Indian Institute of Technology Kharagpur

CS60094: Computational Number Theory, Spring 2023
End Semester Examination

25 APRIL 2023 | CSE 107, 2PM - 5PM | TOTAL MARKS = 100

Answer Question 1, two questions from Section I and two questions from Section II.
Note that *exactly five* questions must be answered.
Keep your answers clear and concise. State all assumptions you make.

---

1. Let $\alpha \in \mathbb{F}_{p^n}^*$ and $r = (p^n - 1)/(p-1) = 1 + p + p^2 + \cdots + p^{n-1}$.
   (a) Prove that $\alpha^r \in \mathbb{F}_p$.
   (b) Show how α^{-1} can be efficiently computed using the fact that $\alpha^{-1} = (\alpha^r)^{-1} \alpha^{r-1}$.

$\boxed{10+10 = 20}$

SECTION I

2. Let p, q be primes, $n = pq$, $a \in \mathbb{Z}_n^*$ and $d = \gcd(p-1, q-1)$.
   (a) Prove that n is a pseudoprime to base a if and only if $a^d \equiv 1 \pmod{n}$.
   (b) Prove that n is a pseudoprime to exactly d^2 bases in $\mathbb{Z}_n^*$.
   (c) To how many bases in $\mathbb{Z}_n^*$ is n a pseudoprime if $q = 2p - 1$?

$\boxed{8+6+6 = 20}$

3. Prove the following assertions.
   (a) Fermat's little theorem holds for all Carmichael numbers (i.e., if n is a Carmichael number, then $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}_n$).
   (b) An odd prime p is a strong pseudoprime in any base not divisible by p.
   (c) An odd composite integer n is not an Euler pseudoprime to at least half the bases in $\mathbb{Z}_n^*$.

$\boxed{5+5+10 = 20}$

4. Consider a primality testing algorithm $\mathcal{A}$ that takes as input an odd integer $n > 1$ and a positive integer parameter k, described as follows.

   $\mathcal{A}(n, k)$
   Choose $a_1, a_2, \ldots, a_k$ at random from $\mathbb{Z}_n^+$
   for $i \leftarrow 1, 2, \ldots, k$
   compute $b_i \leftarrow a_i^{(n-1)/2} \bmod n$
   if $b_i \neq \pm 1$, output "NO"
   if $b_i = 1$ for all $i = 1, 2, \ldots, k$, then output "NO"
   output "YES"

   Prove the following.
   (a) If n is prime, $\mathcal{A}$ outputs "NO" with probability at most 2^{-k}.
   (b) If n is composite, $\mathcal{A}$ outputs "YES" with probability at most 2^{-k}.

$\boxed{10+10 = 20}$

Section II

5. We say that a positive integer n can be written as the sum of two squares if $n = a^2 + b^2$ for some positive integers a, b.

   (a) Show that is two integers m, n can be written as sums of two squares, then mn can also be so written.

   (b) Prove that no $n \equiv 3 \pmod 4$ can be written as a sum of two squares.

   (c) Let a square-free composite integer n be a product of (distinct) primes each congruent to 1 modulo 4. Show that n can be written as a sum of 2 squares in at least 2 different ways.

   (d) Let n be as in Part (c) and we know that $n = a^2 + b^2 = c^2 + d^2$ with a, b, c, d being distinct. Describe how n can be factored easily.

   $\boxed{3+3+6+8 = 20}$

6. 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 $2 \le d \le k$. Using this black box, devise an algorithm to factor a positive integer n in polynomial (in $\log n$) time. Deduce the running time of your algorithm. $\boxed{20}$

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

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

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

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

   $\boxed{5+5+10 = 20}$