Crandall R., Pomerance C. Prime numbers. A computational perspective (2ed., Springer, 2005)

Notes from [CP].

1 Primes!

1.1 Problems and progress

1.2 Celebrated conjectures and curiosities

1.3 Primes of special form

1.4 Analytic number theory

1.4.1 The Riemann zeta function

1.4.2 Computational successes

1.4.3 Dirichlet L-functions

2 Number-theoretical tools

2.1 Modular arithmetic

2.2 Polynomial arithmetic

2.3 Squares and roots

2.3.1 Quadratic residues

Definition. (2.3.6) The quadratic Gauss sum $G(a;N)$ is defined for integers a, N as

$$G(a;N) = \sum_{j=0}^{N-1} e^{2\pi i a j^2/N}.$$

Theorem (Gauss). *(2.3.7) For odd prime p and integer $a \not\equiv 0 \pmod{p}$,*

$$G(a;p) = \left(\frac{a}{p}\right) G(1;p),$$

and generally, for positive integer m,

$$G(1;m) = \frac{1}{2}\sqrt{m}(1+i)(1+(-i)^m).$$

For $a \not\equiv 0 \pmod{p}$

$$\left(\frac{a}{p}\right) = \frac{c}{\sqrt{p}} \sum_{j=0}^{p-1} \sum_{j=0}^{p-1} e^{2\pi i a j^2/p} = \frac{c}{\sqrt{p}} \left(\frac{j}{p}\right) \sum_{j=0}^{p-1} \sum_{j=0}^{p-1} e^{2\pi i a j/p} \tag{2.12}$$

2.3.2 Square roots

3 Recognizing primes and composites

3.1 Trial division

3.2 Sieving

3.3 Recognizing smooth numbers

3.4 Pseudoprimes

3.4.1 Fermat pseudoprimes

For a coprime to n

$$a^{n-1} \equiv 1 \pmod{n}. \tag{3.3}$$

3.4.2 Carmichael numbers

3.5 Probable primes and witnesses

Theorem. *(3.5.1) Suppose that n is an odd prime and $n - 1 = 2^s t$, where t is odd. If a is not divisible by n then*

$$\begin{cases} \text{either } a^t \equiv 1 \pmod{n}, \\ \text{or } a^{2^i t} \equiv -1 \pmod{n} \text{ for some } i \text{ with } 0 \le i \le s-1. \end{cases} \tag{3.4}$$

strong probable prime base a

Definition. (3.5.3) *strong pseudoprime base a* = composite number fulfilling (3.4)

$$\mathcal{S}(n) = \{a \pmod{n}) \colon n \text{ is a strong pseudoprime base } a\} \tag{3.5}$$

and $S(n) = \#\mathcal{S}(n)$

Theorem. *(3.5.4) For each odd composite integer $n > 9$ we have $S(n) \le \frac{1}{4}\varphi(n)$.*

Definition. (3.5.5) If n is an odd composite number and a is an integer in $[1, n-1]$ for which (3.4) fails, we say that a is a witness for n. Thus, for an odd composite number n, a witness is a base for which n is not a strong pseudoprime.

Lemma. *(3.5.8) Say n is an odd composite number with $n - 1 = 2^s t$, t odd. Let $\nu(n)$ denote the largest integer such that $2^{\nu(n)}$ divides $p - 1$ for each prime p dividing n. If n is a strong pseudoprime base a, then $a^{2^{\nu(n)-1}} t \equiv \pm 1 \pmod{n}$.*

$$\overline{\mathcal{S}}(n) = \{a \pmod n \colon a^{2^{\nu(n)-1}t} \equiv \pm 1 \pmod n\}, \qquad \overline{S}(n) = \#\overline{\mathcal{S}}(n) \quad (3.6)$$

Lemma. *(3.5.9) Let $\omega(n)$ the number of different prime factors of n. We have*

$$\overline{S}(n) = 2 \cdot 2^{(\nu(n)-1)\omega(n)} \prod_{p|n} \gcd(t, p-1).$$

For an odd prime p and positive integer j, the group $\mathbb{Z}^*_{p^j}$ of reduced residues modulo p^j is cyclic of order $p^{j-1}(p-1)$; that is, there is a primitive root modulo p^j. (This theorem is mentioned in Section 1.4.3 and can be found in most books on elementary number theory. Compare, too, to Theorem 2.2.5.)

