CS60082/CS60094 Computational Number Theory

End-semester examination

Maximum marks: 100 April 23, 2009 (AN) **Duration:** 3 hours

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

1 Suppose we want to compute the smallest prime $p \geqslant n$, where n is a given positive integer. Assume that $n \gg 1$. The obvious strategy is to test the primality of $n, n+1, n+2, \ldots$ until a prime $n+k$ is found. During the search, it is natural to exclude the integers which are *obviously* not prime. For example, there is no need to check the primality of even integers, the multiples of 3, the multiples of 5, and so on. A sieve can be used to throw away multiples of small primes $p_1, p_2, \ldots, p_t$ and check the primality of only those integers of the form $n+i$ that do not have prime divisors $\leqslant p_t$. One takes t between 10 and 1000.

A prime p is called a *Sophie Germain prime* if $2p+1$ is also a prime. It is conjectured that there are infinitely many Sophie Germain primes. If p is a Sophie Germain prime, the prime $2p+1$ is called a *safe prime*. Safe primes are frequently used in cryptography.

In this exercise, you are asked to extend the above sieve for locating the smallest Sophie Germain prime $p \geqslant n$ for a given positive integer $n \gg 1$. Sieve over the interval $[n, n+M]$.

(a) Determine a value of M such that there is (at least) one Sophie Germain prime of the form $n+i$, $0 \leqslant i \leqslant M$, with high probability. The value of M should be as small as possible. **(5)**

(b) Describe a sieve to throw away the values of $n+i$ for which either $n+i$ or $2(n+i)+1$ has a prime divisor $\leqslant p_t$. Take t as a constant (like 100). **(10)**

(c) Describe the gain in the running time, that you achieve using the sieve. **(10)**

2 In Floyd's variant of Pollard's rho method for factoring the integer n, we compute the values of x_k and x_{2k} and then $\gcd(x_k - x_{2k}, n)$, for $k = 1, 2, 3, \ldots$. Suppose that we instead compute x_{rk+1} and x_{sk} and subsequently $\gcd(x_{rk+1} - x_{sk}, n)$, for $k = 1, 2, 3, \ldots$, where $r, s \in \mathbb{N}$.

(a) Deduce a condition relating r, s and the length l of the cycle such that this method is guaranteed to detect a cycle of length l. **(10)**

(b) Characterize all the pairs (r, s) such that this method is guaranteed to detect cycles of any length. **(5)**

3 Dixon's method for factoring an integer n can be combined with a sieve in order to reduce its running time to $L[3/2]$. Instead of choosing random values of $x_1, x_2, \ldots, x_s$ in the relations, we first choose a random value of x and, for $-M \leqslant c \leqslant M$, we check the smoothness of the integers $(x+c)^2 \pmod{n}$ over t small primes $p_1, p_2, \ldots, p_t$. As in Dixon's original method, take $t = L[1/2]$.

(a) Determine the value of M for which one expects to get a system of the desired size. **(5)**

(b) Describe a sieve over the interval $[-M, M]$ for detecting the smooth values of $(x+c)^2 \pmod{n}$. **(10)**

(c) Deduce how you achieve a running time of $L[3/2]$ using this sieve. **(10)**

4 (a) Let $h \in \mathbb{F}_q^*$ have order m (a divisor of $q-1$). Prove that for $a \in \mathbb{F}_q^*$, the discrete logarithm $\operatorname{ind}_h a$ exists if and only if $a^m = 1$. **(10)**

(b) Suppose that g and g' are two primitive elements of $\mathbb{F}_q^*$. Show that if one can compute discrete logarithms to the base g in $\mathrm{O}(f(\log q))$ time, then one can also compute discrete logarithms to the base g' in $\mathrm{O}(f(\log q))$ time. (You may assume that $f(\log q)$ is a super-polynomial expression in $\log q$.) **(10)**

5 Suppose that in the linear sieve method for computing discrete logarithms in $\mathbb{F}_p$, we obtain an $m \times n$ system of congruences, where $n = t + 2M + 2$ and $m = 2n$. Assume that the $T(c_1, c_2)$ values behave as random integers (within a bound). Calculate the expected number of non-zero entries in the $m \times n$ coefficient matrix. You may make use of the fact that, for a positive real number x, the sum of the reciprocals of the primes $\leqslant x$ is approximately $\ln \ln x + \mathcal{B}_1$, where $\mathcal{B}_1 = 0.2614972128\ldots$ is known as the *Mertens constant*. (Note that the expected number of non-zero entries is significantly smaller than the obvious upper bound $\mathrm{O}(m \log p)$.) **(15)**

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