Exercise sheet 2

Quadratic residues

Exercice 1 (Some applications of the quadratic reciprocity law).
Let p be a prime number.

(1) Compute Legendre's symbol $(\frac{754}{7})$.

(2) Compute Jacobi's symbol $(\frac{254}{1003})$.

(3) Assume p is different from 2 and 3. Show that 3 is a square in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod{12}$.

(4) Show that a quadratic residue modulo p is not a generator of $\mathbb{F}_p^*$.

(5) Let $a \in \mathbb{Z}$. Show that if $(\frac{a}{n}) = -1$, then a is not a square modulo n. Does the converse holds true ?

(6) Assume that p is different from 5. Find a necessary and sufficient condition on the last digit of p for 5 to be a square in $\mathbb{F}_p$.

Exercice 2. Let p be an odd prime and let n be the smallest natural integer that is not a square modulo p. Show that $n < 1 + \sqrt{p}$.

Exercice 3 (Squares in $\mathbb{Z}/p^r\mathbb{Z}$). Let p be an odd prime and let $r \in \mathbb{N}^*$.

(1) Let a be an integer coprime with p. Show that if a is a quadratic residue modulo p^r, then it is so modulo p^{2r}.

(2) Let a be an integer coprime with p. Show that the number of square roots of a modulo p^r is $1 + \left(\frac{a}{p}\right)$.

(3) Let a be an odd integer. For $r \geqslant 3$, show that the number of square roots of a modulo 2^r is 4 when $a \equiv 1 \mod 8$ and 0 otherwise. What is it for $r < 3$?

(4) Let n and a be two coprime integers. From the previous questions, deduce a necessary and sufficient condition for a to be a square modulo n. Give a formula for the number of square roots of a modulo n.

Exercice 4 (Computation of a square root in $\mathbb{F}_p$). Let p be an odd prime and let a be a nonzero square modulo p. Our goal is to compute the square roots of a in $\mathbb{F}_p$.

(1) Prove that a admits exactly 2 square roots modulo p.

(2) Show that if there exists an odd integer k such that $a^k \equiv 1 \mod p$, then the square roots of a are $\pm a^{\frac{k+1}{2}}$.

(3) What are the square roots of a for $p \equiv 3 \mod 4$?

For now on, assume that $p \equiv 1 \mod 4$. Write $p = 1 + 2^e s$ with s odd and $e \geqslant 2$.

(4) Prove that if there exists c such that $c^2 a^s \equiv 1 \mod p$, then the square roots of a are $\pm c a^{\frac{s+1}{2}}$.

The next step is to prove the existence of such an element c. Consider the 2-primary part G of $\mathbb{F}_p^*$, that is the subgroup of elements whose order is a power of 2. In particular, G is a cyclic group of order 2^e. Let z be a generator of G.

(5) Show that $a^s \in G$ and a^s is a square in G. Deduce an expression of the square roots of a. We now look for an algorithm to produce an element c such that $c^2 a^s \equiv 1 \mod p$. Let u be an integer that is *not* a square modulo p. Let ℓ be the smallest nonnegative integer such that $(a^s)^{2^\ell} = 1 \mod p$ and assume that $\ell \geqslant 1$. Define $v_1 = (u^s)^{2^{e-\ell-1}}$ and let similarly ℓ_1 be the smallest nonnegative integer such that $(v^2 a^s)^{2^{\ell_1}} = 1$.

(6) Show that $\ell_1 < \ell$. What can we say when $\ell_1 = 0$?

(7) For $\ell_1 \neq 0$, find an element v_2 such that $((v_2 v_1)^2 a^s)^{2^{\ell_1 - 1}} \equiv 1 \mod p$.

(8) More generally, give an algorithm that outputs an element c satisfying $c^2 a^s \equiv 1 \mod p$.

(9) Use the above method to determine the square roots of 5 in $\mathbb{Z}/41\mathbb{Z}$.

Some algorithms

Exercice 5. (1) Write the extend Euclid's algorithm and prove that it indeed outputs a Bézout relation.

(2) Consider the Fibonacci sequence given by $F_0 = 0, F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$. Let a and b be integers such that $a \geqslant b > 0$. Let n denote the number of steps in Euclid's algorithm on inputs (a, b). In other words, if we write $(r_m)_{m \in \mathbb{N}}$ for the sequence of rests in the division, with $r_0 = a$ and $r_1 = b$, then r_n is the last nonzero rest. Prove that

$$a \geqslant (a \wedge b) F_{n+2} \qquad \text{et} \qquad b \geqslant (a \wedge b) F_{n+1}.$$

(3) Using that $F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n + \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$, give a bound on the number n of steps of the algorithm in terms of the inputs a and b. Is this bound optimal ?

(4) Assuming that the cost of elementary operations is linear in the length of the inputs, give the complexity of the extended Euclid's algorithm.

Exercice 6. Implement the algorithms of decomposition of a rational number into a sum of Egyptian fractions discussed in exercise sheet 1.

Exercice 7. Write and implement an algorithm computing Jacobi's symbol $\left(\frac{a}{n}\right)$, for $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ odd, without using the decomposition into prime factors. What is the complexity of this algorithm ?