

Pries: 676 Number Theory. Homework 2.

Quadratic Reciprocity.

Here p is always prime. Let (a/p) denote the Legendre symbol.

Applications: Problems 1 and 5 give examples of primality tests. Problems 2 and 3 show how to find a solution to $x^2 \equiv a \pmod{p}$ in special cases.

1. Compute $11^{864} \pmod{1729}$. Hint: this is fast with successive squares $11, 11^2, 11^4, \dots$ and the binary expansion of 864. Compute $(11/1729)$ using quadratic reciprocity. What can you conclude about 1729?
2. Suppose that $(a/p) = 1$ and $p \equiv 5 \pmod{8}$. Show that either $x = a^{(p+3)/8}$ or $x = 2a(4a)^{(p-5)/8}$ is a solution of the congruence $x^2 \equiv a \pmod{p}$.
3. Use Wilson's Theorem and the congruence $k(p-k) \equiv -k^2 \pmod{p}$ to find a solution to $x^2 = -1$ when $p \equiv 1 \pmod{4}$.
4. Suppose $p \equiv 3 \pmod{8}$ and that $q = (p-1)/2$ is also prime. Show that 2 is a primitive root mod p .
5. Suppose $p \equiv 3 \pmod{4}$ and that $q = 2p+1$ is also prime. Prove that $2^p - 1$ is not prime.
6. Use quadratic reciprocity to find the primes for which 7 is a quadratic residue.
7. If $x^3 = 1$ and $x \neq 1$, show that $(2x+1)^2 = -3$. Use the fact that $(\mathbb{Z}/p)^*$ is cyclic to give a direct proof that $(-3/p) = 1$ when $p \equiv 1 \pmod{3}$.
8. Let $\omega = e^{2\pi i/3}$. Determine $(-3/p)$ using the Gauss sum method of Ireland/Rosen 6.2 with the equation from Exercise 7.
9. Prove there exist infinitely many primes $p \equiv 7 \pmod{12}$.
10. Show that $f_p \equiv (p/5) \pmod{p}$ (for $p \neq 2, 5$). Here f_p is the p th Fibonacci number. Hint: Use the closed form formula for f_p .