

without factoring any odd integers, instead using the reciprocity law for the Jacobi symbol.

11. Evaluate the following Legendre symbols:
 - (a) $(\frac{11}{37})$; (b) $(\frac{19}{31})$; (c) $(\frac{97}{101})$; (d) $(\frac{31}{167})$; (e) $(\frac{5}{160465489})$; (f) $(\frac{3083}{3911})$;
 - (g) $(\frac{43691}{65537})$.
12. (a) Let p be an odd prime. Prove that -3 is a residue in \mathbf{F}_p if and only if $p \equiv 1 \pmod{3}$.
 (b) Prove that 3 is a quadratic nonresidue modulo any Mersenne prime greater than 3 .
13. Find a condition on the last decimal digit of p which is equivalent to 5 being a square in \mathbf{F}_p .
14. Prove that a quadratic residue can never be a generator of \mathbf{F}_p^* .
15. Let p be a Fermat prime.
 - (a) Show that any quadratic nonresidue is a generator of \mathbf{F}_p^* .
 - (b) Show that 5 is a generator of \mathbf{F}_p^* , except in the case $p = 5$.
 - (c) Show that 7 is a generator of \mathbf{F}_p^* , except in the case $p = 3$.
16. Let p be a Mersenne prime, let $q = p^2$, and let i be a root of $X^2 + 1 = 0$, so that $\mathbf{F}_q = \mathbf{F}_p(i)$.
 - (a) Suppose that the integer $a^2 + b^2$ is a generator of \mathbf{F}_p^* . Prove that $a + bi$ is a generator of \mathbf{F}_q^* .
 - (b) Show that either $4 + i$ or $3 + 2i$ will serve as a generator of $\mathbf{F}_{3^{12}}^*$.
17. Let p be an odd prime and a be an integer between 1 and $p - 1$. Estimate in terms of p the number of bit operations needed to compute $(\frac{a}{p})$ (a) using the reciprocity law for the Jacobi symbol, and (b) using Proposition II.2.2 and Proposition I.3.6.
18. (a) Let p be an odd prime, and let a, b, c be integers with $p \nmid a$. Prove that the number of solutions $x \in \{0, 1, 2, \dots, p - 1\}$ to the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is given by the formula $1 + (\frac{D}{p})$, where $D = b^2 - 4ac$ is the discriminant.
 (b) How many solutions in \mathbf{F}_{83} are there to each of the following equations: (i) $x^2 + 1 = 0$; (ii) $x^2 + x + 1 = 0$; (iii) $x^2 + 21x - 11 = 0$; (iv) $x^2 + x + 21 = 0$; (v) $x^2 - 4x - 13 = 0$?
 (c) How many solutions in \mathbf{F}_{97} are there to each of the equations in part (b)?
19. Let $p = 2081$, and let n be the smallest positive nonresidue modulo p . Find n , and use the method in the text to find a square root of 302 modulo p .
20. Let $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be an odd integer, and suppose that a is prime to m and is the square of some integer modulo m . Your object is to find x such that $x^2 \equiv a \pmod{m}$. Suppose that for each j you know a nonresidue modulo p_j , i.e., an integer n_j such that $(\frac{n_j}{p_j}) = -1$.
 - (a) For each fixed $p = p_j$ and $\alpha = \alpha_j$, suppose you use the algorithm in the text to find some x_0 such that $x_0^2 \equiv a \pmod{p}$. Show how you can then find some $x = x_0 + x_1p + \cdots + x_{\alpha-1}p^{\alpha-1}$ such that $x^2 \equiv a \pmod{p^\alpha}$.