CS60082/CS60094 Computational Number Theory, Spring 2010–11

End-Semester Test

Maximum marks: 55 Date: April 2011 Duration: 3 hours

Roll no: ____________________ **Name:** ____

[*Write your answers in the question paper itself. Be brief and precise. Answer all questions.*]

1. Represent $\mathbb{F}_{27} = \mathbb{F}_{3^3}$ as $\mathbb{F}_3(\theta)$, where $\theta^3 + 2\theta + 1 = 0$. Let $\alpha = \theta^2 + 2$.

(a) Determine whether α is a primitive element of $\mathbb{F}_{27}$. **(5)**

(b) Determine whether α is a normal element of $\mathbb{F}_{27}$. **(5)**

2. Let s and t be bit lengths with $s > t$. Your task is to find a random s-bit prime p for which $p - 1$ has a prime divisor of bit length t.

(a) Describe an *efficient* algorithm to compute such a prime p. **(5)**

(b) Express the expected running time of your algorithm in terms of the bit lengths s and t. **(5)**

3. [*Pocklington primality test*] Let n be a positive odd integer whose primality is to be checked. Write $n - 1 = uv$, where the complete prime factorization of u is known, whereas v is composite with no known factors. (The case $v = 1$ is also allowed.) Suppose also that for some integer a, we have $a^{n-1} \equiv 1 \pmod{n}$, whereas $\gcd(a^{(n-1)/q} - 1, n) = 1$ for all prime divisors q of u.

(a) Prove that every prime factor p of n satisfies $p \equiv 1 \pmod{u}$. (**Hint:** First, show that $u \mid \operatorname{ord}_p(a)$.) **(5)**

(b) Conclude that if $u \geqslant \sqrt{n}$, then n is prime. **(5)**

(c) Describe a situation when the criterion of Part (b) leads to an efficient algorithm for determining the primality of n. (**Hint:** Let all prime factors of u be *small*.) **(5)**

4. Consider the subexponential expression

$$L_n(\omega, c) = \exp\left[c\,(\ln n)^{\omega}(\ln\ln n)^{1-\omega}\right]$$

for constants ω and c with $0 < \omega < 1$ and $c > 0$. Take $n \approx 2^{1024}$. Find the values of the expressions $n^{1/4}$, $L_n(1/2, 1)$ and $L_n(1/3, 2)$. What do these values tell about known integer-factoring algorithms? **(5)**

5. In the original QSM, we sieve around $\sqrt{n}$. Suppose we instead take $H = \left\lceil \sqrt{2n} \right\rceil$ and $J = H^2 - 2n$.

(a) Describe how we can modify the original QSM to work for these values of H and J. It suffices to describe how we get a relation in the modified QSM. There is no need to describe the sieving process or the linear-algebra phase, or to recommend optimal values for M (sieving limit) and t (size of the factor base). **(5)**

(b) Explain why the modified QSM is poorer than the original QSM. (**Hint:** Look at the approximate average value of $|T(c)|$.) **(5)**

(c) Despite the objection in Part (b) about the modified QSM, we can exploit it to our advantage. Suppose that we run two sieves: one around $\sqrt{n}$ (the original QSM), and the other around $\sqrt{2n}$ (the modified QSM), each on a sieving interval of length half of that for the original QSM. Justify why this reduction in the length of the sieving interval is acceptable. Discuss what we gain by using the dual sieve. **(5)**