LECTURE 12

3/19/2012

Note Title 3/15/2012

TODAY: PRIMALITY TESTING

[AGARWAL, KAYAL, SAXENA '02]

PROBLEM: Given n-bit integer N,

output YES if N is prime, NO otherwise.

Brief History

??? [Pratt] "NP ∩ coNP" "algorithm"

certifies primes; certificates hard to find

1970's: [Miller, Rabin] "Co-RP" algorithm

[Solovay, Strassen]

randomized algorithm; finds certificate for non-primality

1980's: [Goldwasser Kilian] "RP ∩ coRP"

randomized but never wrong.

Certifies Primes.

· 2002: [AKS] Deterministic; (certifies both)

Novelty: Algebraic Approach to Number Theoretic Problem!!

Background [Agarwal, Biswas]

CoRP

New ^ algorithm for primality:

Key Identity

$\forall a$ rel. prime to N $\left\{ (x+a)^N = x^N + a \pmod N \right\}$

$\Leftrightarrow$ N is prime

Proof • N prime $\Rightarrow \binom{N}{i} = 0 \pmod N$

$\forall i$

• $N = P \cdot Q$, (Q, P) rel. prime

$\Rightarrow \binom{N}{P} \equiv Q \pmod P$

$\not\equiv 0 \pmod N$ ☒

Implications

- Can we check if $(x+a)^N = x^N + a \pmod N$

  - not directly. LHS is a degree N polynomial in x. Can't compute coefficients explicitly (in $\text{poly}(\log N)$ time).

  - [Agarwal-Biswas]

    * Pick random polynomial $Q(x) \in \mathbb{Z}_N[x]$ of degree $\text{poly} \log N$

    * Verify $(x+a)^N - x^N - a \equiv 0 \pmod{N, Q}$

  - Analysis:

Claim 1: Conditioned on Q being irred.

$\Pr\left[(x+a)^N - x^N - a \equiv 0 \pmod{Q} \mid \cdot\right] \to 0$ (CRT)

Claim 2:

$\Pr[Q \text{ irreducible}] \geq \frac{1}{\deg(Q)}$ (allowed to in lecture 2)

[AKS]

- "Derandomization" of [AB]

- Find special set S of Q's of $\text{poly}(\log N)$ and special small set A of a's

size. Prove that if

$$(X+a)^N - X^N - a \equiv 0 \pmod{Q, N}$$

$$\forall\, Q \in S$$

$\Rightarrow N$ is prime.

$S = ?$ "cyclotomic polynomials"

$A = ?$ any large enough set will do.

$$S = \{(x^r - 1) \mid 1 \le r \le (\log N)^{O(1)}\}$$

$\exists c$ s.t.

Main Theorem: if $N \neq p^t$ for some prime p,

then $\exists r \leq (\log N)^c$ $\forall A \in \{1, \dots N-1\}$

$|A| \geq (\log N)^c$, $\exists a \in A$ s.t.

$$(X+a)^N - X^N - a \equiv 0 \pmod{N, X^r - 1}$$

Key Ideas in Proof:

(1) Work with ring $R = \mathbb{Z}_N[x] / x^r - 1$ "pseudofield".

- Let p be prime dividing N & $h(x)$ be irred. factor of $x^r - 1 \in \mathbb{F}_p[x]$.

Then R "more informative" than $K = \mathbb{F}_p[x]/h$ (field)

- if $L = \mathbb{F}_p[x]/x^r - 1$,

then $K \hookrightarrow L \hookrightarrow R$

② "Introverting numbers":

- m is introverting for $f(x) \in L$ if $f(x^m) = f(x)^m$
- p is introverting for all $f(x) \in L$
- Test $\Rightarrow$ N is introverting for
  1. $f(x) = x + a$
  2. $f(x) = \prod_{a \in A} (x+a)^{d_a}$

Claim: m is introverting for f, g $\Rightarrow$ m is introverting for $f \cdot g$

Proof:

$$(f \cdot g)(x^m) = f(x^m) \cdot g(x^m) = f(x)^m \cdot g(x)^m = \left((f \cdot g)(x)\right)^m$$

$\square$

- Next claim $\Rightarrow N^i p^j$ introverting for

$$f(x) = \prod_{a \in A} (x+a)^{d_a}$$

Claim A, B introverting for $f \in L$

$\Rightarrow A \cdot B$ introverting for $f \in L$

Proof: $f(x)^A = f(x^A) \mod x^r - 1$ — (1)

$f(x)^B = f(x^B) \mod (x^r - 1)$ — (2)

$f(x)^{AB} = f(x^A)^B \mod x^r - 1$ — (3)

(raising (1) to power B)

$f(x^A)^B = f(x^{AB}) \mod (x^{Ar} - 1)$ — (4)

(replacing x by x^A in (3))

$= f(x^{AB}) \mod (x^r - 1)$ — (5)

$(x^r - 1 \mid x^{Ar} - 1)$

(3) + (5) $\Rightarrow$ ☒

What use is introversion?

