CS60082 Computational Number Theory, Spring 2007

End-semester examination: Solutions

---

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.

Solution The order of the group $\mathbb{F}_{16}^*$ is 15, i.e., every element $\alpha \in \mathbb{F}_{16}^*$ has order $1, 3, 5,$ or 15. We have $\theta \neq 1$, $\theta^3 \neq 1$, and $\theta^5 = \theta(\theta + 1) = \theta^2 + \theta \neq 1$. Thus, θ is a primitive element of $\mathbb{F}_{16}$.

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

Solution $\phi(15) = (3 - 1)(5 - 1) = 8$.

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

Solution We have $\theta + 1 = \theta^4 = \theta^{2^2}$, i.e., $\theta + 1$ is a conjugate of θ, and therefore has the same minimal polynomial as θ, i.e., $\mathrm{minpoly}_{\theta+1}(x) = x^4 + x + 1$.

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 $\mathrm{ind}_\gamma\, \alpha$ (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 $\mathrm{ind}_\gamma\, \alpha$ is even.

Solution Let $\alpha = \gamma^{2k}$. Then $x^2 = \alpha$ has a solution $x = \gamma^k$. Conversely, suppose $x^2 = \alpha$ has a solution $\beta = \gamma^k$. Then $\alpha = \beta^2 = \gamma^{2k} = \gamma^{(2k) \,\mathrm{rem}\, (q-1)}$. Since q is odd, $(2k) \,\mathrm{rem}\, (q - 1)$ is even.

(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 $\alpha, \beta \in \mathbb{F}_q^*$, $k = \mathrm{ind}_\gamma\, \alpha$, and $l = \mathrm{ind}_\gamma\, \beta$. Express l as an efficiently computable formula in k and q.

Solution If k is even, then $l = k/2$. If k is odd, then $l = [k + (q - 1)]/2$. Another (less efficient) formula is $l \equiv kq/2 \pmod{q - 1}$.

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

Solution In order to prove the irreducibility of $f(x) = x^4 + 2x + 7$ over $\mathbb{Q}$, we look at $f(x + 1) = (x^4 + 4x^3 + 6x^2 + 4x + 1) + 2(x + 1) + 7 = x^4 + 4x^3 + 6x^2 + 6x + 10$. Now apply Eisenstein's criterion with respect to the prime $p = 2$.

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

Solution Let $f_1(x) = x^2 + 4$, and $f_2(x) = x^3 + 4$. We have $f_1(0) = 0$, $f_1(1) = 5$, $f_1(2) = 1$, $f_1(3) = 6$, $f_1(4) = 6$, $f_1(5) = 1$, and $f_1(6) = 5$. Also $f_2(0) = 4$, $f_2(1) = 5$, $f_2(2) = 5$, $f_2(3) = 3$, $f_2(4) = 5$, $f_2(5) = 3$, and $f_2(6) = 3$. Therefore, $f_1(x)$ and $f_2(x)$ have no roots in $\mathbb{F}_7$, and so are irreducible.

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

Solution We have $x^5 + 4x^3 + 4x^2 + 2 \equiv x^5 + 4x^3 + 4x^2 + 16 \equiv (x^2 + 4)(x^3 + 4) \pmod 7$.

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

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

Solution Replace $y+2$ by y to rewrite the equation of the curve as $y^2 = x^3 - 3x - 6 + 4$, i.e., $y^2 = x^3 - 3x - 2$. The polynomial $x^3 - 3x - 2 = (x + 1)^2(x - 2)$ has multiple roots, and so C_1 is singular.

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

Solution Again replace $y + 2$ by y to rewrite the equation of the curve as $y^2 = x^3 - 3x + 10$, i.e., $y^2 = x^3 + 4x + 3$. We have $x^3 + 4x + 3 = (x + 4)(x^2 + 3x + 6)$, where the quadratic factor is irreducible. Since $x^3 + 4x + 3$ is square-free, it follows that C_2 is an elliptic curve.

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.

Solution $P + Q = (6, 0)$, $2P = (3, 6) = Q$, and $3Q = \mathcal{O}$.

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

Solution We have $6P = 3Q = \mathcal{O}$, i.e., $\operatorname{ord} P \mid 6$. Now $P \neq \mathcal{O}$, $2P = Q \neq \mathcal{O}$, and $3P = P + 2P = P + Q = (6, 0) \neq \mathcal{O}$. Therefore, $\operatorname{ord} P = 6$.

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

Solution Easy calculations show that $E(\mathbb{F}_7) = \{\mathcal{O}, (2, 1), (2, 6), (3, 1), (3, 6), (6, 0)\}$, i.e., $|E(\mathbb{F}_7)| = 6$, i.e., the trace of Frobenius for E at 7 is $t = (7 + 1) - 6 = 2$. We have $1 - 2x + 7x^2 = (1 - \alpha x)(1 - \beta x)$, where $\alpha = 1 + \mathrm{i}\sqrt{6}$, and $\beta = 1 - \mathrm{i}\sqrt{6}$. Thus $|E(\mathbb{F}_{7^2})| = 7^2 + 1 - (\alpha^2 + \beta^2) = 50 - 2(1 - 6) = 60$.

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.

Solution Since $p \equiv 2 \pmod 3$, we have $p - 1 \equiv 1 \pmod 3$, i.e., $\gcd(p - 1, 3) = 1$, i.e., the map $\mathbb{F}_p \to \mathbb{F}_p$ taking x to $x^3 \pmod p$ is a bijection, and so also is the map $\mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto x^3 + a \pmod p$ for any integer a. We evaluate the right side of the equation $y^2 = x^3 + a$ at all the points of $\mathbb{F}_p$. Exactly $(p - 1)/2$ of the values are quadratic residues, and exactly one value is 0. Thus the total number of finite points on E is $2 \times [(p - 1)/2] + 1 = p$. Additionally considering the point at infinity gives the desired result.