CS 681: Computational Number Theory and Algebra	**Lecture 11**
Lecturer: Manindra Agrawal	**Notes by: Ashwini Aroskar**
	August 30, 2004.

1 Recall

Fact 1.1 $Res(f, g) = 0$ *iff* $gcd(f, g) > 1$

Fact 1.2 *There exists* $y \in F_q$ *such that* $gcd(e(x) - y, f(x)) > 1$

We want $y \in F_q$ such that $Res(e(x) - y, f(x)) = 0$
$Res(e(x) - y, f(x))$ is a polynomial in y over F_q of degree $\leq 2d - 1$
Let this polynomial be $g(y)$.

If we can find a root of g in F_q then we can factorize f.

Let $\hat{g}(y) = gcd(g(y), y^q - y)$
All roots of $g(y)$ in F_q are roots of $\hat{g}(y)$ too.

Now, the remaining problem is to find roots of a given polynomial over a finite field F_q.
No polynomial time algorithm is known for this problem.

2 A Randomized polynomial time algorithm for root finding

Let $f(x)$ be a square-free polynomial over F_q of degree d and such that f factors completely over F_q.

Let $f(x) = \Pi_{i=1}^{d}(x - \alpha_i)$
Note that $\alpha_i \neq \alpha_j$.

Let $f_{ss}(x) = f(x^2 + \beta) = \Pi_{i=1}^{d}(x^2 + \beta - \alpha_i)$

If there exist α_i and α_j such that $x^2 + \beta - \alpha_i$ is reducible and $x^2 + \beta - \alpha_j$ is irreducible, then f_{ss} can be factored.
Using factors of f_{ss}, f can be factored.

Fix $\{\alpha_i, \alpha_j\} = \{\alpha_1, \alpha_2\}$

$Prob[x^2 + \beta - \alpha_1$ and $x^2 + \beta - \alpha_2$ are both reducible or irreducible$]$
$= Prob[$both $\alpha_1 - \beta$ and $\alpha_2 - \beta$ are squares in F_q or neither is$]$
$= Prob[\beta \epsilon F_q : (\alpha_1 - \beta)^{\frac{q-1}{2}} = (\alpha_2 - \beta)^{\frac{q-1}{2}}]$
$= \frac{1}{|F_q|}($ number of roots of polynomial $(\alpha_1 - z)^{\frac{q-1}{2}} - (\alpha_2 - z)^{\frac{q-1}{2}})$
$\leq \frac{q-1}{2q} < \frac{1}{2}$

Choose k values of β.
$Prob[$no value of β helps factor $f_{ss}] < \frac{1}{2^k}$

Repeating this algorithm makes the probability of error very small.
Roots of f can be computed using repeated applications of the algorithm.

There exist randomized polynomial time algorithms for factoring multivariate polynomials in compact representation.

A polynomial over the field of rationals can be factored in polynomial time.