CSG399: Gems of Theoretical Computer Science. Lectures 18-20. Mar. 17-24 2009.
Instructor: Emanuele Viola Scribe: Zhifeng Sun

Primes is in P

In these notes we present Agrawal, Kayal, and Saxena's algorithm that determines if a given integer n is prime in deterministic polynomial time, i.e. time polylog(n). Previously there were various other algorithms, but these were either randomized, or relied on unproven conjectures in number theory, or had running time slightly superpolynomial, such as Adleman, Pomerance, and Rumely's algorithm that runs in deterministic time $(\log n)^{O(\log\log\log n)}$.

1 Preliminaries

A polynomial of d is a formal sum $\sum_{i=0}^{d} a_i x^i$. We often consider polynomials modulo n, which means that the coefficients are intended modulo n. We also take polynomials modulo other polynomials. For example we consider polynomials modulo $x^r - 1$ which means that the powers of x are intended modulo r. We will consider polynomials modulo $(n, x^r - 1)$ which means that the coefficients are taken modulo n while the powers of x modulo r.

Polynomials can be divided like integers; we write $f(x) | g(x)$ if $\exists h(x)$ such that $f(x) \cdot h(x) = g(x)$. The following lemma gives an example we will use extensively.

Lemma 1. *$\forall a, b, n$: $x^a - x^b \mid x^{na} - x^{nb}$. In particular, $x^a - 1 \mid x^{na} - 1$.*

Proof. For $u := x^a$ and $v := x^b$, $u^n - v^n = (u - v)(u^{n-1} + u^{n-2}v + u^{n-3}v^2 + \ldots + v^{n-1})$. □

Polynomials modulo $(p, h(x))$ is the set of polynomials obtained as remainders when dividing polynomials by $h(x)$, where the coefficients are considered modulo p. If $h(x)$ is of degree d and irreducible modulo p, then these remainders form a field of size p^d. For example, let $p := 2$ and $h(x) := x^2 + x + 1$. The polynomials $\{0, 1, x + 0, x + 1\}$ form a field of size $2^2 = 4$.

We write $a(x) \equiv b(x) \bmod (n, h(x))$ if $h(x) | a(x) - b(x)$ when the coefficients are interpreted modulo n.

2 The new characterization of primes

Some previous algorithms for primality had their roots in Fermat's little theorem, stated next.

Theorem 2 (Fermat's little theorem)**.** *If p is a prime, then for any integer a, $a^p \equiv_p a$.*

The algorithm we are going to discuss has its root in the following generalization of Fermat's little theorem.

Theorem 3. *$\forall a, n$ such that $(a, n) = 1$ (i.e. a and n are co-prime), we have*

$$(x + a)^n \equiv_n x^n + a \iff n \text{ is prime.}$$

Proof. In general,

$$(x+a)^n - x^n - a = \sum_{i=0}^{n} \binom{n}{i} x^i a^{n-i} - x^n - a = \sum_{i=1}^{n-1} \binom{n}{i} x^i a^{n-i} + a^n - a.$$

If n is prime, by Theorem 2, $a^n \equiv_n a$, and for $i = 1, \ldots, n-1$, $n \mid \binom{n}{i}$. This means $(x + a)^n \equiv_n x^n + a$.

If n is not a prime, let $p \mid n$, p prime, and let p^k be the highest power of p that divides n. Consider $\binom{n}{p}$, since p cannot divide $n-1, n-2, \ldots, n-p+1$, it is still the case that p^k is the highest power of p dividing the numerator of $\binom{n}{k}$. But p divides the denominator of $\binom{n}{p}$. So $p^k \nmid \binom{n}{p}$, which means $n \nmid \binom{n}{p}$. □

The crux of the polynomial-time primality algorithm is the following new characterization of prime numbers. This characterization requires to be given a number r modulo which n has high order, where recall n has order t mod r if $n^t \equiv 1 \bmod r$, and $\forall i \in \{1, \ldots, t-1\}$ $n^i \neq 1 \bmod r$. We later point out how, given n, we can efficiently find such an r which is at most $\operatorname{poly}\log n$ by brute-force search among the first $\operatorname{poly}\log n$ integers.

Theorem 4 (Main)**.** *$\exists c > 0$, $\forall n$ if n has order $\geq \log^c n \bmod r$, then n is a prime if and only if the following conditions are all satisfied:*

1. *n is not a perfect power;*
2. *n does not have factors $\leq r + \log^c n$; and*
3. *$\forall a \leq r \cdot \log^c n$, $(x + a)^n \equiv x^n + a \bmod (n, x^r - 1)$.*

We now prove this theorem relying on the following fact about the factorization of the polynomial $x^r - 1$ modulo p. By Lemma 1 this polynomial can always be divided by $x - 1$ and therefore it is not irreducible. The following fact states that it has an irreducible factor $h(x)$ which has degree at least 2 and moreover is such that the order of x is r, where x is interpreted as an element in the field of polynomials mod $(p, h(x))$.

