CS60094 Computational Number Theory

End-Semester Test

Maximum marks: 100 April 29, 2010 (AN) **Duration:** 3 hours

Roll No | | | | | | | | | **Name** | |

[*This test is open-notes. Answer all questions. Be brief and precise.*]

1 Let $f(x) \in \mathbb{F}_p[x]$ be a monic irreducible polynomial of degree $n > 1$. Let θ be a root of f. We use the polynomial-basis representation $\mathbb{F}_q = \mathbb{F}_p(\theta)$, where $q = p^n$.

(a) If $f(x)$ has only a few non-zero coefficients, we call it a sparse polynomial. On the other hand, if many coefficients of $f(x)$ are non-zero, we call it a dense polynomial. Explain how sparse irreducible polynomials can make the arithmetic of $\mathbb{F}_q$ efficient (as opposed to dense polynomials). **(6)**

Irreducible binomials, trinomials and quadrinomials (that is, polynomials with only two, three or four non-zero terms) are often employed in the polynomial-basis representation. However, for all values of p and n, such polynomials do not exist.

(b) Check the irreducibility of $x^8 + x + 1 \in \mathbb{F}_2[x]$. **(6)**

(c) Check the irreducibility of $x^8 + x^3 + 1 \in \mathbb{F}_2[x]$. **(6)**

(d) Prove or disprove: There does not exist an irreducible binomial/trinomial/quadrinomial of degree $n = 8$ in $\mathbb{F}_2[x]$. **(6)**

2 An odd prime of the form $k2^r + 1$ with $r \geqslant 1$, k odd and $k < 2^r$ is called a *Proth prime* (after the name of a French farmer François Proth (1852–1879)).

(a) List the four smallest Proth primes > 10. **(6)**

(b) Describe an efficient way to recognize whether an odd positive integer (not necessarily prime) is of the form $k2^r + 1$ with $r \geqslant 1$, k odd and $k < 2^r$. Henceforth, we will call such an integer a *Proth number*. **(6)**

(c) Suppose that a Proth number $n = k2^r + 1$ satisfies the condition that $a^{(n-1)/2} \equiv -1 \pmod{n}$ for some integer a. Prove that n is prime. **(6)**

(d) Devise a (Yes-biased) probabilistic polynomial-time algorithm to test the primality of a Proth number. **(6)**

(e) Discuss how the algorithm of Part (d) can produce a wrong answer. Also estimate the probability of this error. **(6)**

(f) Prove that if the extended Riemann hypothesis (Section 1.9 of notes) is true, one can arrive at a deterministic polynomial-time algorithm to test the primality of a Proth number. **(6)**

3 Find all the points at infinity on the following curves.

(a) The ellipse $\dfrac{X^2}{a^2} + \dfrac{Y^2}{b^2} = 1$ with a, b real and positive, treated as a curve over $\mathbb{C}$. **(6)**

(b) The ellipse $\dfrac{X^2}{1234^2} + \dfrac{Y^2}{5678^2} = 1$ defined over the prime field $\mathbb{F}_{10007}$. **(6)**

4 Consider the cubic curve $E : Y^2 = X^3 + 2X^2 + 1$ defined over $\mathbb{F}_3$.

(a) Prove that E is smooth, that is, an elliptic curve. **(6)**

(b) Find all the points in $E(\mathbb{F}_3)$. **(6)**

(c) Let $P = (0, 1)$ and $Q = (1, 2)$. Determine $P + Q$ and $2P$ as explicit points in $E(\mathbb{F}_3)$. **(6+6)**

5 Let p be an odd prime, and $E : Y^2 = X^3 + aX + b$ an elliptic curve defined over $\mathbb{F}_p$. Prove that the size of the group $E(\mathbb{F}_p)$ is odd if and only if $X^3 + aX + b$ is irreducible in $\mathbb{F}_p[X]$. **(6+6)**