THEORY OF NUMBERS, Math 115 B
Homework

1. For which positive integers a is the congruence $ax^4 \equiv 2 \ mod \ 13$ solvable?
2. Let p be an odd prime. Show that the congruence $x^4 \equiv -1(mod\ p)$has a solution if and only if p is of the form $8k+1$.
3. Using the previous exercise prove that there are infinitely many primes of the form $8k+1$.
4. Use the index system modulo 60 to find the solutions of $11x^7 \equiv 43(mod\, 60)$.
5. Encrypt the message DO NOT PASS GO using the ElGamal cryptosystem with the public-key $(p, r, b) = (2251, 6, 33)$. Show how the resulting ciphertext can be decrypted using the private key a=13.
6. Find all the quadratic residues of the following integers: a) 7, b) 8, c) 15, d) 18.
7. Find the values of the Legendre symbols $(\frac{j}{5})$ for $j = 1, 2, 3, 4, 5$
8. Show that that there are infinitely many primes of the form $4k+1$.
9. What is the law of quadratic reciprocity?
10. Evaluate the Legendre symbols of $(\frac{3}{53})$ $(\frac{111}{991})$ $(\frac{31}{641})$
11. Show that there are infinitely many primes of the form $5k+4$.
12. Find the solution to the following quadratic congruence $x^2 + 5x + 1 \equiv 0$ $(mod\ 7)$.