# CS681: Endterm Examination

Maximum Marks: 50

Due by Nov 18, 2009, 19:00 Hrs

**Question 1 (marks 10).** In the deterministic primality test discussed in the class, one needed to test the equation

$$(X + a)^n = X^n + a \ (mod\ n, X^r - 1)$$

for every $a \leq 2\sqrt{r}\log n$. Suppose we know a number $\eta \in Z_n$ such that $\zeta = \eta^{\frac{n-1}{r}} \in Z_n$ is a primitive $r$th root of unity (of course, this requires the condition that $r \mid n-1$). Further assume that polynomial $X^r - \eta$ is irreducible modulo $p$ where $p$ is a prime divisor of $n$ and $r > 4\log^2 n$. Show that the test can be modified to simply testing:

$$(X + 1)^n = X^n + 1 \ (mod\ n, X^r - \eta).$$

Hint: Show that if the above equation holds then so do

$$(\zeta^i X + 1)^n = \zeta^i X^n + 1 \ (mod\ n, X^r - \eta)$$

for every $i < r$. This gives $r$ distinct linear terms (in $X$) for which the equation holds. Now argue over the field $F_p[X]/(X^r - \eta)$.

**Question 2 (marks 15).** This is a simplified *picture differentiation* problem. Given two pictures, as grids of $n \times n$ pixels with each pixel represented by three bytes of RGB values, we need to check if the first one is a simple rotation (along a vertical axis passing through the center of the picture) of the second one. Since the quality of the image may not be good towards the edges, we compare the pictures only inside a circle of radius $\frac{n}{4}$ pixels around the center. Design an efficient algorithm for solving the problem assuming that the angle of rotation is always a multiple of $\frac{2\pi}{m}$ where $m$ is given as a parameter. Analyze the time complexity of your algorithm. What happens if $m$ is unknown? Can you still design an efficient algorithm that will work reasonably well?

**Question 3 (marks 10+5).** Let $f(x, y)$ be a bivariate polynomial over the finite ring $Z_n$ with the degrees of variable $x$ and $y$ bounded by $\ell$ and $m$ respectively in $f$ with $f(x, y) = x^\ell y^m +$ lower degree terms. Define the set

$$P_\epsilon = \{(x, y) \in Z \times Z \mid |x|, |y| \leq n^\epsilon, \wedge f(x, y) = 0 \pmod{n}\}.$$

In other words, $P_\epsilon$ is the set of "small" roots of $f$ modulo $n$.

- Design an efficient algorithm that for $\epsilon \leq \frac{1}{8(\ell+m)}$ and for large enough $n$, finds a polynomial $h(x, y)$ such that if $(x, y) \in P_\epsilon$ then $h(x, y) = 0$ over integers.
- Design an efficient algorithm that, for the above bound on $\epsilon$, computes *all* degree $d$ curves $y = g(x)$ such that

$$|\{(x, y) \mid (x, y) \in P_\epsilon \ \wedge \ y = g(x)\}| > 2dm + 2\ell.$$

**Question 3 (marks 5+5).** Let $n = p \cdot q$.

- Prove that $n$ can be factored efficiently if the number of automorphisms of the ring $Z_n[X]/(X^2)$ can be efficiently computed. *Automorphism* of a ring $R$ is a map $\phi : R \mapsto R$ such that for all $a, b \in R$, $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.
- Suppose that 3 does not divide $p - 1$ and there is an $a$ with $a^3 = 2 \pmod{p}$; in addition, there is no $b$ such that $b^3 = 2 \pmod{q}$. Prove that, given a non-trivial automorphism $\phi$ of the ring $Z_n[X]/(X^3 - 2)$, number $n$ can be factored efficiently. A *non-trivial* automorphism of ring $R$ is an automorphism that is not identity. (Hint: count the size of the set $\{e \mid \phi(e) = e\}$.)