3.5.1 The least witness for n

3.6 Lucas pseudoprimes

3.7 Fibonacci and Lucas pseudoprimes

$u_j = 0, 1, 1, 2, 3, 5, \ldots$ starting with $j = 0$

Theorem. *(3.6.1) If n is prime then*

$$u_{n-\varepsilon_n} \equiv 0 \pmod n \quad (1)$$

where $\varepsilon_n = 1$ when $n \equiv \pm 1 \pmod 5$, $\varepsilon_n = -1$ when $n \equiv \pm 2 \pmod 5$ and $\varepsilon_n = 0$ when $n \equiv 0 \pmod 5$.

Definition. We say that a composite number n is a Fibonacci pseudoprime if (1) holds.

$f(x) = x^2 - ax + b$, where a, b are integers with $\Delta = a^2 - 4b$ is not square

$$U_j = U_j(a,b) = \frac{x^j - (a-x)^j}{x - (a-x)} \pmod{f(x)} \quad (2)$$

$$V_j = V_j(a,b) = x^j + (a-x)^j \pmod{f(x)} \quad (3)$$

where the notation means that we take the remainder in $\mathbb{Z}[x]$ upon division by $f(x)$. [1]

recurrence

$$U_j = aU_{j-1} - bU_{j-2}, \qquad V_j = aV_{j-1} - bV_{j-2}$$

with $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = a$

[1] My note: This is the same as $\frac{\varphi_1^n - \varphi_2^n}{\varphi_1 - \varphi_2}$ and $\varphi_1^n + \varphi_2^n$, where $\varphi_{1,2}$ are the roots of the polynomial $f(x)$.

Theorem. *(3.6.3) If p is a prime with $gcd(p, 2b\Delta) = 1$, then*

$$U_{p-\left(\frac{\Delta}{p}\right)} \equiv 0 \pmod{p}. \tag{4}$$

Definition. We say that a composite number n with $gcd(n, 2b\Delta) = 1$ is a *Lucas pseudoprime* with respect to $x^2 - ax + b$ if $U_{n-\left(\frac{\Delta}{n}\right)} \equiv 0 \pmod{n}$..

3.7.1 Grantham's Frobenius Test

3.7.2 Implementing Lucas and quadratic Frobenius test

$$U_m = \frac{2V_{m+1} - aV_m}{\Delta} \tag{5}$$

$$V_{j+k} = V_j V_k - b^j V_{k-j} \text{ for } 0 \leq j \leq k \tag{6}$$

$$\tag{7}$$

Suppose now that $b = 1$

$$V_{2j} = V_j^2 - 2, \qquad V_{2j+1} = V_j V_{j+1} - a \tag{8}$$

Exercise 3.41?

3.8 Counting primes

3.9 Exercises

3.10 Research problems

4 Primality proving

4.1 The $n - 1$ test

Theorem (Lucas theorem). *(4.1.1) If a, n are integers with $n > 1$ and*

$$a^{n-1} \equiv 1 \pmod{n}, \text{ but } a^{(n-1)/q} \not\equiv 1 \pmod{n} \text{ for every prime } q \mid n-1, \tag{9}$$

then n is prime.

Theorem (Pepin test). *(4.1.2) For $k \geq 1$, the number $F_k = 2^{2^k} + 1$ is prime if and only if $3^{(F_k-1)/2} \equiv -1 \pmod{F_k}$.*

4.2 The $n + 1$ test

4.2.1 The Lucas-Lehmer test

$$f(x) = x^2 - ax + b, \qquad \Delta = a^2 - 4b \tag{4.12}$$

$$U_j = U_j(a,b) = \frac{x^j - (a-x)^j}{x-(a-x)} \pmod{f(x)} \tag{4.13}$$

$$V_j = V_j(a,b) = x^j + (a-x)^j \pmod{f(x)} \tag{10}$$

Definition. (4.2.1) With the above notation, if n is a positive integer with $\gcd(n, 2b\Delta) = 1$, the *rank of appearance* of n denoted by $r_f(n)$, is the least positive integer r with $U_r \equiv 0 \pmod n$.

