Math 261 — Exam 2

November 7, 2018

The use of notes and books is **NOT** allowed.

Exercise 1: Polynomials mod 691 (30 pts)

In this exercise, you may freely use the fact that 691 *is* ***prime****.*

Consider the polynomials $f(x) = x^4 + 4x^3 + 4x^2 - 5x - 12$ and $g(x) = x^2 + 3x + 4$ in $(\mathbb{Z}/691\mathbb{Z})[x]$.

1. (5 pts) Check that $g(x) \mid f(x)$, and find a polynomial $h(x)$ such that $f(x) = g(x)h(x)$.
2. (5 pts) State the law of quadratic reciprocity.
3. (16 pts) Use Legendre symbols to prove that neither $g(x)$ nor $h(x)$ have any roots in $\mathbb{Z}/691\mathbb{Z}$.
4. (4 pts) What is the complete factorization of $f(x)$ in $(\mathbb{Z}/691\mathbb{Z})[x]$?

   Make sure to justify that your factors are irreducible.

Exercise 2: The Pépin test (30 pts)

In the 17th century, the French mathematician Pierre de Fermat studied the numbers

$$F_n = 2^{2^n} + 1,$$

where $n \in \mathbb{N}$. The purpose of this exercise is to establish a criterion to test whether F_n is prime. In the rest of the exercise, we fix $n \in \mathbb{N}$.

1. (4 pts) Prove that $F_n \equiv -1 \pmod 3$ and that $F_n \equiv 1 \pmod 4$.
2. (4 pts) Let $p \in \mathbb{N}$ be a prime such that $p \equiv 1 \pmod 4$. Prove that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$.
3. (7 pts) Use the previous questions to prove that if F_n is prime, then

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

4. (15 pts) Conversely, prove that if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, then F_n is prime. *Hint: Square both sides. What is $F_n - 1$, and what does this tell you about the multiplicative order of* 3 mod F_n*?*

Exercise 3: The Solovay-Strassen test (40 pts)

In this exercise, we fix an **odd** integer $N \geqslant 3$, **not** necessarily prime. Let

$$N = \prod_{i=1}^{r} p_i^{v_i}$$

be its factorization, where the p_i are distinct primes. We **define** the Jacobi symbol by the formula

$$\left[\frac{x}{N}\right] = \prod_{i=1}^{r} \left(\frac{x}{p_i}\right)^{v_i} \in \mathbb{Z}$$

for all $x \in \mathbb{Z}$, where $\left(\frac{x}{p_i}\right)$ is the usual Legendre symbol defined in class. In particular, if N is prime, then $\left[\frac{x}{N}\right] = \left(\frac{x}{N}\right)$.

1. In this question, we investigate some basic properties of the symbol $\left[\frac{x}{N}\right]$.

   The sub-questions of this question are independent from each other.

   (a) (3pts) Prove that if $x \equiv y \pmod{N}$, then $\left[\frac{x}{N}\right] = \left[\frac{y}{N}\right]$.

   (b) (6 pts) Prove that $\left[\frac{x}{N}\right] \neq 0 \iff x$ is invertible mod N.

   (c) (3 pts) Prove that $\left[\frac{xy}{N}\right] = \left[\frac{x}{N}\right]\left[\frac{y}{N}\right]$.

   We now introduce the function

$$\begin{array}{rccc} S: & (\mathbb{Z}/N\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^\times \\ & x & \longmapsto & \left[\frac{x}{N}\right] x^{\frac{N-1}{2}}. \end{array}$$

2. (10 pts) Prove that if N is prime, then $S(x) = 1$ for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$.

3. The goal of this question is to prove that conversely, if N is not prime, then $S(x)$ is not always 1.

   *In order to make things easier, we will suppose that N is composite and **squarefree**, that is to say that $N = p_1 p_2 \cdots p_r$ with the p_i distinct primes and $r \geqslant 2$. We **define** $M = N/p_1 = p_2 \cdots p_r$.*

   (a) (10 pts) Prove that there exists a $t \in \mathbb{Z}$ such that $\left(\frac{t}{p_1}\right) = -1$ and that $t \equiv 1 \pmod{M}$.
   Hint: CRT.

   (b) (8 pts) Prove that if t is as in the previous question, then $S(t) \neq 1$.
   Hint: Compute $S(t)$ mod M.

END