Homework I, Advanced algorithms, Spring 1995

This howework is due Tuesday March 28 at the beginning of the lecture.

1. Let a Carmichael number be a square free (i.e. for no prime p does p^2 divide N), composite number N such that for any prime p dividing N, $p-1$ divides $N-1$. These are numbers which are bad with respect to the converse of Fermat's little theorem. Prove that a Carmichael number cannot be the product of only two primes.

2. Prove that it is easy to factor Carmichael numbers, i.e. give a fast (possibly probabilistic) algorithm and analyze it. Remember that Carmichael numbers almost satisfy Fermat's little theorem, but fail the Miller-Rabin test.

3. (3p) In the proof of Miller-Rabin's primality test we needed the following lemmas

   Lemma 1 *Let p be a prime where $p-1 = 2^{r'}t'$ where t' is odd. Show that the*
   $$Pr[a^{2^r t} \equiv -1 \ mod \ p \mid a^{2^s t} \equiv 1 \ mod \ p]$$
   where t is odd is bounded by $\max(2^{r-r'}, 2^{r-s})$ when $r < \min(r', s)$ and 0 otherwise.

   Lemma 2 *Let p be a prime where $p-1 = 2^{r'}t'$ where t' is odd. Suppose $s < r'$ then the*
   $$Pr[a^{2^s t} \equiv 1 \ mod \ p]$$
   where t is odd is bounded by $2^{s-r'}$.

   Lemma 3 *Let p be a prime where $p-1 = 2^{r'}t'$ where t' is odd. Show that the*
   $$Pr[a^t \equiv 1 \ modp \mid a^{2^s t} \equiv 1 modp]$$
   where t is odd is bounded by $\max(2^{-r'}, 2^{-s})$.

   In my lecture I stated the bound incorrectly for Lemma 1 since I was assuming that $s \geq r'$. That the algorithm fails in this case is covered by Lemma 2. I apologize just the same. Your task is to prove lemmas. Remember that the multiplicative group mod p is isomorphic to the additive group mod $p-1$. In this isomorphism 1 corresponds to 0 and -1 to $(p-1)/2$. Squaring in the multiplicative setting corresponds to multiplication by 2 In the additive setting and you can then analyze what power of two divides the numbers in question.

4. Let f be a random mapping of $[0, p-1]$ to $[0, p-1]$, i.e. $f(x)$ is picked uniformly and independently for each x. Let $x_0 = 0$ and let $x_{i+1} = f(x_i)$. Let the return time be the first j such that $x_j = x_k$ for some $k < j$. Prove that the expected value of the return time is bounded by $O(\sqrt{p})$.

5. In Pollard's ρ-test it would have been more efficient to have $f(x) = ax + b$ rather than $f(x) = x^2 + 1$. However, this will not work and let us give an informal reason. Linear functions are one-to-one mod p (prove this). Now in the previous exercise assume that f is a random 1-1 function and estimate the expected return time.

6. (2p) It is well known that each prime p that satisfies $p \equiv 1 \ mod \ 4$ can be written as the sum of two squares. In particular $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$. The goal of this exercise is to find an algorithm to find this representation efficiently i.e. in time polynomial in $\log p$ (and possibly using randomness). We will work with the Gaussian

integers i.e. number on the form $a + ib$ where a and b are integers and i is the imaginary unit. The conjugate number to $X = a + bi$ is $\bar{X} = a - bi$ and a key concept is the norm of a number X which is defined $X\bar{X} = a^2 + b^2$. Your first task is:

Generalize the Euclidean algorithm to Gaussian integers and analyze the complexity of the resulting algorithm. The important step is that given Gaussian integers X and Y find a Gaussian integer Z such that $X = ZY + R$ where the norm of R is less than the norm of Y.

It follows that we have unique factorization of Gaussian integers. It turns out that if p is a prime such that $p \equiv 1 \ mod\ 4$ then p factors as $p = (a + bi)(a - bi)$ and this gives $p = a^2 + b^2$. Consider the following two steps.

1. Find $c + di$ such that p divides $c^2 + d^2$ but such that p does not divide c or d.

2. Compute $GCD(c + di, p)$.

Prove that this indeed finds a solution to our problem (at least give an argument to this effect). Describe how to implement the steps and analyze the complexity.

Hint: The first part can be achieved fast probabilistically with $d = 1$.