

Problem Set 4

Due Monday June 20.

1. Let p be a prime satisfying $p \equiv 3 \pmod{4}$ and suppose that a is a quadratic residue mod p .
 - (a) Show that $x = a^{(p+1)/4}$ is a solution to $x^2 \equiv a \pmod{p}$. This gives an explicit way to find square roots mod p for primes congruent to 3 mod 4.
 - (b) Find a solution between 1 and 786 to the congruence $x^2 \equiv 7 \pmod{787}$.
2. Use Quadratic Reciprocity to evaluate the following Legendre symbols. You may check your answer with software like Sage, but show work involved in using Quadratic Reciprocity.
 - (a) $\left(\frac{83}{541}\right)$ (b) $\left(\frac{11768}{21661}\right)$
3. Given that $11^{1728} \equiv 1 \pmod{1729}$, we might suspect that 1729 is a prime but the existence of pseudoprimes would give us pause. The following illustrates how quadratic residue theory can possibly answer whether a probable prime is composite.
 - (a) Euler's criterion says that if p is prime then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$. Use successive squaring to compute $11^{864} \pmod{1729}$ and use Quadratic Reciprocity to compute $\left(\frac{11}{1729}\right)$. Do they agree? What can you conclude concerning the possible Primality of 1729?
 - (b) The following are all Carmichael Numbers (composites that are pseudoprimes to most bases): 6601, 8911, 10585, 15841, 29341, 41041. Pick one of these numbers and identify whether it can be "unmasked" as a composite number using quadratic residue theory as in part (a).