Fact 1. *If p is a prime and $(p, r) = 1$, then $x^r - 1$ has an irreducible factor $h(x) \bmod p$ such that:*

1. *The degree of $h(x)$ is no less than 2, and*
2. *the order of $x \bmod (p, h(x))$ is r.*

We omit the proof of the above fact which is essentially in Example 19.1 in Victor Shoup's "A Computational Introduction to Number Theory and Algebra" (version 2).

3 Proof of Theorem 4

The "⇒" direction is easy: part (1) and (2) are obvious, and part (3) is true by Theorem 3.

In the rest of this section we prove the "⇐" direction by contradiction. We assume that n is not prime and satisfies the conditions in Theorem 4, and we derive a contradiction. Let p be a prime that divides n, and let $h(x)$ be the polynomial from Fact 1. Denote by F the field of polynomials modulo $(p, h(x))$. Define

$$G := \left\{ \Pi_a (x+a)^{l_a} \mod (p, h(x)), \text{ for } a \leq r \cdot \log^c n, l_a \in \mathbb{N} \right\},$$

$$R := \left\{ n^i p^j \bmod r \ \forall i, j \right\}.$$

We reach the contradiction by double-counting G. Specifically we show:

Lemma 5. $|G| \leq n^{2\sqrt{|R|}}$.

Lemma 6. $|G| \gg n^{2\sqrt{|R|}}$.

To prove the lemmas we need a couple more of definitions. Define H like G, but modulo $(p, x^r - 1)$ instead of modulo $(p, h(x))$, i.e.

$$H := \left\{ \Pi_a (x+a)^{l_a} \mod (p, x^r - 1), \text{ for } a \leq r \cdot \log^c n, l_a \in \mathbb{N} \right\}.$$

Also let

$$S := \left\{ k : \forall \text{ polynomial } g(x) \in H, g(x)^k \equiv g\left(x^k\right) \mod (p, x^r - 1) \right\}.$$

Observe that $G \subseteq F^* = F \setminus \{0\}$, because $h(x)$ has degree no less than 2 and thus the elements of G are obtained by multiplying together non-zero elements of F.

3.1 Proof of Lemma 5

We need the following claim.

Claim 1. *We have:*
(1) $a, b \in S \Rightarrow a \cdot b \in S$;
(2) $a, b \in S$, $a \equiv b \bmod r \Rightarrow a \equiv b \bmod |G|$;
(3) $n \in S, p \in S$.

To prove the lemma from the claim consider the integers $n^i p^j$ for $i, j \in \left\{0, 1, \ldots, \sqrt{|R|}\right\}$. There are more than $|R|$ distinct such integers, because n is not a perfect power of p (no duplicates). So two of them are congruent modulo r by the definition of R. Let $n^i p^j \equiv n^{i'} p^{j'} \bmod r$. They are both in S by part 1 and part 3 of Claim 1. And by part 2 of Claim 1, $|G| \mid \left| n^i p^j - n^{i'} p^{j'} \right| \Rightarrow |G| \leq n^{\sqrt{|R|}} \cdot p^{\sqrt{|R|}} \leq n^{2\sqrt{|R|}}$.

Proof of Claim 1. For part 1: any $g(x) \in H$ is of the form $\Pi_a (x+a)^{l_a}$. Since $b \in S$, $g(x)^b \equiv g\left(x^b\right) \mod (p, x^r - 1)$. By changing variables, we have $g(x^a)^b \equiv g\left(x^{ab}\right) \mod (p, x^{ar} - 1)$. Since $x^r - 1 \mid x^{ar} - 1$, we have $g(x^a)^b \equiv g\left(x^{ab}\right) \mod (p, x^r - 1)$. Conclude as follows: since $a \in S$, $g(x)^{ab} \equiv g(x^a)^b \equiv g\left(x^{ab}\right) \mod (p, x^r - 1)$, which means $ab \in S$.

For part 2: Assuming without loss of generality that $a \geq b$, and since $a \equiv b \bmod r$, $\forall g(x)$ we have

$$x^r - 1 \mid x^{a-b} - 1 \mid x^a - x^b \mid g(x^a) - g\left(x^b\right),$$

where the last step follows because if $g(x) = \sum_{i=0}^{d} c_i x^i$, then $g(x^a) - g\left(x^b\right) = \sum_{i=1}^{d} c_i \left((x^a)^i - \left(x^b\right)^i\right)$, and recall that $\forall i \geq 1$, $x^a - x^b \mid (x^a)^i - \left(x^b\right)^i$ by Lemma 1. Combining this with the assumption that $a, b \in S$ we have that for $g \in G$, $g(x)^a \equiv g(x^a) \equiv g\left(x^b\right) \equiv g(x)^b$. Therefore $g(x)^{a-b} \equiv 1 \mod (p, h(x))$. Now pick $g(x)$ to be a generator of G which exists because $G \subseteq F^*$ (F^* is cyclic and a subgroup of a cyclic group is cyclic). This shows $|G| \mid a - b$.

