Prof. Friedrich Eisenbrand
Alfonso Cevallos and Yuri Faenza

Discussions from: March 18, 2014

Computer Algebra

Spring 2014

Assignment Sheet 3

Exercises marked with a $\star$ can be handed in for bonus points. Due date is April 01.

Exercise 1
Given a non-Carmichael number N, what is the running time needed to certify with the Fermat Test that N is prime with probability at least .99?

Exercise 2
Show that, if $a, p \in \mathbb{N}$ such that $a^p - 1$ is prime, then $a = 2$ or $p = 1$.

Exercise 3
Recall that an algorithm is said *polynomial time* if its running time is polynomial in the length of the input. A *proper factor* of an integer N is a number distinct from N that divides N. Show that a polynomial time algorithm for the following problem (P):

`INPUT: a pair of positive integers` $\ell \leq N$.
`OUTPUT: 'YES' if` N `has a proper factor greater than` ℓ `; 'NO' otherwise.`

implies the existence of a polynomial time algorithm for the following problem (F).

`INPUT: a number` N, `OUTPUT: a factorization of` N `in prime numbers.`

Exercise 4
Suppose you *know* the answer to a problem for a given input. How do you convince someone that you are right? This is captured by the following definitions. A *YES-instance* (resp. *NO-instance*) for (P) is a pair ℓ, N such that the answer to problem (P) with input ℓ, N is YES (resp. NO). We say that $S : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is a *YES-certificate* (resp. *NO-certificate*) for (P) if:

- $S(\ell, N)$ is of size polynomial in $\log(N)$;
- there exists a polynomial time algorithm that, given N, ℓ and $S(\ell, N)$ as an input, answers YES (resp. NO) if and only if ℓ, N is a YES- (resp. NO-) instance.

Give YES- and NO-certificates for the problem (P) from the previous exercise.

Exercise 5
Recall that in class we defined a Carmichael number as a number N such that $a^{N-1} \equiv 1 \mod N$ for each $a \in \mathbb{Z}_N^*$. Show that the following are equivalent definitions.

1. $a^N \equiv a \mod N$ for all $a \in \mathbb{Z}_n$.
2. N is composite, odd, each of its prime factors have multiplicity exactly one in its factorization and $p-1|N-1$ for all primes $p|N$.

Exercise 6
Let $N = \prod_{i=1}^{k} p_i$ be a Carmichael number, with $p_1, \ldots, p_k$ primes. What is the probability that the Fermat Test will answer "composite" when N is given as an input?

Exercise 7 ($\star$)

(a) Implement an algorithm that takes as input $N \in \mathbb{N}$, generates a random number with N bits, and uses the Miller-Rabin tests to certify with probability at least 0.999 that the random number is prime.

(b) Implement an algorithm that uses two prime numbers (obtained via (a)) to generate private and public keys for the RSA cryptosystem, and an algorithm that decodes a message coded through this scheme.

Exercise 8 ($\star$)
Show that, for each $x \in \mathbb{R}_+$, $\sum_{p \le x : p \text{ is a prime}} \frac{\log p}{p} = \log x + O(1)$. *Hint: First show* $\log(n!) = \sum_{p \le n} \lfloor n/p \rfloor \log p + O(n)$. *Then combine it with others results seen in class or at the exercise sessions.*

Exercise 9
Assuming $\pi(x) = \{p \le x : p \text{ is prime}\} \sim x/\log x$, show the following: for each $\epsilon > 0$, there exists $c \in \mathbb{R}_+$, $N \in \mathbb{N}$ such that, for each $n \ge N$, one has $\pi((1+\epsilon)n) - \pi(n) \ge c\frac{n}{\log n}$.

Exercise 10
Show that the following *Sieve of Eratosthenes* detects the primes smaller or equal to an input n (at the end of the routine, a number $t \in [2, n]$ is prime iff $A[t] = 1$). Assuming that for each $n \in \mathbb{N}$, $\sum_{p \le n : p \text{ is a prime}} \frac{1}{p} = \log(\log n) + O(1)$, show it has running time $O(n \log(\log n))$.

```
INPUT: integer n ∈ ℕ,   OUTPUT: vector A[2,...,n].

FOR k = 2 to n SET A[k] = 1
FOR k = 2 to ⌊n/2⌋
     IF A[k] = 1
          SET i = 2k
          WHILE i ≤ n
               SET A[i] = 0
               SET i = i + k
RETURN A[2,...,n]
```