- $f(x^m) = f(x)^m$ is not "algebraic"
- how to convert above to algebraically useful stuff.
- Suppose $m_1 = m_2 \pmod r$

  Then $x^{m_1} = x^{m_2} \pmod{x^r - 1}$

  $f(x^{m_1}) = f(x^{m_2}) \pmod{x^r - 1}$

  Suppose further m_1, m_2 introverting for f

  Then $f(x)^{m_1} = f(x)^{m_2} \pmod{x^r - 1}$
- Thus $f \in L$ is a root of $z^{m_1} - z^{m_2}$!
- L is not a field, but it contains K which is!
- if many f's are distinct & m_1, m_2 small, then we have something!

(m_1, m_2) small

PHP !

Let $\mathcal{Y}_t = \left\{ \prod_{a \in A} (x+a)^{d_a} \;\middle|\; \sum d_a \le t \right\}$

Claim: $\exists\ m_1, m_2 \le N^{2\sqrt{r}}$ s.t.

(1) $\forall\ t\ \forall\ f \in \mathcal{Y}_t$, m_1, m_2 interverted for $\mathcal{Y}_t$

(2) $m_1 \equiv m_2 \pmod r$

Proof: Try all the numbers $X = \left\{ p^i N^j \;\middle|\; \begin{matrix} i \le \sqrt{r} \\ j \le \sqrt{r} \end{matrix} \right\}$

All X interverted for $\mathcal{Y}_t$. $|X| > r$

$\Rightarrow \exists\ m_1 \neq m_2 \in X$ s.t. $m_1 = m_2 \pmod r$

$\boxtimes$

Fix m_1, m_2 & Let $P(z) = z^{m_1} - z^{m_2} \in K[z]$

if $t = \deg h - 1$

then all c'ts of y_t distinct mod h

So every c't of $y_t \in K$ is a root

of $P(z)$. Yields contradiction if

$$|y_t| > N^{2\sqrt{r}} > \max\{m_1, m_2\}$$

$$|y_t| \geq \binom{t+|A|}{t} \geq 2^{|A|} \geq N^{2\sqrt{r}}$$

provided $t \geq 2|A|$ & $|A| \geq 2\sqrt{r}\log N$

— ϕ —

Number-theoretic conclusion:

Thm 1: [Fouvry] $\exists$ prime r s.t.

$\deg(h)$ [irred. factor of $x^r - 1$] $\geq r^{2/3}$

(bit complex to prove ....)

But we can do better (more self-contained)

Key Idea to improved analysis

Work with $\mathcal{I}_t$ with $t > \deg h$

Let $T = \{ N^i p^j \pmod r \mid i,j \in \mathbb{Z}^+ \}$

$t \triangleq |T|$

Lemma 1: $\exists\, m_1, m_2 \le N^{2\sqrt{t}}$ s.t.

$m_1, m_2 \in \{ N^i p^j \}$

$m_1 = m_2 \pmod r$

Proof: PHP as before ⊠

Lemma 2: if $f(x), g(x) \in \mathcal{I}_{t-1}$

then $f(x) \not\equiv g(x) \pmod{h(x), p}$

Proof: Recall $K = \mathbb{F}_p[x]/h(x)$

Consider $\ell(z) = f(z) - g(z)$

$\deg \ell \leq t-1$; $\ell \neq 0$;

But $\ell(x) = 0$ if $f(x) = g(x) \pmod{h(x)}$

Furthermore

$$\ell(x^a) = 0 \quad \forall \; a \in T$$

since $f(x^a) = f(x^{N^i p^j}) \pmod{x^r - 1}$

$= f(x)^{N^i p^j}$ (introvertedness)

& same for $g(x^a)$

So $\{x^a \mid a \in T\}$ are all roots of ℓ.

