Heads and Tails, summer 2009

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

3. Exercise sheet
Hand in solutions until Sunday, 10 May 2009, 24:00h.

Exercise 3.1 (Fermat's test and Carmichael numbers). (12 points)

A *Fermat witness* is a number $a \in \mathbb{Z}_N^\times$ satisfying $a^{N-1} \neq 1$ in $\mathbb{Z}_N^\times$. During a Fermat test such a number proves that a number N is composite.

A *Carmichael number* is a composite number N satisfying $x^{N-1} = 1$ for all $x \in \mathbb{Z}_N^\times$. Carmichael number are exactly those numbers for which there exist no Fermat witnesses, although they are not prime. The Fermat test will always answer 'probably prime' for these numbers, in spite of the fact that they are composite.

The *(multiplicative) order* $\mathrm{ord}_N(x)$ *of* x *modulo* N is the smallest natural number e greater zero satisfying $x^e \equiv 1 \pmod{N}$. This is just the order of $x \bmod N$ in the group $\mathbb{Z}_N^\times$. Lagrange's theorem states that the order $\mathrm{ord}_N(x)$ of x modulo N is always a divisor of $\varphi(N)$, where φ denotes Euler's totient function.

(i) Let N and M be coprime. Let e be the order of x modulo N and f the order of x modulo M. Show: The least common multiple $\mathrm{lcm}(e, f)$ of e and f is the order of x modulo $N \cdot M$. Hint: CRT. [4]

(ii) Compute the (multiplicative) order of 3 modulo 100. [2]

(iii) Generalize (i) to allow for more coprime factors $N_1 \cdot \ldots \cdot N_r$ and compute the (multiplicative) order of 3 modulo 100100. [3]

(iv) Show that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number, i.e. for every number a coprime to 561 it holds that: $a^{560} \equiv 1 \pmod{561}$. [3]

Exercise 3.2 (Finding prime numbers). (5 points)

Find a 20 decimal digit prime. Explain how you obtained it and why you believe it is prime. (If you use a computer algebra system's `isprime` or similar, you need to explain its routine, why it works and why it convinces you ...) [5]

Exercise 3.3 (Selecting primes algorithmically uniformly at random). (8 points)

In this exercise we will explore how to select primes *in practice* uniformly at random from a finite set. As in the second exercise sheet we fix a bound $B \in \mathbb{N}$ and select a prime from the interval $[B+1, 2B]$ uniformly at random. To do so we employ a probabilistic algorithm IsPrime that tests the compositeness of m. In particular let us assume that the algorithm returns on composite numbers `"probably prime"` with probability at most $1/2$.

Consider now the following algorithm:

Algorithm.
Input: A positive integer $B \in \mathbb{N}$, a number of rounds $k \in \mathbb{N}$.
Output: An integer p from $[B+1, 2B]$.

1. Repeat 2–7
2. $\quad m \leftarrow_R [B+1, 2B]$
3. $\quad b \leftarrow$ `"probably prime"`
4. $\quad$ For i from 1 to k do 5–7
5. $\quad\quad$ If IsPrime$(m) =$ `"composite"` then
6. $\quad\quad\quad b \leftarrow$ `"composite"`
7. $\quad\quad\quad$ break
8. Until b = `"probably prime"`
9. $p \leftarrow m$
10. Return p

3 (i) We first analyze the k-fold iteration of the primality test. Assume that in any step the random choices made in the algorithm are independent from the previous ones. In particular the algorithm will answer `"probably prime"` if all k tests say so, otherwise it will output "`composite`". Proof that the k-fold iterated algorithm returns on composite numbers `"probably prime"` with probability at most $1/2^k$.

5 (ii) Show that the algorithm produces a prime with probability at least $1 - 2^{-k+1}$ and uses an expected number of $\mathcal{O}(k \log B)$ elementary operations. We assume here that one run of the procedure IsPrime(m) runs in $\mathcal{O}(1)$ elementary operations (which is of course wrong in practice). Hint: Consider two events C and T, where the former means that the chosen random number is composite and the latter that the k-round test answers "`probably prime`". Now work with conditional probabilities.

Exercise 3.4 (Playing fair). (4 points)

4 Suppose you are given a coin for which the probability of Heads, say p, is unknown. If $p \neq 1/2$ we call the coin *biased*. How can you use this coin to generate unbiased (prob(Heads) = prob(Tails) $= 1/2$) coin flips? Giva a scheme for which the expected number of flips of the biased coin for extraction one unbiased coin-flip is no more than $\frac{1}{p(1-p)}$. Hint: Consider two consecutive flips of the biased coin.