MA 341 HW #9, due Friday, Apr. 7

1. Prove that if a prime p divides a number of the form $n^2 + 1$, then p is either 2 or else $p \equiv 1 \pmod 4$.

2. Prove there are infinitely many primes which are 1 modulo 4, by filling in the details of this proof: if there were only finitely many, say $p_1, \ldots, p_t$, then let $n = p_1 \cdots p_t$, and consider $(2n)^2 + 1$.

3. Compute $\left(\frac{341}{2017}\right)$.

4. We saw in class that $\left(\frac{3}{p}\right)$ only depends on what p is modulo 12. Find the smallest integer n such that the following statement is true: For a prime p, $\left(\frac{5}{p}\right)$ depends only on what p is modulo n. Then do the same for $\left(\frac{7}{p}\right)$.

5. Show that if g is a primitive root modulo an odd prime p, then $\left(\frac{g}{p}\right) = -1$.

6. Let p be a Sophie Germain prime: this means that $p = 2q + 1$, where q is another prime number. Let $a \in U_p$. Show that if $a \not\equiv \pm 1 \pmod p$ and $\left(\frac{a}{p}\right) = -1$, then a is a primitive root mod p. (Think about what the order of a could be.)

7. 1823 is a Sophie Germain prime. Use the previous problem to find a primitive root mod 1823, without having to use modular exponentiation.