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)**

Solution Multiplication in $\mathbb{F}_q$ involves multiplication of two polynomials over $\mathbb{F}_p$ of degrees $< n$, followed by reduction modulo $f(x)$. For a sparse $f(x)$, the modular reduction becomes efficient, since only a few coefficients need to be adjusted in each iteration of the polynomial division loop.

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)**

Solution We have the following gcd computations in $\mathbb{F}_2[x]$:

$$\begin{aligned} \gcd(x^8 + x + 1, x^2 + x) &= 1, \\ \gcd(x^8 + x + 1, x^4 + x) &= x^2 + x + 1, \end{aligned}$$

that is, $x^8 + x + 1$ is not irreducible.

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

Solution We have the following gcd computations in $\mathbb{F}_2[x]$:

$$\begin{aligned}
\gcd(x^8 + x^3 + 1, x^2 + x) &= 1, \\
\gcd(x^8 + x^3 + 1, x^4 + x) &= 1, \\
\gcd(x^8 + x^3 + 1, x^8 + x) &= x^3 + x + 1,
\end{aligned}$$

that is, $x^8 + x^3 + 1$ is not irreducible.

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

Solution TRUE. No binomial or quadrinomial (of degree > 1) in $\mathbb{F}_2[x]$ can be irreducible, since such a polynomial has the root 1, that is, the factor $x + 1$. An irreducible trinomial in $\mathbb{F}_2[x]$ must be of the form $x^n + x^r + 1$ for $1 \leqslant r \leqslant n - 1$. Since $x^n + x^r + 1$ is irreducible if and only if its opposite $x^n + x^{n-r} + 1$ is irreducible, it suffices to restrict our attention to $1 \leqslant r \leqslant n/2$. For $n = 8$, the polynomials corresponding to $r = 1$ and $r = 3$ are reducible (previous two parts). Finally, $x^8 + x^2 + 1 = (x^4 + x + 1)^2$ and $x^8 + x^4 + 1 = (x^2 + x + 1)^4$.

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)**

Solution 13, 17, 41, 97.

(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)**

Solution Let n be the input integer. If n is even, reject it. If n is odd, compute $n - 1$ (set the least significant bit to 0). Find r (the multiplicity of 2 in $n - 1$) by looking at the bits of $n - 1$ at the least significant end. Finally, compute k by right-shifting $n - 1$ (or n) by r bit positions, and check whether the bit length of k is $\leqslant r$.

(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)**

Solution We prove this by contradiction. Suppose that n is composite. Let p be the smallest prime divisor of n. Then $3 \leqslant p \leqslant \sqrt{n}$. By the given condition, $a^{(n-1)/2} \equiv -1 \not\equiv 1 \pmod{p}$, whereas $a^{n-1} \equiv (-1)^2 \equiv 1 \pmod{p}$, that is, $\operatorname{ord}_p a = t2^r$ for some odd $t \geqslant 1$. But $\operatorname{ord}_p a | p - 1$, that is, $t2^r | p - 1$, that is, $2^r | p - 1$. But $p \neq 1$, so $p - 1 \geqslant 2^r$, that is, $p \geqslant 2^r + 1 > \sqrt{k2^r} + 1 = \sqrt{n-1} + 1 \geqslant \sqrt{n}$, a contradiction to the choice of p.

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

Solution Assume that the input integer n is already a Proth number.

> Repeat the following steps for t times:
>
> 1. Choose a random base a in the range $1 \leqslant a \leqslant n-1$.
> 2. If $a^{(n-1)/2} \equiv -1 \pmod{n}$, return YES.
>
> Return NO.

The running time of this algorithm is dominated by (at most) t modular exponentiations. So long as t is a constant (or a polynomial expression in $\log n$), the running time of this algorithm is bounded from above by a polynomial in $\log n$.

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

Solution When the algorithm returns YES, n is definitely prime (Part (c)). However, the answer NO does not imply that n is certainly composite. In fact, n may be prime, and the algorithm fails to locate a quadratic non-residue in all of the t random choices for a. Since exactly half of $\mathbb{Z}_n^*$ contains quadratic residues (when n is prime), the probability of failure in this case is $1/2^t$.

