modulo p, we can extract square roots mod p in polynomial time (bounded by the fourth power of the number of bits in p).

3. Strictly speaking, it is not known (unless one assumes the validity of the so-called "Riemann Hypothesis") whether there is an algorithm for finding a nonresidue modulo p in polynomial time. However, given any $\epsilon > 0$ there is a polynomial time algorithm that finds a nonresidue with probability greater than $1-\epsilon$. Namely, a randomly chosen number n, $0 < n < p$, has a 50% chance of being a nonresidue, and this can be checked in polynomial time (see Exercise 17 below). If we do this for more than $log_2(1/\epsilon)$ different randomly chosen n, then with probability $> 1-\epsilon$ at least one of them will be a nonresidue.

Exercises

1. Make a table showing all quadratic residues and nonresidues modulo p for $p = 3,\ 5,\ 7,\ 13,\ 17,\ 19$.
2. Suppose that $p|2^{2^k}+1$, where $k > 1$.
(a) Use Exercise 4 of § I.4 to prove that $p \equiv 1 \ mod\ 2^{k+1}$.
(b) Use Proposition II.2.4 to prove that $p \equiv 1 \ mod\ 2^{k+2}$.
(c) Use part (b) to prove that $2^{16}+1$ is prime.
3. How many 84-th roots of 1 are there in the field of 11^3 elements?
4. Prove that $(\frac{-2}{p}) = 1$ if $p \equiv 1$ or $3\ mod\ 8$, and $(\frac{-2}{p}) = -1$ if $p \equiv 5$ or $7\ mod\ 8$.
5. Find $(\frac{91}{167})$ using quadratic reciprocity.
6. Find the Gauss sum $G = \sum_{j=1}^{q-1}(\frac{j}{q})\xi^j$ (here ξ is a q-th root of 1 in $\mathbf{F}_{p^f}$, where $p^f \equiv 1\ mod\ q$) when:
(a) $q = 7,\ p = 29,\ f = 1,\ \xi = 7$;
(b) $q = 5,\ p = 19,\ f = 2,\ \xi = 2-4i$, where i is a root of X^2+1;
(c) $q = 7,\ p = 13,\ f = 2,\ \xi = 4+\alpha$, where α is a root of X^2-2.
7. Let $m = a^4+1$, $a \geq 2$. Find a positive integer x between 0 and $m/2$ such that $x^2 \equiv 2\ mod\ m$. Use this to find $\sqrt{2}$ in $\mathbf{F}_p$ when p is each of the following: the Fermat primes 17, 257, 65537; $p = 41 = (3^4+1)/2$, $p = 1297$, and $p = 1201$. (Hint: see the proof of Proposition II.2.4.)
8. Let p and q be two primes with $q \equiv 1\ mod\, p$. Let ξ be a primitive p-th root of unity in $\mathbf{F}_q$. Find a formula in terms of ξ for a square root of $(\frac{-1}{p})p$ in $\mathbf{F}_q$.
9. (a) Let $m = a^p - 1$, where p is an odd prime and $a \geq 2$. Find a positive integer x between 0 and $m/2$ such that $x^2 \equiv (\frac{-1}{p})p\ mod\ m$. Use this to find $\sqrt{5}$ in $\mathbf{F}_{31}$, $\sqrt{-7}$ in $\mathbf{F}_{127}$, $\sqrt{13}$ in $\mathbf{F}_{8191}$, and $\sqrt{-7}$ in $\mathbf{F}_{1093}$.
(b) If $q = 2^p-1$ is a Mersenne prime, find an expression for the least positive integer whose square is $\equiv (\frac{-1}{p})p\ mod\ q$.
10. Evaluate the Legendre symbol $(\frac{1801}{8191})$ (a) using the reciprocity law only for the Legendre symbol (i.e., factoring all numbers that arise), and (b)