Math 261 — Final exam

December 13, 2017

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

Exercise 1: Since today is the 13th... (10 pts)

Factor $1+3i$ into irreducibles in $\mathbb{Z}[i]$.

Make sure to justify that your factorization is complete.

Exercise 2: Primes of the form x^2+4y^2 (28 pts)

Let $p \in \mathbb{N}$ be a prime. The goal of this exercise is to give **two** proofs of the following statement:

p is of the form x^2+4y^2 with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$. $(\star)$

Suggestion: In some of the questions below, you may find it easier to treat the cases $p \neq 2$ and $p = 2$ separately.

1. (10 pts) Find all primitive reduced quadratic forms of discriminant -16.
2. (10 pts) Deduce a proof of $(\star)$ using the theory of quadratic forms.
3. (8 pts) Use the theorem on the sum of 2 squares to find another proof of $(\star)$.

   Hint: $4y^2 = (2y)^2$.

Exercise 3: A Pell-Fermat equation (18 pts)

1. (10 pts) Compute the continued fraction of $\sqrt{37}$.

   *This means you should somehow find a formula for **all** the coefficients of the continued fraction expansion, not just finitely many of them.*

2. (8 pts) Use the previous question to find the fundamental solution to the equation $x^2 - 37y^2 = 1$.

Please turn over

Exercise 4: Carmichael numbers (44 pts)

1. (8 pts) State Fermat's little theorem, and explain why it implies that if $p \in \mathbb{N}$ is prime, then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.

   A *Carmichael number* is an integer $n \geqslant 2$ which is **not** prime, but nonetheless satisfies $a^n \equiv a \pmod{n}$ for all $a \in \mathbb{Z}$. Note that this can also be written $n \mid (a^n - a)$ for all $a \in \mathbb{Z}$.

2. (6 pts) Let $n \geqslant 2$ be a Carmichael number, and let $p \in \mathbb{N}$ be a prime dividing n. Prove that $p^2 \nmid n$.

   Hint: Apply the definition of a Carmichael number to a particular value of a.

3. Let $n \geqslant 2$ be a Carmichael number. According to the previous question, we may write
$$n = p_1 p_2 \cdots p_r$$
   where the p_i are distinct primes. Let p be one the the p_i.

   (a) (6 pts) Recall the definition of a primitive root mod p.

   (b) (9 pts) Prove that $(p-1) \mid (n-1)$.
   Hint: Consider an $a \in \mathbb{Z}$ which is a primitive root mod p.

4. (9 pts) Conversely, prove that if an integer $m \in \mathbb{N}$ is of the form
$$m = p_1 p_2 \cdots p_r$$
   where the p_i are distinct primes such that $(p_i - 1) \mid (m-1)$ for all $i = 1, 2, \cdots, r$, then m is a Carmichael number.

   Hint: Prove that $p_i \mid (a^m - a)$ for all $i = 1, \cdots, r$ and all $a \in \mathbb{Z}$.

5. (6 pts) Let $n \geqslant 2$ be a Carmichael number. The goal of this question is to prove that n must have at least 3 distinct prime factors. Note that according to question 2., n cannot have only 1 prime factor.

   Suppose that n has exactly 2 prime factors, so that we may write
$$n = (x+1)(y+1)$$
   where $x, y \in \mathbb{N}$ are distinct integers such that $x+1$ and $y+1$ are both prime. Use question 3.(b) to prove that $x \mid y$, and show that this leads to a contradiction.

END