CS60082/CS60094 Computational Number Theory

Mid-semester examination

Maximum marks: 70 | February 26, 2009 (AN) | **Duration:** 2 hours

---

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

1 Let $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$. Assume that $a \neq 1$ and $b \neq 1$.

(a) Prove that there exist integers u, v such that $ua + vb = 1$ with $|u| < b$ and $|v| < a$. **(5)**

(b) Prove that any integer $n \geqslant ab$ can be expressed as $n = sa + tb$ with integers $s, t \geqslant 0$. **(5)**

(c) Devise a polynomial-time (in $\log n$) algorithm to compute s and t of Part (b). **(5)**

(d) Determine the running time of your algorithm. **(5)**

(**Remark:** The *Frobenius coin change problem* deals with the determination of the largest positive integer that cannot be represented as a linear non-negative integer combination of some given positive integers $a_1, a_2, \ldots, a_k$ with $\gcd(a_1, a_2, \ldots, a_k) = 1$. For $k = 2$, this integer is $a_1a_2 - a_1 - a_2$.)

2 Let $n \in \mathbb{N}$. Suppose that we want to compute $x^r y^s \pmod{n}$, where r and s are positive integers of the same bit size. By using the repeated square and multiply algorithm, one can compute $x^r \pmod{n}$ and $y^s \pmod{n}$ independently, and then multiply these two values. Alternatively, one may rewrite the square and multiply algorithm using only one loop in which the bits of both the exponents r and s are simultaneously considered. After each square operation, one multiplies by 1, x, y, or xy.

(a) Elaborate the algorithm outlined above. **(5)**

(b) What speedup is this modification expected to produce? **(5)**

(c) Generalize the concept to the computation of $x^r y^s z^t \pmod{n}$, and analyze the speedup. **(5)**

(**Remark:** Computation of elements of the form $x^r y^s \pmod{n}$ is quite common in cryptosystems based on the discrete logarithm problem. Making this computation faster is, therefore, useful in cryptography.)

3 (a) Prove that the polynomial $x^2 + x + 2$ is irreducible modulo 3. **(5)**

Represent $\mathbb{F}_9$ as $\mathbb{F}_3(\theta)$, where $\theta^2 + \theta + 2 = 0$.

(b) Find the roots of $x^2 + x + 2$ in $\mathbb{F}_9$. **(5)**

(c) Find the roots of $x^2 + x + 2$ in $\mathbb{Z}_9$. **(5)**

(d) Prove that θ is a primitive element of $\mathbb{F}_9$. **(5)**

(e) Prove that the polynomial $y^2 - \theta$ is irreducible over $\mathbb{F}_9$. **(5)**

Represent $\mathbb{F}_{81}$ as $\mathbb{F}_9(\psi)$, where $\psi^2 - \theta = 0$.

(f) Determine whether ψ is a primitive element of $\mathbb{F}_{81}$. **(5)**

(g) Find the minimal polynomial of ψ over $\mathbb{F}_3$. **(5)**

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