CS 681: Computational Number Theory and Algebra Lecture 13: Primality Testing (Continued)
Lecturer: Manindra Agrawal **Notes by: Arun Iyer**

September 8, 2005.

1 Last Lecture Recap

A potential primality test was proposed which generalised the basic approach of using the idea $a^n \equiv a(mod\, n)$ whenever n is prime, over a ring of polynomials. So we have a ring R,

$$R = \mathbb{Z}_n[X]/(X^r - 1)$$

where n is square-free. Also we have a map,

$$\psi(e(X)) = e^n(X),\ e(X) \in R$$

The following question was to be answered, "Is ψ an automorphism of R?".

2 Proceeding towards Proof

To check if ψ is a linear map :

$$\text{test } \psi(e(X)) = e(\psi(X)), \forall e(X) \in R.$$

Let p be a prime divisor of n. Let $h(x)$ be an irreducible factor of $x^r - 1$ over F_p. Let $F = F_p[X]/(h(X))$. Let $deg(h) = d$ then $|F| = p^d$. Field F occurs as one of the components in the direct sum representation of R.

Lemma 2.1 *(First Size Reduction Lemma)*
Let $S \subseteq F$ such that,

1. $\psi(S) \subseteq S$
2. $\forall e(X) \in S,\ \psi(e(X)) = e(\psi(X))$
3. $|S| > n^{2\sqrt{r}}$

Then $n = p^j$ for some j.

Proof: Let $\phi(e(X)) = e^p(X),\ e(X) \in F$. Let $G = \{\, \phi^i\psi^j(X) \,|\, i, j \geq 0,\ X \in F \,\}$. Let $t = |G|$.
Choose a pair $(\alpha, \beta), (\gamma, \delta)$ such that,

1. $(\alpha, \beta) \neq (\gamma, \delta)$
2. $0 \leq \alpha, \beta, \gamma, \delta \leq \sqrt{t}$
3. $\phi^{\alpha}\psi^{\beta}(X) = \phi^{\gamma}\psi^{\delta}(X)$

Such a pair always exists due to pigeonhole principle.
Consider $\phi^{\alpha}\psi^{\beta}(e(X)), e(X) \in S$. Then,

$$\begin{aligned}
\phi^{\alpha}\psi^{\beta}(e(X)) &= \phi^{\alpha}\psi^{\beta-1}(e(\psi(X))) && \dots \text{[By definition of S]} \\
&= \phi^{\alpha}\psi^{\beta-2}(e(\psi^2(X))) && \vdots \\
&\vdots && \vdots \\
&= \phi^{\alpha}(e(\psi^{\beta}(X))) && \vdots \\
&= \phi^{\alpha-1}(e(\phi\psi^{\beta}(X))) && \dots \text{[Since } \phi \text{ is linear over } F\text{]} \\
&\vdots && \vdots \\
&= e(\phi^{\alpha}\psi^{\beta}(X)) && \vdots
\end{aligned}$$

Similarly, it can be shown that,

$$\phi^{\gamma}\psi^{\delta}(e(X)) = e(\phi^{\gamma}\psi^{\delta}(X))$$

Hence,

$$\phi^{\alpha}\psi^{\beta}(e(X)) = \phi^{\gamma}\psi^{\delta}(e(X)), \forall e(X) \in S$$

This implies that, $\phi^{\alpha}\psi^{\beta}(y) - \phi^{\gamma}\psi^{\delta}(y)$ has atleast $|S|$ many roots in F.
Let $P(y) = \phi^{\alpha}\psi^{\beta}(y) - \phi^{\gamma}\psi^{\delta}(y) = y^{n^{\beta}p^{\alpha}} - y^{n^{\delta}p^{\gamma}}$.
$deg(P) = max\left\{n^{\beta}p^{\alpha}, n^{\delta}p^{\gamma}\right\} \leq n^{2\sqrt{t}}$.
However, since $|S| > n^{2\sqrt{r}}$ and $t \leq r$, it implies,

$$\begin{aligned}
\implies \quad P &= 0 \\
\implies \quad n^{\beta}p^{\alpha} &= n^{\delta}p^{\gamma} \\
\implies \quad n^{\alpha'} &= p^{\beta'} && \dots \text{[for some } \alpha', \beta'\text{]} \\
\implies \quad n &= p^{j} && \dots \text{[for some } j\text{]}
\end{aligned}$$

Hence Proved. ■

Let $T = \{\, X^j + a \,|\, 0 \leq j \leq r,\ 0 \leq 2\sqrt{r}logn,\ X \in F \,\}$. Now $|T| \leq 2r^{\frac{3}{2}}logn$, which is small if r is small. Let S be the multiplication closure of T in F.

Lemma 2.2 *(Second Size Reduction Lemma)*
If $p > t > 4log^2 n$ and $\psi(e(X)) = e(\psi(X)), \forall e(X) \in T$, then

1. $\psi(S) \subseteq S$
2. $\psi(e(X)) = e(\psi(X))$

3. $|S| > n^{2\sqrt{t}}$

Proof:

1. Let $e(X) \in S$. Therefore, $e(X) = \prod_{i=1}^{k} e_i(X)$, $e_i(X) \in T$.

$$\begin{aligned} \psi(e(X)) &= \psi(\textstyle\prod_{i=1}^{k} e_i(X)) \\ &= \textstyle\prod_{i=1}^{k} e_i(\psi(X)) \end{aligned}$$

   Since $e_i(\psi X) \in T$, $\psi(e(X)) \in S$.

2. $\psi(e(X)) = \prod_{i=1}^{k} e_i(\psi(X)) = e(\psi(X))$

3. Let $Q = \left\{ \prod_{i=1}^{t}(y + a_i) \,|\, 0 \leq a_i \leq 2\sqrt{r}logn \right\}$.
   Let $q(y) \in Q$. Then, $q(X) \in S$.

$$\begin{aligned} \text{Number of polynomials in Q} &= \begin{pmatrix} 2\sqrt{r}logn + t \\ t \end{pmatrix} \\ &> \begin{pmatrix} 2\sqrt{r}logn + 2\sqrt{t}logn \\ 2\sqrt{t}logn \end{pmatrix} \\ &\geq \begin{pmatrix} 4\sqrt{t}logn \\ 2\sqrt{t}logn \end{pmatrix} \\ &> 2^{2\sqrt{t}logn} \\ &= n^{2\sqrt{t}} \end{aligned}$$

   Now, we make a claim,
   Claim : The map $y \mapsto X$ is 1-1 on Q
   Proof : Let $q_1(y), q_2(y) \in Q$, $q_1 \neq q_2$. Suppose that $q_1(X) = q_2(X)$ in F. We have $q_1(X), q_2(X) \in S$ and,

$$\begin{aligned} & q_1(X) = q_2(X) \\ \implies \quad & \psi(q_1(X)) = \psi(q_2(X)) \\ \implies \quad & q_1(\psi(X)) = q_2(\psi(X)) \\ \implies \quad & q_1(\psi^j(X)) = q_2(\psi^j(X)) \\ \implies \quad & q_1(\phi^i\psi^j(X)) = q_2(\phi^i\psi^j(X)) \\ \implies \quad & q_1(e(X)) = q_2(e(X)) \end{aligned}$$

   The above implies that every $e(X) \in G$ is a root of the polynomial $q_1(y) - q_2(y)$ in F. But $deg(q_1(y) - q_2(y)) \leq t - 1$, which gives us a contradiction. Therefore the map is 1-1.
   The above proof tells us that $|S| = |Q| \geq n^{2\sqrt{t}}$.

Hence Proved. ■