1. (a) Define the Legendre symbol.
   For a prime and a an integer, \((\frac{a}{p}) := 1\) if \(a\) is a quadratic residue mod \(p, \) \(-1\) if \(a\) is a quadratic non-residue mod \(p,\) and \(0\) if \(p|a.\)
   (If \(m \geq 2\) and \((a, m) = 1\) then \(a\) is a quadratic residue mod \(m\) if \(x^2 \equiv a \pmod{m}\) is solvable and otherwise it is a quadratic non-residue.)

(b) State the law of quadratic reciprocity.
   For distinct primes \(p, q \geq 3,\) \((\frac{p}{q})(\frac{q}{p}) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}.)

(c) Define what a primitive root mod \(m\) is.
   If \(m \geq 2\) and \((g, m) = 1\) then \(g\) is a primitive root mod \(m\) if and only if \(\text{ord}_m(g) = \phi(m).\)
   (\(\text{ord}_m(g) := \min\{k \geq 1 : g^k \equiv 1 \pmod{m}\}\) is the order of \(g,\) thus the condition is that \(g\) have maximum possible order.)

(d) Which \(m\) have primitive roots?
   Only \(m = 2, 4, p^a,\) or \(2p^a\) where \(p\) is an odd prime. (Thus these are the only \(m\) for which Euler’s criterion works. For the statement of the criterion see 5a)

2. For what primes \(p\) is 3 a quadratic residue mod \(p?\)
   If \(p = 2,\) then \(3 \equiv 1 \pmod{2}\) is a quadratic residue mod 2. If \(p = 3\) then \((3, p) \neq 1\) and so 3 is neither a residue nor a non-residue. Suppose \(p > 3.\) Thus \(p = 4k + 1\) or \(4k + 3\) and furthermore \(p = 3l + 1\) or \(3l + 2.\)
   By quadratic reciprocity, \((\frac{3}{p}) = (\frac{p}{3})\) if \(p = 4k + 1\) and \((\frac{3}{p}) = -(\frac{p}{3})\) if \(p = 4k + 3.\) Furthermore \((\frac{3}{p}) = (\frac{1}{3}) = 1\) if \(p = 3l + 1\) and \((\frac{3}{p}) = (\frac{3}{p}) = -1\) if \(p = 3l + 2.\) Putting these together we get that \((\frac{3}{p}) = 1\) iff both \(p = 4k + 1\) and \(p = 3l + 1\) or both \(p = 4k + 3\) and \(p = 3k + 2.\) Thus \((\frac{3}{p}) = 1\) iff \(p = 2, 12m + 1\) or \(12m + 11.\)

3. Show that there are infinitely many primes of the form \(8n + 7.\) (Show which odd primes \(p\) could possibly divide \(x^2 - 2.\))
   This is just like a certain HW problem.
Suppose \( p \) is an odd prime and \( p \mid (x^2 - 2) \). Then \( x^2 \equiv 2 \pmod{p} \) which implies \( \left( \frac{2}{p} \right) = 1 \). But \( \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8} = 1 \) if \( p = 8k + 1 \) or \( 8k + 7 \). Thus \( p = 8k + 1 \) or \( 8k + 7 \).

Suppose \( p_1, \ldots, p_n \) is a list of primes of the form \( 8k + 7 \). We show that there is one more prime \( q = 8k + 7 \) not on the list. Let \( N = (p_1 \cdots p_n)^2 - 2 \). \( N \) is of the form \( 8k + 7 \). Since \( N \) is odd, \( N \) is a product of odd primes \( q \) and they must be all of the form \( 8k + 1 \) or \( 8k + 7 \).

But if all the \( q \) were of the form \( 8k + 1 \) then \( N \) would be of the form \( 8k + 1 \), a contradiction. So some \( q \) must be of the form \( 8k + 7 \). Since \( q \mid N = (p_1 \cdots p_n)^2 - 2 \) and \( q \) is odd it can’t be any of the \( p_i \).

4. (a) What are the roots of \( f(x) = x^4 - 1 \) mod 5?

They are \( x \equiv 1, 2, 3, 4 \pmod{5} \) by Euler’s theorem: \( a^{\phi(m)} \equiv 1 \pmod{m} \) for all \( (a, m) = 1 \).

(b) How many roots does \( f(x) \) have mod 25?

Since \( f'(x) = 4x^3 \), \( f'(x) \not\equiv 0 \pmod{5} \) for any root \( x \not\equiv 0 \pmod{5} \). All the roots are non-singular and thus they all lift to roots mod 25 by Hensel’s Lemma. Thus there are 4 roots mod 25.

(c) \( a_1 = 2 \) is a root of \( f(x) \) mod 5. What root \( a_2 \) mod 25 does \( a_1 \) lift to?

By Hensel’s Lemma \( a_1 \) mod 5 lifts to \( a_2 = a_1 - \overline{f(a_1)}f(a_1) \pmod{25} \). \( f'(a_1) = f'(2) = 4(2^3) = 32 \equiv 2 \pmod{5} \) and \( f(a_1) = 15 \) so \( a_2 = 2 - 2 \cdot 15 = 2 - 3 \cdot 15 = -43 \equiv 7 \pmod{25} \).

5. (a) Suppose \( p \) is an odd prime. How many roots does \( f(x) = x^4 - 1 \) have mod \( p^\alpha \)?

Euler’s criterion states that if \( m = 2, 4, p^\alpha \), or \( 2p^\alpha \) where \( p \) is an odd prime then \( x^n \equiv a \pmod{m} \) has \( k = (n, \phi(m)) \) solutions if \( a^{\phi(m)/k} \equiv 1 \pmod{m} \) and otherwise it has none. Here \( k = (4, \phi(p^\alpha)) = (4, p^\alpha - 1(p - 1)) \). If \( p = 4l + 1 \) then \( k = (4, p^{\alpha-1}4l) = 4 \). If \( p = 4l + 3 \) then \( k = (4, p^{\alpha-1}2(2l + 1)) = 2 \) since \( p^{\alpha-1}(2l + 1) \) is odd. Thus it has 4 solutions if \( p = 4l + 1 \) and 2 if \( p = 4l + 3 \).

You could also do it using methods of lifting and quadratic residues. \( f(x) = x^4 - 1 = (x^2 + 1)(x + 1)(x - 1) \equiv 0 \pmod{p} \) where \( p \) is an odd prime, always has the roots \( 1, -1 \). If will additionally have the two distinct non-zero roots of \( x^2 + 1 \equiv 0 \pmod{p} \) if \( \left( \frac{-1}{p} \right) = 1 \) (i.e. iff
Thus $f(x)$ will have 4 non-zero roots if $p = 4l + 1$ and 2 if $p = 4l + 3$. Since $p$ is odd, $f'(x) = 4x^3 \not\equiv 0 \pmod{p}$ if $x \not\equiv 0 \pmod{p}$. Thus all the roots will be non-singular, and thus lift to $p^a$ for any $a$, by Hensel’s Lemma.

(b) Suppose $m \geq 3$ is odd. How may roots does $f(x)$ have mod $m$? This is like the HW about the number of roots of $x^2 - 1 \pmod{m}$.

Let $m = \prod_{i=1}^{r} p_i^{a_i} \prod_{j=1}^{s} q_i^{b_i}$ where the $p_i$’s are distinct primes of the form $4l + 1$ and the $q_i$’s distinct primes of the form $4l + 3$. By the Chinese Remainder Theorem the number of roots mod $m$ is the product of the number of roots mod $p_i^{a_i}$ and mod $q_i^{b_i}$, or $4^r 2^s$. 