For part 3: $n \in S$ because $\left(\Pi_a (x+a)^{l_a}\right)^n \equiv \Pi_a \left((x+a)^n\right)^{l_a} \equiv \Pi_a (x^n + a)^{l_a} \mod (n, x^r - 1)$ by condition (3) of Theorem 4. Also, $p \in S$ by a similar argument and Theorem 3. □

3.2 Proof of Lemma 6

Let $B := \sqrt{|R|} \cdot \log^{c'} n$ where $c' := c/4$. Consider the polynomials

$$\Pi_{a \in T} (x + a)$$

for all $T \subseteq \{0, 1, \ldots, B\}$. Note $|B| \leq r \cdot \log^c n$, and in particular the values a are contained in the range of values a in the last condition of Theorem 4.

Claim 2. *All these polynomials give distinct elements of G.*

To prove the lemma from this claim note that $|G| \geq 2^{|B|} = 2^{\sqrt{|R|} \cdot \log^{c'} n} \gg n^{2\sqrt{|R|}}$.

Proof of Claim 2. Take $f(x) = \Pi_{a \in T} (x + a)$ where $T \subseteq \{0, 1, \ldots, B\}$, and $g(x) = \Pi_{a \in T'} (x + a)$ where $T' \subseteq \{0, 1, \ldots, B\}$. Assume for the sake of contradiction that $f(x) \equiv g(x) \mod (p, h(x))$. By Fact 1, x has order $r \mod (p, h(x))$. We use this to show $f(x) - g(x)$ has more roots than its degree, which implies that $f(x) - g(x) = 0$, i.e. $f(x) = g(x)$.

Because x has order $r \mod (p, h(x))$, the value x^k are different $\mod (p, h(x))$ for different $k \in R$. We can write $k = s + b \cdot r$ where $s \in S, b \in \mathbb{Z}$. Let $\Delta(x) := f(x) - g(x)$. We have

$$\begin{aligned} \Delta\left(x^k\right) &\equiv \Delta(x^s) \mod x^r - 1 \\ &= f(x^s) - g(x^s) \\ &\equiv f(x)^s - g(x)^s \mod (p, x^r - 1) \\ &\equiv 0 \mod (p, h(x)). \end{aligned}$$

So $\Delta(x)$ has at least $|R|$ roots in F. Now we look at the degree of $\Delta(x)$. This is no more than $B = \sqrt{|R|} \cdot \log^{c'} n$. So we have more roots than the degree if $|R| > \sqrt{|R|} \cdot \log^{c'} n \Leftrightarrow \sqrt{|R|} > \log^{c'} n$. Recall n has order at least $\log^c n \bmod r$. So $|R| \geq \log^c n$, which means $\sqrt{|R|} \geq \log^{c/2} n > \log^{c'} n$, completing the proof. □

4 A polynomial-time algorithm for primality

To devise a deterministic algorithm that tests primality in polylog(n) time based on Theorem 4, we need to be able to:

1. in polylog(n) time compute $r \leq \text{polylog}(n)$ such that the order of n mod r is at least $\log^c n$;
2. in polylog(n) time check if $n = a^b$ for $a, b \in \mathbb{N}$; and
3. in polylog(n) time check if $(x+a)^n \equiv x^n + a \bmod (n, x^r - 1)$ $\forall a \leq r \cdot \log^c n$.

The following claim plus brute-force search gives (1).

Claim 3. *$\forall c$, $\exists d$ such that for every n there is $r \leq \log^d n$ such that the order of n mod r is $\geq \log^c n$.*

Proof. We are going to prove this claim by contradiction. Suppose that $\forall r \leq \log^d n$, n has order smaller than $\log^c n$. Take any prime $r \leq \log^d n$, we have $r \mid n-1$ or $r \mid n^2 - 1$ or $\ldots$ or $r \mid n^{\log^c n} - 1$. Then we have $r \mid \Pi_{i=1}^{\log^c n}(n^i - 1)$. So every prime $\leq \log^d n$ divides $\Pi_{i=1}^{\log^c n}(n^i - 1)$. Equivalently, the product of these primes divides $\Pi_{i=1}^{\log^c n}(n^i - 1)$. But

$$\left(\#\text{ of primes that are smaller or equal to } \log^d n\right) \geq \frac{\log^d n}{\text{polyloglog}(n)} \geq \log^{d-1} n.$$

Since every prime is ≥ 2, the product of these primes $\geq 2^{\log^{d-1} n}$. On the other hand,

$$\Pi_{i=1}^{\log^c n}\left(n^i - 1\right) \leq \left(n^{\log^c n}\right)^{\log^c n} = n^{\log^{2c} n}.$$

We have a contradiction for $2^{\log^{d-1} n} > n^{\log^{2c} n}$, which follows for a suitable choice of d depending on c. □

The following are the solutions to the 3 problems listed at the beginning of this section: (1) follows by Claim 3 plus the fact that we can verify if the order of n mod r is at least $\log^c n$ in polylog(n) time; (2) follows because for any b we can use binary search to check if $n = a^b$, and there are only $\log n$ b's; (3) is standard fast modular exponentiation.