(b) Describe how to find an x such that $x^2 \equiv a \bmod m$.
The technique in parts (a)–(b) of this exercise is known as "lifting" a square root from $\mathbf{F}_{p_j}$ $(1 \le j \le r)$ to $\mathbf{Z}/m\mathbf{Z}$.

21. In the text we saw that if n is an odd prime and $g.c.d.(b,n) = 1$, then

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \bmod n. \qquad (*)$$

The purpose of this exercise is to show that, if n is an odd composite integer, then the relation $(*)$ is false for at least 50% of all b for which $g.c.d.(b,n) = 1$.
(a) Prove that if $(*)$ is true for b_1 and is false for b_2, then it is false for the product $b_1 b_2$. Use this to prove that if $(*)$ is false for even a single b, then the number of b's for which it is false is at least as great as the number of b's for which it is true.
(b) If n is divisible by the square of a prime p, show how to find an integer b prime to n such that $b^{(n-1)/2}$ is not $\equiv \pm 1 \bmod n$.
(c) If n is a product of distinct primes, if p is one of those primes, and if b has the property that $(\frac{b}{p}) = -1$ and $b \equiv 1 \bmod n/p$, prove that $(*)$ fails for b. Then show that such a b always exists.

22. Explain why the following probabilistic algorithm gives a square root of a modulo p: Choose t in $\mathbf{F}_p$ at random until you find t such that $t^2 - a$ is a *non*square modulo p. Let α denote the element $\sqrt{t^2 - a}$ in the quadratic extension $\mathbf{F}_{p^2}$. Then compute $b = (t + \alpha)^{(p+1)/2}$. Show that b is in $\mathbf{F}_p$ and has the property that $b^2 = a$.

23. Suppose that p is a prime $\equiv 1 \bmod 4$, and suppose you have found a quadratic nonresidue n. Describe an algorithm for expressing p as a sum of two squares $p = c^2 + d^2$ that takes time $O(log^3 p)$.

References for Chapter II

1. L. Adleman, K. Manders, and G. Miller, "On taking roots in finite fields," *Proc. 20th Annual Symposium on the Foundations of Computer Science* (1979), 175–178.
2. E. R. Berlekamp, "Factoring polynomials over large finite fields," *Math. Comp.*, **24** (1970), 713–735.
3. I. Blake, X. Gao, A. Menezes, R. Mullen, S. Vanstone, and T. Yaghoobian, *Applications of Finite Fields*, Kluwer Acad. Publ., 1992.
4. C. F. Gauss, *Disquisitiones Arithmeticae*, Yale Univ. Press, 1966.
5. E. Grosswald, *Topics from the Theory of Numbers*, 2nd ed., Birkhäuser, 1984.
6. I. N. Herstein, *Topics in Algebra*, 2nd ed., Wiley, 1975.
7. K. Ireland and M. I. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer–Verlag, 1990.