Assignment 10.

This homework is due *Thursday* April 5.

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 (up to 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) (9.3.1abcd) 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] $(1234/4567)$.

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

(3) (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 $N = (2p_1p_2\cdots p_r)^2 + 3$.)

(4) (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 $23 \pmod{24}$.

(5) (a) [2pt] Show that if p is a prime number, $a, b \in \mathbb{Z}$ are coprime with p, and $a^2x \equiv b^2 \pmod p$, then $(x/p) = 1$.
   (b) [2pt] (9.3.13a) Show that if p is prime divisor of $839 = 38^2 - 5\cdot 11^2$, then $(5/p) = 1$. Use this fact to conclude that 839 is a prime number. (*Hint:* It suffices to consider primes under 29 because $29^2 = 841 > 839$.)

— see next page —

(6) (9.4.2) Solve the following congruences:
   (a) [2pt] $x^2 \equiv 7 \pmod{3^3}$,
   (b) [2pt] $x^2 \equiv 14 \pmod{5^3}$.
   (c) [2pt] $x^2 \equiv 2 \pmod{7^3}$.

(7) [4pt] ($\sim$9.4.8) For fixed *odd* $n > 1$, show that all solvable congruences $x^2 \equiv a \pmod{n}$ with $\gcd(a, n) = 1$ have the same number of solutions.

(8) (a) [2pt] Without finding them, determine the number of solutions of the congruences $x^2 \equiv 3 \pmod{11^2 \cdot 23^2}$ and $x^2 \equiv 16 \pmod{3 \cdot 5^3 \cdot 7^2}$.
   (b) [3pt] Same question for $x^2 \equiv 9 \pmod{3 \cdot 5^3 \cdot 7^2}$.
   (c) [3pt] Solve congruence $x^2 \equiv 16 \pmod{3 \cdot 5^3 \cdot 7^2}$.