CS60082 Computational Number Theory

Mid-semester examination

Maximum marks: 60 February 29, 2008 (AN) **Duration:** 2 hours

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

1 Compute all the simultaneous solutions of the following congruences. **(15)**

$$\begin{aligned} 5x &\equiv 3 \pmod{47}, \\ 3x^2 &\equiv 5 \pmod{49}. \end{aligned}$$

2 Let $\sigma(n)$ denote the sum of positive integral divisors of $n \in \mathbb{N}$. Let $n = pq$ with two distinct primes p, q. Devise a polynomial-time algorithm to compute p, q from the knowledge of n and $\sigma(n)$. **(10)**

3 Let $n = pq$ be a product of two distinct *known* primes p, q. Assume that $q^{-1} \pmod{p}$ is available.

Suppose we want to compute $b \equiv a^e \pmod{n}$ for $a \in \mathbb{Z}_n^*$ and $0 \leqslant e < \phi(n)$. To that effect, we first compute $e_p = e \text{ rem } (p-1)$ and $e_q = e \text{ rem } (q-1)$ and then the modular exponentiations $b_p \equiv a^{e_p} \pmod{p}$ and $b_q \equiv a^{e_q} \pmod{q}$. Finally, compute $t \equiv q^{-1}(b_p - b_q) \pmod{p}$.

(a) Prove that $b \equiv b_q + tq \pmod{n}$. **(10)**

(b) Suppose that p, q are both of bit sizes roughly half of that of n. Explain how computing b in this method speeds up the exponentiation process. You may assume classical (that is, high-school) arithmetic for the implementation of products and Euclidean division. **(5)**

4 Imitate the binary gcd algorithm in order to compute the Jacobi symbol $(\frac{a}{b})$. **(10)**

5 **(a)** Compute the continued fraction expansion of $\sqrt{5}$. **(5)**

(b) It is known that all the solutions of $x^2 - 5y^2 = 1$ with $x, y > 0$ are of the form $x = h_n$ and $y = k_n$, where h_n/k_n is a convergent to $\sqrt{5}$. Find the solution of $x^2 - 5y^2 = 1$ with the smallest possible $y > 0$. **(5)**

(c) Let (a, b) denote the smallest solution obtained in Part (b). Define the sequence of pairs (x_n, y_n) of positive integers recursively as follows.

$$\begin{aligned} (x_0, y_0) &= (a, b) \text{ and} \\ (x_n, y_n) &= (ax_{n-1} + 5by_{n-1}, bx_{n-1} + ay_{n-1}) \text{ for } n \geqslant 1. \end{aligned}$$

Prove that each (x_n, y_n) is a solution of $x^2 - 5y^2 = 1$. (In particular, there are infinitely many solutions in positive integers of the *Pell equation* $x^2 - 5y^2 = 1$.) **(5)**

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