Assignment 9.

This homework is due *Thursday* March 29.

There are total 40 points in this assignment. 32 points is considered 100%. If you go over 32 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) (~9.2.1) Using basic properties of Legendre symbol and Euler's criterion, compute the following Legendre symbols:
   (a) [2pt] $(19/23)$,
   (b) [2pt] $(-23/59)$,
   (c) [2pt] $(20/31)$.

(2) (~9.2.2) Using Gauss's lemma, compute the following Legendre symbols (that is, in each case obtain the integer n for which $(a/p) = (-1)^n$):
   (a) [2pt] $(8/11)$,
   (b) [2pt] $(5/19)$.

(3) (9.2.4a) [3pt] Let p be be an odd prime, let a be an integer such that $\gcd(a, p) = 1$. Show that the Diophantine equation

$$x^2 + py + a = 0$$

has an integral solution if and only if $(-a/p) = 1$.

(4) (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

$$(n^2 - 2)(n^2 - 3)(n^2 - 6)$$

(5) 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] $x - 6 \equiv 6x^2 \pmod{13}$.

(6) [4pt] Let p be be an odd prime, let a, b be integers. Show that the congruence

$$x^2 + 2ax + b \equiv 0 \pmod{p}$$

has two distinct solutions mod p if and only if $\gcd(a^2 - b, p) = 1$ and $\left(\frac{a^2-b}{p}\right) = 1$. (*Hint:* Complete the square.)

— see next page —

(7) (9.2.7)

(a) [2pt] Let p be and odd prime, a an integer such that $\gcd(a(a+1), p) = 1$. Prove that $\left(\frac{a(a+1)}{p}\right) = \left(\frac{1+a'}{p}\right)$, where a' is defined by $aa' \equiv 1 \pmod{p}$. (*Hint:* Replace 1 by aa'.)

(b) [3pt] Prove that

$$\sum_{a=1}^{p-2} \left(\frac{a(a+1)}{p}\right) = -1.$$

(*Hint:* Use item (a). Don't forget to keep track which values a' runs through as a runs from 1 to $p-2$.)

(8) [4pt] (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.)

(9) [4pt] (9.2.17) Prove that the odd prime divisors p of $9^n + 1$ are of the form $p \equiv 1 \pmod 4$.