if these el'ts are distinct, then this contradicts $\deg(\ell) \leq t-1$. if not, then

$x^i = 1$ in K for some $i < 1$

$\Rightarrow x^i - 1 \mid h(x) \Rightarrow \gcd(x^i - 1, x^r - 1) \neq x - 1$

Contradiction if r = prime. ☒

Lemma 3: if $O_r(N) > \Omega(\log N)^2$ then contradiction

Proof: Note $t \geq O_r(N)$

So $|y_{t-1}| \geq \binom{|A|+t}{t} \geq 2^t$ if $t = 2|A|$

But $\deg\left(Q(z) \equiv z^{m_1} - z^{m_2}\right) \leq N^{2\sqrt{t}}$

So contradiction if

$$N^{2\sqrt{t}} < 2^t$$

$$\Rightarrow 2\sqrt{t}\log N < t$$

$$t > (\log N)^2 \quad \blacksquare$$

Resulting Alg: - Find r prime s.t. $O_r(N) \geq c\cdot(\log N)^2$

- $t = O_r(N)$ & $A = \{1 \ldots \frac{t}{2}\}$
- Verify $a \in A$ does not divide N,
- Verify $N \neq m^t$ for integer t,
- Verify $(x+a)^N - x^N - a \equiv 0 \bmod N$ $\forall\, a \in A$.

Number-Theoretic Lemma

Lemma: $\exists$ prime $r \leq O(\ell^2 \log N)$

$$O_r(N) = \left| \{ N^i \pmod r \mid i \in \mathbb{Z}^+ \} \right| \geq \ell$$

Proof: (uses Corollary from following section)

if $O_r(N) < \ell$, then

$$r \mid M \triangleq \underbrace{\prod_{i=1}^{\ell-1} (N^i - 1)}_{} \quad ; \quad m \leq N^{\ell^2}$$

But

$$\prod_{\substack{\text{prime } r \\ r \leq X}} r > c^X$$

(see Corollary in upcoming pages)

$\Rightarrow$ Such r exists if $X \geq \Omega(\ell^2 \log N)$

Weak Prime Number Theorem: (Proof due M. Nair, cited in [AKS])

Lemma: $\mathrm{LCM}(1,2,\dots 2m+1) \geq 4^m$

Proof: Consider $I = \int_0^1 x^m (1-x)^m dx$

- On the one hand we have $0 \leq x^m(1-x)^m \leq \frac{1}{4^m}$

  & so $0 \leq I \leq \frac{1}{4^m}$. $-(1)$

- On the other, we have

$$I = \int_0^1 \sum_{i=0}^{m} (-1)^i \binom{m}{i} x^{m+i}$$

$$= \sum_{i=0}^{m} (-1)^i \binom{m}{i} \int_0^1 x^{m+i}$$

$$= \sum_{i=0}^{m} (-1)^i \binom{m}{i} \frac{1}{m+i+1}$$

$$= \frac{N}{\mathrm{LCM}(1\dots 2m+1)} \quad \text{for some integer } N$$

$$\geq \frac{1}{\mathrm{LCM}(1\dots 2m+1)} \quad -(2)$$

$(1)+(2) \Rightarrow$ ☒

Weak Prime Number Theorem:

$$\#\{\text{prime numbers} \leq 2m+1\} \geq \frac{m}{\log_4(2m+1)}$$

Proof: Let $p_1 \dots p_k$ be all the primes less than $2m+1$.

Then $\operatorname{LCM}(1 \dots 2m+1) = \prod_{i=1}^{k} p_i^{e_i}$, where $p_i^{e_i} \leq 2m+1$

So $\operatorname{LCM}(1 \dots 2m+1) \leq (2m+1)^k$

$\Rightarrow (2m+1)^k \geq 4^m$ (using Lemma)

$\Rightarrow k \geq \frac{m \log 4}{\log(2m+1)} = \frac{m}{\log_4(2m+1)}$

∎

Corollary: $\exists\, C > 1$ s.t.

$$\prod_{\substack{p_i \leq m \\ p_i \text{ prime}}} p_i > C^m$$

Proof: $\Rightarrow k! \geq \left(\frac{k}{e}\right)^k \geq \left(\frac{m}{\log m}\right)^{m/\log m} \geq C^m$

where $k = \#\{\text{primes} \leq m\}$