Math 261 — Exam 2

November 4, 2017

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

Exercise 1: Since today is November 4... (22 pts)

1. (8 pts) Factor 114 into irreducibles in $\mathbb{Z}[i]$.

   Make sure to justify that your factorization is complete.

2. (6 pts) Is 114 a sum of 2 squares ? Of 3 squares ? Of 4 squares ?

3. (8 pts) Given that $p = 1142017$ is prime, find the number of elements of $\mathbb{Z}[i]$ of norm p.

Exercise 2: Legendre symbols (17 pts)

1. (5 pts) State the law of quadratic reciprocity.

2. (7 pts) Compute the Legendre symbol $\left(\frac{33}{79}\right)$.

   You may use without proof the fact that 79 is prime.

3. (5 pts) Solve the equation $x^2 = x + 8$ in $\mathbb{Z}/79\mathbb{Z}$.

Exercise 3: A really big number (24 pts)

1. (6 pts) Prove that every integer $n \in \mathbb{N}$ is congruent to the sum of its digits mod 9.

2. (15 pts) Let $A = 4444^{4444}$, let B be the sum of the digits of A, let C be the sum of the digits of B, and finally let D be the sum of the digits of C. Compute D mod 9.

3. (3 pts) Deduce that $D = 7$.

Exercise 4: A primality test (37 pts)

Let $p \in \mathbb{N}$ be a prime such that $p \equiv 3 \pmod 4$, and let $P = 2p+1$. The goal of this exercise is to prove that P is prime if and only if $2^p \equiv 1 \bmod P$.

1. In this question, we suppose that P is prime, and we prove that $2^p \equiv 1 \bmod P$.

   (a) (6 pts) Compute the Legendre symbol $\left(\dfrac{2}{P}\right)$.

   (b) (5 pts) Deduce that $2^p \equiv 1 \pmod P$.
   Hint: What is $\frac{P-1}{2}$*?*

2. In this question, we suppose that $2^p \equiv 1 \bmod P$, and we prove that P is prime.

   (a) (6 pts) Prove that $2 \in (\mathbb{Z}/P\mathbb{Z})^\times$. What is its multiplicative order?

   (b) (6 pts) Deduce that $p \mid \phi(P)$.

   (c) (9 pts) Prove that p and P are coprime, and deduce that there exists a prime divisor q of P such that $q \equiv 1 \pmod p$.
   Hint: $\phi(\prod p_i^{a_i}) = \prod (p_i - 1) p_i^{a_i - 1}$.

   (d) (5 pts) Deduce that P is prime.
   Hint: How large can P/q *be?*

END