=0}^{mn} c_k x^k,$$

where

$$c_k = \sum_{\substack{i+j=k \\ 0 \le i \le n \\ 0 \le j \le m}} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}.$$

With this addition and multiplication, the set $R[x]$ of all polynomials with coefficients in R is a commutative ring. Moreover,

$$\deg(f+g) \leq \max(\deg(f), \deg(g)).$$

If $f, g \in F[x]$ for some field F, then

$$\deg(fg) = \deg(f) + \deg(g),$$

and the leading coefficient of fg is $a_m b_n$.

For every $\alpha \in R$, the *evaluation map* $\Theta_\alpha : R[x] \to R$ defined by

$$\Theta_\alpha(f) = f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$$

is a ring homomorphism, that is, $(f+g)(\alpha) = f(\alpha) + g(\alpha)$ and $(fg)(\alpha) = f(\alpha)g(\alpha)$. The element α is called a *zero* or a *root* of the polynomial $f(x)$ if $\Theta_\alpha(f) = f(\alpha) = 0$.

We say that the polynomial $d(x)$ divides the polynomial $f(x)$ if there exists a polynomial $q(x)$ such that $f(x) = d(x)q(x)$.

Theorem 3.1 (Division algorithm for polynomials) *Let F be a field. If $f(x)$ and $d(x)$ are polynomials in $F[x]$ and if $d(x) \neq 0$, then there exist unique polynomials $q(x)$ and $r(x)$ such that $f(x) = d(x)q(x) + r(x)$ and either $r(x) = 0$ or the degree of $r(x)$ is strictly smaller than the degree of $d(x)$.*

Theorem 3.2 *Let* $f(x) \in F[x]$, $f(x) \neq 0$, *and let* $N_0(f)$ *denote the number of distinct zeros of* $f(x)$ *in* F. *Then* $N_0(f)$ *does not exceed the degree of* $f(x)$, *that is,*

$$N_0(f) \leq \deg(f).$$

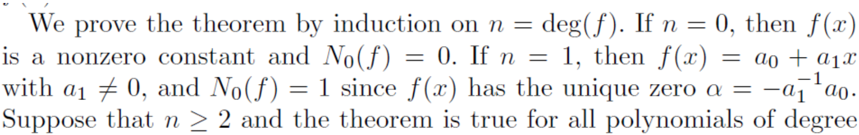
Proof. We use the division algorithm for polynomials. Let $\alpha \in F$. Dividing $f(x)$ by $x - \alpha$, we obtain

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

where $r(x) = 0$ or $\deg(r) < \deg(x - \alpha) = 1$, that is, $r(x) = r_0$ is a constant. Letting $x = \alpha$, we see that $r_0 = f(\alpha)$, and so

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

for every $\alpha \in F$. In particular, if α is a zero of $f(x)$, then $x - \alpha$ divides $f(x)$.



We prove the theorem by induction on $n = \deg(f)$. If $n = 0$, then $f(x)$ is a nonzero constant and $N_0(f) = 0$. If $n = 1$, then $f(x) = a_0 + a_1 x$ with $a_1 \neq 0$, and $N_0(f) = 1$ since $f(x)$ has the unique zero $\alpha = -a_1^{-1} a_0$. Suppose that $n \geq 2$ and the theorem is true for all polynomials of degree at most $n-1$. If $N_0(f)=0$, we are done. If $N_0(f)\geq 1$, let $\alpha\in F$ be a zero of $f(x)$. Then

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

and

$$\deg(q)=n-1.$$

If β is a zero of $f(x)$ and $\beta\neq\alpha$, then

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

and so β is a zero of $q(x)$. Since $\deg(q)=n-1$, the induction hypothesis implies that

$$N_0(f)\leq 1+N_0(q)\leq 1+\deg(q)=n.$$

This completes the proof. □

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

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

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

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

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 $\text{ind}_2(a)$ for $a = 1, \ldots, 12$:

a	$\text{ind}_2(a)$	a	$\text{ind}_2(a)$
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 $k \geq k_0$.*

thank you