Assignment 10.

This homework is due *Tuesday* April 22.

There are total 48 points in this assignment. 43 points is considered 100%. If you go over 43 points, you will get over 100% for this homework (but not over 115%) and it will count towards your course grade.

Collaboration is welcome. If you do collaborate, make sure to write/type your own paper *and give credit to your collaborators in your pledge*. Your solutions should contain full proofs. Bare answers will not earn you much.

(1) (∼9.2.1) Using only basic properties of Legendre symbol and/or Euler's criterion, compute the following Legendre symbols:
  (a) [2pt] $(19/23)$,
  (b) [2pt] $(-23/59)$,
  (c) [2pt] $(20/31)$.

(2) (9.2.6)
  (a) [2pt] If p is an odd prime and $\gcd(ab, p) = 1$, prove that at least one of a, b, ab is a quadratic residue of p.
  (b) [2pt] Given a prime p, show that, for some choice of $n > 0$, p divides
$$(n^2 - 2)(n^2 - 3)(n^2 - 6).$$
  (*Hint:* Use (a).)

(3) Solve the following congruences by completing the square:
  (a) [2pt] $7x^2 + x + 11 \equiv 0 \pmod{17}$,
  (b) [2pt] $x - 3 \equiv 6x^2 \pmod{13}$,
  (c) [2pt] $x - 6 \equiv 6x^2 \pmod{13}$.

(4) [3pt] (9.2.13) Establish that the product of the quadratic residues of the odd prime p is congruent modulo p to 1 or -1 according as $p \equiv 3 \pmod 4$ or $p \equiv 1 \pmod 4$.
(*Hint:* Represent each quadratic residue a as $a \equiv b^2 \equiv -b(p - b) \pmod p$. Then use Wilson's theorem.)

(5) [3pt] (9.2.17) Prove that the odd prime divisors p of $9^n + 1$ are of the form $p \equiv 1 \pmod 4$. (*Hint:* $9 = 3^2$.)

(6) (9.3.1abcd) Compute the following Legendre symbols (you can take for granted that all denominators below are prime):
  (a) [2pt] $(71/73)$,
  (b) [2pt] $(-219/383)$,
  (c) [2pt] $(461/773)$,
  (d) [2pt] $(1234/4567)$.

(7) (9.3.3) Determine if the following quadratic congruences are solvable (you are not asked to actually solve them):
  (a) [2pt] $x^2 \equiv 219 \pmod{419}$ (take for granted that 419 is prime),
  (b) [2pt] $3x^2 + 6x + 5 \equiv 0 \pmod{89}$,
  (c) [2pt] $2x^2 + 5x - 9 \equiv 0 \pmod{101}$.

— see next page —

(8) (9.3.5)

(a) [3pt] Prove that if $p > 3$ and is an odd prime, then

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{6}; \\ -1 & \text{if } p \equiv 5 \pmod{6}. \end{cases}$$

(b) [3pt] Using part (a), show that there infinitely many primes of the form $6k+1$. (*Hint:* Assume that $p_1, p_2, \ldots, p_r$ are all primes of the form $6k+1$ and consider $N = (2p_1p_2\cdots p_r)^2 + 3$.)

(9) (9.3.10ab) Establish each of the following assertions:

(a) [3pt] $(5/p) = 1$ if and only if $p \equiv 1, 9, 11,$ or $19 \pmod{20}$.

(b) [3pt] $(6/p) = 1$ if and only if $p \equiv 1, 5, 19,$ or $23 \pmod{24}$.