The art of cryptography: security, reductions, and group cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, KONSTANTIN ZIEGLER

4. Assignment

(Due: Thursday, 3 May 2012, 13^{00})

Exercise 4.1 (Squares modulo primes)**.** We are investigating the set of squares mod p, where p is some odd prime. As usual, we denote by $\mathbb{Z}_p^\times$ the group of all 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 positive integer e such that $a^e = 1$ in $\mathbb{Z}_p^\times$.

$$\square_p = \{b^2 \colon b \in \mathbb{Z}_p\}$$

and show the following properties.

(i) (4 points) The set $\square_p$ is a subgroup of $\mathbb{Z}_p^\times$ of size $(p-1)/2$.

[Hint 1: The group $\mathbb{Z}_p^\times$ is cyclic, that is 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.

Hint 2: You may use the fact that $\operatorname{ord} a^k = (\operatorname{ord} a)/\gcd(p-1, k)$ for every positive integer k.]

(ii) (4 points) We have $\square_p = \{b \in \mathbb{Z}_p^\times \colon b^{(p-1)/2} = 1\}$.

(iii) (3 points) For all $b \in \mathbb{Z}_p^\times$, we have $b^{(p-1)/2} \in \{1, -1\}$.

Exercise 4.2 (Squares modulo composites)**.** Let $p, q \in \mathbb{N}$ be two different odd prime numbers and $N = p \cdot q$.

(i) (4 points) Prove that $a \in \mathbb{Z}_N^\times$ is square if and only if a is square in $\mathbb{Z}_p^\times$ and $\mathbb{Z}_q^\times$. How many squares are there in $\mathbb{Z}_N^\times$?

(ii) (4 points) Given square roots of $a \in \mathbb{Z}_N^\times$ in $\mathbb{Z}_p^\times$ and $\mathbb{Z}_q^\times$, show how to compute a square root of a in $\mathbb{Z}_N^\times$.

(iii) (3 points) Let $p = 3$, $q = 11$, and $a = 31$ with square root 1 in $\mathbb{Z}_3$ and square root 8 in $\mathbb{Z}_{11}$. Implement (ii).

Exercise 4.3 (Foundations: quadratic residues)**.** The BLUM-BLUM-SHUB generator uses squaring modulo a BLUM integer N to generate random bits. A BLUM *integer* N is the product $p \cdot q$ of two odd primes p, q, both of which are congruent to 3 mod 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.

Theorem 4.4. *Properties of the Jacobi symbol The* Jacobi symbol $\left(\frac{a}{b}\right)$ *maps an integer 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*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } \gcd(a, p) = 0, \\ +1, & \text{if } a \text{ is a square modulo } p, \\ -1, & \text{otherwise.} \end{cases}$$

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) $\left(\frac{a}{b}\right) = \left(\frac{a \bmod b}{b}\right)$. $\left(\frac{a}{b}\right) = 0$ *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 $b \equiv -1 \pmod 4$. □

We can now quickly compute

$$\left(\frac{5}{17}\right) = (-1)^{2\cdot 8}\left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = (-1)^3 = -1$$

by (i), (iv), and (v).

(i) (4 points) Compute $\left(\frac{1001}{9907}\right)$. Indicate which rule you applied in each step.

(ii) (+6 points) 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 Euclidean algorithm uses time $O(n^2)$.]

(iii) (2 points) 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".

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