Number Theory for Computer Scientists 89-256
Question Sheet 4
Due May 31, 2011 // 27 Iyar 5771

(1) Use the Miller-Rabin primality test to show that $2^{32}+1$ is not prime.

(2) Let $n = 221$. How many elements $a \in (\mathbb{Z}/n\mathbb{Z})^{+} = \{1, 2, \ldots, 220\}$ are there such that the Miller-Rabin test would return an output of "yes" if a were chosen, although n is not prime? Does this contradict the bound we proved in class for the probability of error by this test?

(3) Here is another primality test. Let $n > 1$ be odd and let $k \geq 1$. Pick a random k-tuple $(a_1, \ldots, a_k)$, where the a_i are elements of $(\mathbb{Z}/n\mathbb{Z})^{+}$. For each $1 \leq i \leq k$, let $b_i = a_i^{(n-1)/2}$. If $(b_1, \ldots, b_k) = (\pm 1, \ldots, \pm 1)$, but $(b_1, \ldots, b_k) \neq (1, \ldots, 1)$, the test outputs "yes." Otherwise, it outputs "no."

Prove that this algorithm runs in polynomial time. Prove that if the input n is prime, then the algorithm will output "yes" with probability at least $1 - \frac{1}{2^k}$, and that if n is not prime, then it will output "no" with probability at least $1 - \frac{1}{2^k}$.

(4) Let p be prime. Prove that $n = 2p + 1$ is prime if and only if $2^{n-1} \equiv 1 \mod n$.

(5) Show that a number $n > 1$ is prime if and only if the group $(\mathbb{Z}/n\mathbb{Z})^{*}$ has an element of order $n - 1$.

(6) Recall that $\pi(x)$ is the number of primes not larger than x, recall the function $\theta(x) = \sum_{p \leq x} \ln p$. Prove that for all $0 < \delta < 1$ and for all $x > 2$ the following is true:

$$1 \leq \frac{\pi(x) \ln x}{\theta(x)} \leq \frac{x^{1-\delta} \ln x}{\theta(x)} + \frac{1}{1-\delta}.$$

Deduce that

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{\theta(x)}{\ln x}} = 1.$$

(7) For each natural number n, let $\sigma(n)$ be the sum of all the divisors of n. For example,

$$\begin{aligned} \sigma(18) &= 1 + 2 + 3 + 6 + 9 + 18 &= 39 \\ \sigma(28) &= 1 + 2 + 4 + 7 + 14 + 28 &= 56. \end{aligned}$$

Suppose that $n = pqr$ is a product of three distinct primes. Suppose that the three numbers n, $\varphi(n)$, and $\sigma(n)$ are known. Find a fast algorithm that factors n.

(8) Find all the Carmichael numbers of the form $7 \cdot 23 \cdot q$, where $q > 23$ is a prime number.