Problem Set 2

CPSC 629 Analysis of Algorithms

Andreas Klappenecker

The assignment is due next Tuesday (10/01/2002), before class.

Q1 Show that an integer $p \geq 2$ is a prime if and only if

$$(p-1)! \equiv -1 \bmod p \tag{1}$$

holds. Hint: If p is prime, consider the pairs $x, x^{-1} \in \mathbf{F}_p^* = \mathbf{F}_p \setminus \{0\}$. When is $x^{-1} = x$? The case 'p is not a prime' is easy.

Q2 Dr. S. Mart suggests to use equation (1) to test whether or not p is a prime. He points out that $2^{(\log_2 2 + \log_2 3 + \cdots + \log_2 (p-1))}$ can be used to quickly calculate $(p-1)!$ S. Mart claims that this is much faster than the AKS primality test. Is he right? (Either desribe the flaw of his method or give a prove that he is right)

Let p be an odd prime. A number $a \in \mathbf{F}_p^*$ is a quadratic residue iff $x^2 \equiv a \bmod p$ has a solution for the unknown x. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue modulo p, and to be -1 otherwise.

Q3 Give a short proof that there are exactly $(p-1)/2$ quadratic residues modulo p.

Q4 Show that if $a \in \mathbf{F}_p^*$, then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p.$$

Give an efficient algorithm to determine whether or not a given number a is a quadratic residue modulo p. [Remark: This is useful in the Quadratic Sieve]

The next exercise shows how to find the square root of a quadratic residue. We only consider $p \equiv 3 \bmod 4$, since that is the easiest case.

Q5 Let p be an odd prime of the form $p = 4k + 3$. Show that a^{k+1} is a square root of a modulo p. Which algorithm in the textbook [CLRS] allows to calculate this square root in a fast way? How much time does this algorithm need if p has β bits?

Reading Assignment: Read Chapter 31 in [CLRS] Cormen, Leiserson, Rivest, Stein: Introduction to Algorithms, 2nd edition, MIT Press, 2001.