CS60082 Computational Number Theory

End-semester examination

Maximum marks: 100 April 29, 2008 (AN) **Duration:** 3 hours

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

1 Let n be an odd composite integer and $\gcd(a, n) = 1$. Prove the following assertions.

(a) If n is an Euler pseudoprime to base a, then n is a (Fermat) pseudoprime to base a. **(5)**

(b) There exists a base to which n is not an Euler pseudoprime. **(15)**

(c) n is an Euler pseudoprime to at most half the bases in $\mathbb{Z}_n^*$. **(5)**

2 The *Lehmer sequence* with parameters a, b is defined as

$$\begin{aligned} \bar{U}_0 &= 0, \\ \bar{U}_1 &= 1, \\ \bar{U}_m &= \bar{U}_{m-1} - b\bar{U}_{m-2} \text{ if } m \geqslant 2 \text{ is even}, \\ \bar{U}_m &= a\bar{U}_{m-1} - b\bar{U}_{m-2} \text{ if } m \geqslant 3 \text{ is odd}. \end{aligned}$$

Let α, β be the roots of $x^2 - \sqrt{a}x + b$.

(a) Prove that $\bar{U}_m = \begin{cases} (\alpha^m - \beta^m)/(\alpha^2 - \beta^2) & \text{if } m \text{ is even}, \\ (\alpha^m - \beta^m)/(\alpha - \beta) & \text{if } m \text{ is odd}. \end{cases}$ **(10)**

(b) Let $\Delta = a - 4b$ and n a positive integer with $\gcd(n, 2a\Delta) = 1$. We call n is *Lehmer pseudoprime* with parameters a, b if $\bar{U}_{n-\left(\frac{a\Delta}{n}\right)} \equiv 0 \pmod{n}$. Prove that n is a Lehmer pseudoprime with parameters a, b if and only if n is a Lucas pseudoprime with parameters a, ab. **(10)**

3 Prove that for $m \geqslant 2$, the Fermat number $f_m = 2^{2^m} + 1$ is prime if and only if $5^{(f_m-1)/2} \equiv -1 \pmod{f_m}$. **(10)**

4 (a) Suppose you are given a black-box that, given two positive integers n and k, returns in one unit of time the decision whether n has a factor d in the range $2 \leqslant d \leqslant k$. Using this black-box, devise an algorithm to factor a positive integer n in polynomial (in $\log n$) time. **(10)**

(b) Deduce the running time of your algorithm. **(5)**

5 Write a pseudocode implementing Floyd's variant of Pollard's rho method with block gcd calculations. **(10)**

6 (a) Explain how sieving is carried out in connection with the multiple-polynomial quadratic sieve method, that is, for the general polynomial $T(c) = U + 2Vc + Wc^2$ with $V^2 - UW = n$. **(10)**

(b) Assume that the factor base consists of $L[1/2]$ primes and the sieving interval is of size $L[1]$. Deduce that the sieving process can be completed in $L[1]$ time. **(10)**

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