[2]

It is apparent from the definition that (U_k) is a "divisibility sequence," that is $k \mid j \Rightarrow U_k \mid U_j$. It follows from (4.13) that if $\gcd(n, 2b\Delta) = 1$ then $U_j \equiv 0 \pmod n$ if and only if $j \equiv 0 \pmod{r_f(n)}$.

Theorem. *(4.2.2) With f, Δ as in (4.12) and p a prime not dividing $2b\Delta$, we have $r_f(p) \mid p - \left(\frac{\Delta}{p}\right)$.*

Theorem (Morrison). *(4.2.3) Let f, Δ be as in (4.12) and let n be a positive integer with $\gcd(n, 2b) = 1$, $\left(\frac{\Delta}{n}\right) = -1$. If F is a divisor of $n+1$ and*

$$U_{n+1} \equiv 0 \pmod n, \qquad \gcd(U_{(n+1)/q}, n) = 1 \text{ for every prime } q \mid F \tag{11}$$

then every prime dividing n satisfies $p \equiv \left(\frac{\Delta}{p}\right) \pmod F$. In particular, if $F > \sqrt{n} + 1$ and (11) holds, then n is a prime.

The condition (11) implies $U_{n+1} \equiv 0 \pmod p$ and $U_{\frac{n+1}{q}} \not\equiv 0 \pmod p$ for prime divisors q of F.

Theorem. *(4.2.4) Let p be an odd prime and let N be the number of pairs $a, b \in \{0, 1, \ldots, p-1\}$ such that if f, Δ are given as in (4.12), then $\left(\frac{\Delta}{p}\right) = -1$ and $r_f(p) = p+1$. Then $N = \frac{1}{2}(p-1)\varphi(p+1)$.*

Theorem. *(4.2.5) Let f, Δ be as in (4.12) and let n be a positive integer with $\gcd(n, 2b) = 1$ and $\left(\frac{\Delta}{n}\right) = -1$. If F is an even divisor of $n+1$ and*

$$V_{F/2} \equiv 0 \pmod n, \qquad \gcd(V_{F/2}, n) = 1 \text{ for every prime } q \mid F, \tag{12}$$

then every prime p dividing n satisfies $p \equiv \left(\frac{\Delta}{p}\right) \pmod F$. In particular, if $F > \sqrt{n} + 1$, then n is prime.

Theorem (Lucas-Lehmer test for Mersenne primes). *(4.2.6) Consider the sequence (v_k) for $k = 0, 1, \ldots$, recursively defined by $v_0 = 4$ and $v_{k+1} = v_k^2 - 2$. Let p be an odd prime. Then $M_p = 2^p - 1$ is a prime if and only if $v_{p-2} \equiv 0 \pmod{M_p}$.*

[2]My note: Does $r_f(n)$ exist for each n?

The proof uses the polynomial $f(x) = x^2 - 4x + 1$ with $\Delta = 12$. It is shown that $\left(\frac{\Delta}{M_p}\right) = -1$. [3]

4.3 The finite field primality test

Indeed, we have the following theorem, which appeared in [Adleman et al. 1983]. The proof uses some deep tools in analytic number theory.

Theorem. *(4.3.5) Let $I(x)$ be the least positive squarefree integer I such that the product of primes p with $p - 1 \mid I$ exceeds x. Then there is a number c such that $I(x) < (\ln x)^{c \ln \ln x}$ for all $x > 16$.*

4.4 Gauss and Jacobi sums

In 1983, Adleman, Pomerance, and Rumely [Adleman et al. 1983] published a primality test with the running-time bound of $(\ln n)^{c \ln \ln n}$ for prime inputs n and some positive constant c. The proof rested on Theorem 4.3.5 and on arithmetic properties of Jacobi sums.

4.4.1 Gauss sums test

4.4.2 Jacobi sums test

Contents

[3] My note: Since we know that $V_{2m} = V_m^2 - 2$ from (8), we could perhaps use any polynomial with $\left(\frac{\Delta}{M_p}\right) = -1$? No! (8) is true only for $b = 1$.

References

[CP] R. Crandall and C. Pomerance. *Prime Numbers, a Computational Perspective*. Springer-Verlag, New York, 2001.