PRIMES is in P

Abha, Akshay, Ratul,Pratik,
Shengyi, Shweta, Shruti

January 27, 2014

1 Algorithm

Input: integer $n > 1$

(1) `if` $n = a^b$, for $a, b \geq 2$ && $b < \log n + 1$ `then`

`return` COMPOSITE

(2) choose smallest r such that $o_r(n) > (\log n)^2$

(3) `if` $\exists \gcd(a, n) < n$ for some $a < r$

`return` COMPOSITE

(4) `if` $n \leq r$, `return` PRIME

(5) `for` $a = 1, 2, \ldots, A = \lceil \sqrt{r} \log n \rceil$ `do`

(6) `if` $(X + a)^n \neq X^n + a \pmod{X^r - 1, p}$ `then`

`return` COMPOSITE

(7) `return` PRIME

2 Time Complexity

We define $\widetilde{O}(m) = O(m(\log m)^{O(1)})$.
The total time complexity: $\widetilde{O}((\log n)^{\frac{21}{2}})$

3 Basics

Definition 1 $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

Definition 2 $f(x) \pmod{x^r - 1, n}$ *can be defined as two successive operations*

1. $f(x) \pmod{x^r - 1}$ *[on polynomials]*
2. $f(x) \pmod{n}$ *[on coefficients]*

Definition 3 *Child's Binomial Theorem:* $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$ *and* $gcd(a, n) = 1$. *Then* n *is prime iff*

$$(X + a)^n = X^n + a \pmod{n}$$

Definition 4 *Order of a modulo r: Given* $\gcd(a, r) = 1$, *the order of a modulo r is the smallest number k such that*

$$a^k = 1 \pmod{r}$$

It is denoted as $o_r(a)$.

Definition 5 *Cyclotomic Polynomial: A* n^{th} *cyclotomic polynomial* $\Phi_n(x)$ *is the unique irreducible polynomial with integer coefficients*

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - e^{2i\pi \frac{k}{n}})$$

4 Notations related to the Proof of Correctness

Notation 1 $r \leq \lceil (\log n)^5 \rceil$.

Notation 2 *For each integer* a, $1 \leq a \leq A$, *Let* $h(x)$ *be an irreducible factor of* $\Phi_r(x) \pmod{p}$ *(i.e. in* $(\mathbb{Z}/p\mathbb{Z})[x]$*), then*

$$(x + a)^n = x^n + a \pmod{h(x), p}$$

Notation 3 $\mathbb{F} = \mathbb{Z}[x]/(p, h(x))$.

Notation 4 H *is the multiplicative group modulo* $(x^r - 1, p)$ *generated by* $x, x + 1, x + 2, \cdots, x + A$.

Notation 5 $\mathbb{G}$ *is the (multiplicative) subgroup of* $\mathbb{F}$ *generated by* $x, x + 1, x + 2, \cdots, x + A$.

Notation 6 S *is the set of positive integers* k *for which* $g(x^k) = g(x)^k \pmod{x^r - 1, p}$ *for all* $g \in H$.