Scribe Notes for *Algorithmic Number Theory*
Class 25—June 22, 1998

Scribes: Cara Struble and Craig Struble

Abstract

We start Chapter 9 on testing primality.

1 Testing Primality

Problem: PRIMES
Instance: An integer $n \in \mathbb{Z}^+$.
Question: Is n a prime number?

From Section 5.6, if $2 \nmid n$ then the multiplicative group $(\mathbb{Z}/(n))^*$ is cyclic and of order $\phi(n)$.

Theorem 1.1 (Euler-Fermat Theorem). *If* $\gcd(a, n) = 1$ *then* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Theorem 1.2 (Fermat's Theorem). *If* p *is prime and* $p \nmid a$, *then* $a^{p-1} \equiv 1 \pmod{n}$.

Theorem 1.3 (Theorem 9.1.1). *The positive integer* n *is prime if and only if there exists an integer* a *such that* $a^{n-1} \equiv 1 \pmod{n}$ *and* $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ *for all primes* q *that are factors of* $n - 1$.

These theorems are the background facts we can use in primality testing.

2 Application

An application of testing primality is Rivest-Shamir-Adleman (RSA) public key encryption.

The set up:

1. Choose two large distinct primes p and q.
2. Choose an integer d less than pq such that $\gcd(d, \phi(pq)) = 1$.
3. Compute e such that $ed \equiv 1 \pmod{\phi(pq)}$ with the Extended Euclidean Algorithm.
4. Make public pq and e. Keep p, q, and d private.

Encryption: $E(m) = m^e \pmod{pq}$.
Decryption: $D(x) = x^d \pmod{pq}$.
Check that this works:

$$\begin{aligned} D(E(m)) &= (m^e)^d \pmod{pq} \\ &= m^{ed} \pmod{pq} \\ &= m \pmod{pq}, \end{aligned}$$

because $ed \equiv 1 \pmod{\phi(pq)}$ and $(\mathbb{Z}/(pq))^*$ is cyclic of order $\phi(pq)$.

Example 2.1. Let $p = 47$ and $q = 59$. Then $pq = 2773$. Choose $d = 157$, so $e = 17$ and $de = 1 \pmod{2668}$.

Encryption gives

$$\begin{aligned} E(94) &= 94^{17} \bmod 2773 \\ &= 1883, \end{aligned}$$

while decryption returns

$$\begin{aligned} D(1883) &= 1883^{157} \bmod 2773 \\ &= 94. \end{aligned}$$

Theorem 2.2 (Theorem 9.1.4 (Pratt)). PRIMES $\in NP$.

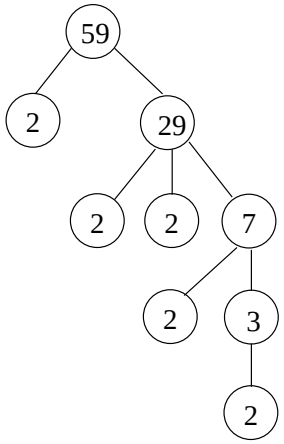
Proof sketch. The strategy is to guess a tree of integers. The tree has these properties:

1. n is at the root.
2. Every leaf is labeled 2.
3. If t is an internal node, then the product of the children of t is $t - 1$.

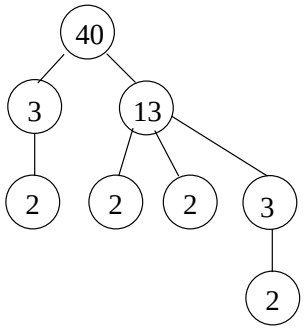
Now proceed bottom-up to prove each integer in the tree is prime. Let s be one such integer. Use Theorem 9.1.1 to guess a_s such that $a_s^{s-1} \equiv 1 \pmod{s}$ and $a_s^{(s-1)/q} \not\equiv 1 \pmod{s}$ for every child q of s. If we find such an a_s, then s is proven to be prime. The tree has polynomial size. The algorithm works in polynomial time. Hence PRIMES $\in NP$. □

The tree together with the a_s's is a **certificate** of the primality of n.

Example 2.3. This is a tree for $n = 59$. (n is prime.)



Example 2.4. This is a tree for $n = 40$. (n is composite.)



The following is a deterministic polynomial time primality test.

```
FELLOWS-KOBLITZ(n, q_1, e_1, ..., q_k, e_k)
 1  ▷ Here  n − 1 = q_1^{e_1} ··· q_k^{e_k}  is the prime factorization of  n − 1
 2  for a ← 2 to ⌊(log n)^2⌋
 3  do if a^{n−1} ≢ 1  (mod n)
 4        then return "composite"
 5     Compute ord_n a                          ▷ Exercise 5.8
 6     for each prime q | ord_n a
 7     do if gcd(a^{(ord_n a)/q} − 1, n) > 1
 8           then return "composite"
 9  h ← lcm{ord_n a} where 2 ≤ a ≤ (log n)^2
10  if h ≤ √n
11    then return "composite"
12    else return "prime"
```

3 Probabilistic Primality Tests

Recall the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ +1 & \text{quadratic residue} \\ -1 & \text{quadratic nonresidue} \end{cases}$$

From Theorem 5.8.1, we have that if p is an odd prime, then

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

Now we introduce the Jacobi symbol, $\left(\frac{a}{n}\right)$, where n may be composite. If n is prime, the Jacobi symbol behaves just as the Legendre symbol. From Section 5.9, we can compute $\left(\frac{a}{n}\right)$ in polynomial time.

The *set of Euler liars* for n is

$$E(n) \quad = \quad \left\{ a \in (\mathbb{Z}/(n))^* : \left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n \right\}.$$

Lemma 3.1 (Lemma 9.4.1). *Let $n \geq 3$ be an odd integer. Then n is prime if an only if $E(n) = (\mathbb{Z}/(n))^*$.*

SOLOVAY-STRASSEN(n)
1 Choose $a \in \{1, \ldots, n-1\}$ uniformly at random.
2 **if** $\gcd(a, n) \neq 1$
3 **then return** "composite"
4 **else if** $\left(\frac{a}{n}\right) \neq a^{(n-1)/2} \bmod n$
5 **then return** "composite"
6 **else return** "prime"

Theorem 3.2 (Theorem 9.4.2). *If n is prime, then Solovay-Strassen returns "prime". If n is composite, then Solovay-Strassen returns "composite" for at least half of the $a \in \{1, \ldots, n-1\}$. The time complexity is $O((\lg n)^3)$ bit operations.*

Solovay-Strassen is a Monte Carlo algorithm for COMPOSITES.