Heads and Tails, summer 2009

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

10. Exercise sheet
Hand in solutions until Sunday, 05 July 2009, 24:00h.

Exercise 10.1 (Designs). (5 points)

Let p be a prime number. As usual, let $\mathbb{F}_p$ be the field with p elements. Consider:

- $S = \mathbb{F}_p^2$,
- $\forall a, b \in \mathbb{F}_p \colon S_{a,b} = \{(x, ax + b) \colon x \in \mathbb{F}_p\} \subseteq S$,
- $D' = \{S_{a,b} \colon a, b \in \mathbb{F}_p\}$.

(i) Arrange the elements of D' into a sequence D. [2]

(ii) Determine the uniquely determined values $k, n, s \in \mathbb{N}$ and the *smallest possible* value $t \in \mathbb{N}$ such that D is a (k, n, s, t)-design. [3]

Exercise 10.2 (Squaring mod p). (11 points)

In this exercise we are going to investigate the set of squares mod p, where p is some prime. As usual, we denote by $\mathbb{Z}_p^\times$ the group of all such invertible elements with multiplication mod p. Additionally define the *order* of $a \in \mathbb{Z}_p^\times$, in symbols $\operatorname{ord}(a)$ to be the smallest nonnegative integer e such that $a^e = 1$ in $\mathbb{Z}_p^\times$. Now consider the set

$$S := \{b^2 \bmod p \colon b \in \mathbb{Z}_p\}.$$

Show the following properties:

(i) S is a subgroup of $\mathbb{Z}_p^\times$ of size $(p-1)/2$, in other words the probability that a randomly selected element from $\mathbb{Z}_p^\times$ is a square mod p with probability $1/2$. Hint: There is an element $g \in \mathbb{Z}_p^\times$, such that every element $a \in \mathbb{Z}_p^\times$ can be written as g^α for some positive integer α. Additionally you may use the fact that $\operatorname{ord} a^k = \frac{\operatorname{ord} a}{\gcd(p-1,k)}$ for every positive integer k. [4]

(ii) $S = \{b \in \mathbb{Z}_q^\times \colon b^{(q-1)/2} = 1\}$. [4]

(iii) $b^{(q-1)/2} \in \{1, -1\}$ for all $b \in \mathbb{Z}_q^\times$. [3]

Exercise 10.3 (Foundations: quadratic residues). (15 points)

The BLUM-BLUM-SHUB generator uses squaring modulo a BLUM number N to generate random bits. A BLUM *number* N is the product $p \cdot q$ of two odd primes p, q, both of which are congruent to $3 \bmod 4$.

To understand this we need some information about quadratic residues. What are the quadratic residues modulo N? The Jacobi symbol and the law of quadratic reciprocity are helpful:

Definition and Theorem. *The* Jacobi symbol $\left(\frac{a}{b}\right)$ *maps an integer number a and an odd natural number b to -1, 0 or $+1$. If $b = p$ is prime, the Jacobi symbol is also called Legendre symbol and it is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \gcd(a,p) \neq 1, \\ +1, & a \text{ is a square modulo } p \text{, i.e. } x^2 \equiv a \pmod{p} \text{ is solvable, } \gcd(a,p) = 1, \\ -1, & \text{otherwise.} \end{cases}$$

If $b = p_1^{e_1} \dots p_r^{e_r}$ is the prime factorization, let

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}.$$

It holds that:

(i) $\left(\frac{a}{b}\right) = \left(\frac{a \operatorname{rem} b}{b}\right)$. $\left(\frac{a}{b}\right) = 0$ *if and only if* $\gcd(a,b) \neq 1$.

(ii) $\left(\frac{1}{b}\right) = +1$, $\left(\frac{a'a}{b}\right) = \left(\frac{a'}{b}\right) \cdot \left(\frac{a}{b}\right)$, $\left(\frac{a}{b'b}\right) = \left(\frac{a}{b'}\right) \cdot \left(\frac{a}{b}\right)$.

(iii) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$. *This is $+1$ for $b \equiv 1 \pmod 4$ and -1 for $b \equiv -1 \pmod 4$.*

(iv) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$. *This is $+1$ for $b \equiv \pm 1 \pmod 8$ and -1 for $b \equiv \pm 3 \pmod 8$.*

(v) The law of quadratic reciprocity *states that, if a is also an odd natural number, then:*

$$\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} \left(\frac{b}{a}\right).$$

Thus the two Jacobi symbols differ in sign if and only if $a \equiv -1 \pmod 4$ and $b \equiv -1 \pmod 4$. □

[10] (i) Develop an algorithm for computing the Jacobi symbol using polynomial time and implement it in a programming language of your choice. [Hint: It can be done in $O(n^2)$. The standard Euclidean algorithm uses time $O(n^2)$.]

[2] (ii) Which numbers have $\left(\frac{a}{N}\right) = 1$? Compare with the two properties 'a is a square modulo p' and 'a is a square modulo q'.

Note: A number a with $\left(\frac{a}{N}\right) = +1$ that is not a square is sometimes called a *pseudosquare modulo N*.

[3] (iii) If $\left(\frac{x}{N}\right) = 1$, then either x is a square and $-x$ is a pseudosquare modulo N or vice versa. [Consider $\left(\frac{-1}{N}\right)$, $\left(\frac{-1}{p}\right)$, $\left(\frac{-1}{q}\right)$.]