Heads and Tails, summer 2009

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

2. Exercise sheet
Hand in solutions until Sunday, 03 May 2009, 24:00h.

Exercise 2.1 (Selecting primes uniformly at random). (8+1 points)

In this exercise we will explore how to select primes uniformly at random from a finite set. For example one can fix a bound $B \in \mathbb{N}$ and select a prime from the interval $[B+1, 2B]$ uniformly at random. There is a famous theorem, called Bertrand's postulate, which says that one can be sure that for any B the number ℓ of primes in $[B+1, 2B]$ is non-zero. Consider now the following algorithm:

Algorithm.
Input: A positive integer $B \in \mathbb{N}$.
Output: A prime p from $[B+1, 2B]$.

1. Repeat
2. $\quad m \leftarrow_R [B+1, 2B]$
3. Until m prime
4. $p \leftarrow m$
5. Return p

Of course the question of deciding whether m is prime or not needs some further attention. For the beginning, let us assume that we are able to decide that problem in a non-probabilistic fashion efficiently. We will come back to that problem later.

(i) Analyze the runtime of the above algorithm, i.e. give an estimate on the expected number of loops of the procedure. Hint: You may use here that $\ell \geq \frac{B}{2 \ln B}$ whenever $B \geq 6$. [3] [+1]

(ii) Show that the above algorithm produces every prime from $[B+1, 2B]$ with the same probability. Hint: Consider the event that the algorithm returns a specific prime after k rounds and sum over all k. [5]

Exercise 2.2 (Fingerprinting huge databases). (5 points)

In the lecture we have seen that one can easily check if two huge databases are synchronized if one considers the two databases as a positive integers $n_1, n_2 \in \mathbb{N}_{<C}$ for some bound $C \in \mathbb{N}$, selects an appropriate prime p uniformly at random from $[B+1, 2B]$ and simply checks if $n_1 \equiv n_2 \pmod{p}$. This exercise will have a closer look on that problem. For the analysis we consider the related problem of checking if $n \equiv 0 \pmod{p}$.

(i) Show that for every $n < C$ we have [2]

$$\text{prob}(n \bmod p = 0 \colon p \in [B+1, 2B]) \leq \frac{\log_B C}{\ell},$$

where ℓ denotes the number of primes in $[B+1, 2B]$.

(ii) Compute a lower bound on B such that for *all* $n < C$ the algorithm decides $n \equiv 0 \pmod{p}$ with error probability at most $\varepsilon \in \mathbb{R}_{>0}$ when p is selected uniformly at random from $[B+1, 2B]$. 3

Exercise 2.3 (Independence of events). (4 points)

4 In the course we have seen that if you roll a fair die, the two events $A := \{1 \leq n \leq 6 \colon n \bmod 2 = 1\}$ and $B := \{1 \leq n \leq 6 \colon n \bmod 3 = 0\}$ are statistically independent. We will explore here that phenomenon in more detail. To do so we use the following fact:

Fact (Chinese remainder theorem, simplified). *Let $m_1, m_2 \in \mathbb{N}$ be two coprime integers, i.e. $\gcd(m_1, m_2) = 1$ and $a, b \in \mathbb{N}$. Then there is an integer c such that $c \equiv a \pmod{m_1}$ and $c \equiv b \pmod{m_2}$. Moreover, c is uniquely determined modulo $m_1 m_2$.*

Suppose we have a two coprime integers $m_1, m_2 \in \mathbb{N}$ and $a, b \in \mathbb{N}$. Consider a random variable X on the ring $\mathbb{Z}_{m_1 m_2}$. Show that the two events $X \in A := \{c \in \mathbb{Z}_{m_1 m_2} \colon c \equiv a \pmod{m_1}\}$ and $X \in B := \{c \in \mathbb{Z}_{m_1 m_2} \colon c \equiv b \pmod{m_2}\}$ are statistically independent.

Exercise 2.4 (The group of units modulo N). (6+4 points)

Let $N \in \mathbb{N}$ be an arbitrary positive integer. Goal of this exercise is to understand how many elements in $\mathbb{Z}_N$ are coprime to N, that is to count the elements in the set

$$\mathbb{Z}_N^\times := \{a \in \mathbb{Z}_n \colon \gcd(a, N) = 1\}.$$

We write $\varphi(N) := \#\mathbb{Z}_N^\times$ for the count.

2 (i) Compute $\varphi(5)$, $\varphi(8)$, $\varphi(10)$ and $\varphi(16)$.

1 (ii) Assume that N is prime. Show that in this case $\varphi(N) = N - 1$.

3 (iii) Now consider the case that N is a prime power, i.e. that $N = p^e$ for some prime p and $e \in \mathbb{N}$. Show that we have now $\varphi(N) = (p-1)p^{e-1}$.

+4 (iv) Derive from the fact in Exercise 2.3 that for all coprime $m_1, m_2 \in \mathbb{N}$ we have $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$. Conclude that if $N = \prod_{p|N} p^{e(p)}$ then $\varphi(N) = \prod_{p|N}(p-1)p^{e(p)-1}$.

Exercise 2.5 (Fermat). (5 points)

5 Let p be a prime. Prove Fermat's little theorem, ie. for all $a \in \mathbb{Z}_p^\times$ we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Hint: Consider the two lists $1, 2, \ldots, p-1$ and $a, 2a, \ldots, (p-1)a$ and show that one is a permutation of the other. Now look at the two products $\prod_{1 \leq i < p} i$ and $\prod_{1 \leq i < p} i \cdot a$.