CS60082 Computational Number Theory, Spring 2007

End-semester examination

Total marks: 100 | April 28, 2007 | **Duration:** 3 hours

[*This test is open-notes. Answer all questions.*]

1 Represent $\mathbb{F}_{16}$ as $\mathbb{F}_2(\theta)$, where $\theta^4 + \theta + 1 = 0$.

(a) Find a primitive element of $\mathbb{F}_{16}$ in this representation. **(5)**

(b) How many primitive elements does $\mathbb{F}_{16}$ have? **(5)**

(c) Determine the minimal polynomial of $\theta + 1 \in \mathbb{F}_{16}$ as a polynomial in $\mathbb{F}_2[x]$. **(5)**

2 Let $\mathbb{F}_q$ be a finite field, and let $\gamma \in \mathbb{F}_q^*$ be a primitive element. For every $\alpha \in \mathbb{F}_q^*$, there exists a unique x in the range $0 \leqslant x \leqslant q-2$ such that $\alpha = \gamma^x$. Denote this x by $\operatorname{ind}_\gamma \alpha$ (index of α with respect to γ).

(a) First assume that q is odd. Prove that the equation $x^2 = \alpha$ is solvable in $\mathbb{F}_q$ for $\alpha \in \mathbb{F}_q^*$ if and only if $\operatorname{ind}_\gamma \alpha$ is even. **(2 + 3)**

(b) Next consider $q = 2^n$. In this case, for every $\alpha \in \mathbb{F}_q$, there exists a unique $\beta \in \mathbb{F}_q$ such that $\beta^2 = \alpha$. In fact, $\beta = \alpha^{2^{n-1}}$. Suppose that $\alpha, \beta \in \mathbb{F}_q^*$, $k = \operatorname{ind}_\gamma \alpha$, and $l = \operatorname{ind}_\gamma \beta$. Express l as an efficiently computable formula in k and q. **(5)**

3 Prove that the polynomial $x^4 + 2x + 7$ is irreducible in $\mathbb{Q}[x]$. **(10)**

4 (a) Prove that the polynomials $x^2 + 4$ and $x^3 + 4$ are irreducible in $\mathbb{F}_7[x]$. **(5 × 2)**

(b) Compute the complete factorization of $x^5 + 4x^3 + 4x^2 + 2$ in $\mathbb{F}_7[x]$. **(5)**

5 Determine which of the following curves is/are non-singular (i.e., elliptic curves). **(5 × 2)**

(a) $C_1 : y^2 + 4y = x^3 - 3x - 6$ defined over $\mathbb{Q}$.

(b) $C_2 : y^2 + 4y = x^3 - 3x + 6$ defined over $\mathbb{F}_7$.

6 Consider the elliptic curve $E : y^2 = x^3 + 2x + 3$ defined over $\mathbb{F}_7$, and the points $P = (2, 1)$ and $Q = (3, 6)$ on the curve.

(a) Compute the points $P + Q$, $2P$, and $3Q$ on the curve. **(5 × 3)**

(b) Determine the order of P in the elliptic curve group $E(\mathbb{F}_7)$. **(5)**

(c) What is the number of points on E treated as an elliptic curve over $\mathbb{F}_{49} = \mathbb{F}_{7^2}$? **(10)**

7 Let p be an odd prime with $p \equiv 2 \pmod 3$, and let a be an integer not divisible by p. Prove that the elliptic curve $y^2 = x^3 + a$ defined over $\mathbb{F}_p$ contains exactly $p + 1$ points. **(10)**

Dr. Abhijit Das, Dept. of Computer Science & Engineering, IIT Kharagpur, India