Math 350 Assignment 6, Spring 2017

Due in class on Monday, February 27

Part 1.

1. Find all solutions to the congruence equation
$$36x+91 \equiv 31 \pmod{78}$$
2. Determine the number of solutions of the congruence equation
$$x^2+x+1 \equiv 0 \pmod{101}$$
3. Determine the number of solutions of the congruence equation
$$2x^2+1 \equiv 0 \pmod{1729}$$
4. Determine the number of solutions of the congruence equation
$$3x^2+1 \equiv 8 \pmod{56}$$
5. Determine the number of cubic roots of 1 in $\mathbb{Z}/9700Z$.

Part 2. (extra credit)

A. Let n be a positive integer whose primary factorization is $n = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1, \ldots, p_r$ are distinct prime numbers, and $e_1, \ldots, e_r$ are positive integers. What is the highest order of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$?

(Recall that the *order* of an element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ is the smallest positive integer $d \geq 1$ such that $a^d = 1 \bmod n$.)

B. (a sufficient criterion for primality, related to Fermat's theorem) Let p be an odd prime number, and let h be a natural number with $0 < h < p$. Let $n = hp+1$. Suppose that
$$2^h \not\equiv 1 \pmod{n} \quad \text{and} \quad 2^{n-1} \equiv 1 \pmod{n},$$
then n is a prime number.

Below are some more practice problems. Note that the Jacobi symbol is not officially included in the in-class exam, but you can use it in the exam.

P1. Suppose that a is an element of $\mathbb{Z}/101\mathbb{Z}$ such that $a^{513} = 1$. Is it possible that a is a primitive 100-th root of 1 in $\mathbb{Z}/101\mathbb{Z}$? Either give an example of a primitive element whose 513rd power is 1, or prove that there does not exist such an element.

P2. Determine whether the following statements are true or false.
(a) For prime numbers p, the Legendre symbol $\left(\frac{5}{p}\right)$ depends only on the congruence class of p modulo 5.
(b) For prime numbers p, the Legendre symbol $\left(\frac{11}{p}\right)$ depends only on the congruence class of p modulo 11.
(c) For non-zero natural numbers a, b which are relatively prime, the Jacobi symbol $\left(\frac{a}{b}\right)$ depends only on the congruence class of a modulo b.
(d) For non-zero natural numbers a, b which are relatively prime, the Jacobi symbol $\left(\frac{a}{b}\right)$ depends only on the congruence class of b modulo $4a$.

P3. Let p, q be prime numbers, $p \neq q$. Find a natural number n with $0 \neq n < pq$ such that $p^{2q-1} + q^{2p-1} \equiv n \pmod{pq}$. (The number n should be given in terms of p and q.)

P4. Suppose that d is a positive odd integer such that the Jacobi symbol $\left(\frac{-1}{d}\right) = 1$. Is -1 necessarily a square in $\mathbb{Z}/d\mathbb{Z}$? Either give a proof, or provide a counter-example.

P5. Prove or disprove the following statement: For every positive integer $n \geq 2$ there exists an element $(a \in \mathbb{Z}/n\mathbb{Z})^{\times}$ such that every element of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is a power of a?