(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)**

Solution The extended Riemann hypothesis implies that the smallest quadratic non-residue modulo a prime n is $< 2\ln^2 n$. Therefore, checking the congruence $a^{(n-1)/2} \equiv -1 \pmod{n}$ for all the bases $a = 1, 2, 3, \ldots, \lfloor 2\ln^2 n \rfloor$ allows us to deterministically conclude about the primality of n. The running time of this derandomized algorithm is $O(\ln^5 n)$.

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)**

Solution Two points at infinity: $[a, \mathrm{i}b, 0]$ and $[a, -\mathrm{i}b, 0]$.

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

Solution No points at infinity, since -1 does not have a square root modulo a prime congruent to 3 modulo 4.

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)**

Solution Let $f(X, Y) = Y^2 - (X^3 + 2X^2 + 1)$. The partial derivatives $\partial f / \partial X = -4X$ and $\partial f / \partial Y = 2Y$ vanish simultaneously at the point $(0, 0)$. But this point does not lie on the curve. Moreover, a cubic curve of this form is smooth at the point at infinity (this assertion can be explicitly checked using projective coordinates).

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

Solution Put $X = 0$ to get $Y^2 = 1$. This has two roots $Y = 1, 2$.

Put $X = 1$ to get $Y^2 = 1$ which again has two roots 1 and 2.

Finally, put $X = 2$ to get $Y^2 = 2$ which has no roots in $\mathbb{F}_3$.

Therefore, $E(\mathbb{F}_3) = \{\mathcal{O}, (0, 1), (0, 2), (1, 1), (1, 2)\}$.

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

Solution The straight line passing through P and Q has the equation $Y = X + 1$. Plugging in this expression for Y in the equation of the curve gives $(X + 1)^2 = X^3 + 2X^2 + 1$, that is, $X^3 + X^2 + X = 0$, that is, $X(X^2 + X + 1) = 0$, that is, $X(X + 2)^2 = 0$. Thus, the third point of intersection of the line $Y = X + 1$ with the curve is again $Q = (1, 2)$. The opposite of Q is $(1, 1)$, that is, $\boxed{P + Q = (1, 1).}$

The slope of the tangent on the curve at (X, Y) is $\dfrac{\mathbf{d}Y}{\mathbf{d}X} = \dfrac{3X^2 + 4X}{2Y} = \dfrac{2X}{Y}$. At the point $P = (0, 1)$, this slope is 0, that is, the tangent to E at P is $Y = 1$. Substituting this value of Y in the equation of the curve gives $X^2(X + 2) = 0$, that is, the third point of intersection of the tangent with the curve is $(1, 1)$. The opposite of this point is $(1, 2)$, that is, $\boxed{2P = (1, 2) = Q.}$

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)**

Solution [If] $X^3 + aX + b$ has no roots in $\mathbb{F}_p$, that is, for every value of $X = h \in \mathbb{F}_p$, the equation $Y^2 = h^3 + ah + b$ has zero or two roots in $\mathbb{F}_p$ (according as whether $h^3 + ah + b$ is a quadratic non-residue or a quadratic residue modulo p). So the number of finite points in $E(\mathbb{F}_p)$ is even. But $E(\mathbb{F}_p)$ also contains a unique point at infinity.

[Only if] If $X^3 + aX + b$ is reducible, it has one or three roots in $\mathbb{F}_p$. For each such root h, the only solution with $X = h$ is $(h, 0)$. For a non-root h, we have zero or two solutions of $Y^2 = h^3 + ah + b$ as explained in the proof of the "if" part. Therefore, the number of finite points in $E(\mathbb{F}_p)$ is odd, that is, $|E(\mathbb{F}_p)|$ is even.

An algebraic proof: $X^3 + aX + b$ is reducible $\iff$ $X^3 + aX + b$ has a root in $\mathbb{F}_p$ $\iff$ $E(\mathbb{F}_p)$ contains a point of order 2 $\iff$ $|E(\mathbb{F}_p)|$ is even.