Math 261 — Final exam

December 11, 2018

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

Exercise 1: A strange formula (24 pts)

Let a and b be positive integers.

1. (4 pts) Prove that $\gcd(ka, kb) = k\gcd(a, b)$ and that $\operatorname{lcm}(ka, kb) = k\operatorname{lcm}(a, b)$ for all $k \in \mathbb{N}$.

   Suggestion: Bézout (but there are plenty of other ways).

2. (3 pts) Prove that $\dfrac{a}{\gcd(a,b)}$ and $\dfrac{b}{\gcd(a,b)}$ are coprime.

3. (6 pts) Prove that if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.

   Hint: Prime divisor.

4. (6 pts) Prove that $\gcd\big(a + b, \operatorname{lcm}(a, b)\big) = \gcd(a, b)$.

   Hint: Use the previous questions.

5. (5 pts) Application: Suppose that $a + b = 144$ and that $\operatorname{lcm}(a, b) = 420$. Compute ab.

Exercise 2: A Pell-Fermat equation (16 pts)

1. (8 pts) Compute the continued fraction of $\sqrt{40}$.

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

2. (5 pts) Use the previous question to find the fundamental solution to the equation $x^2 - 40y^2 = 1$.

3. (3 pts) Find another non-trivial (i.e. not $x = \pm 1, y = 0$) solution to the equation $x^2 - 40y^2 = 1$ (simply changing the sign of x or y in the previous solution is not good enough).

Please turn over

Exercise 3: Multiples of sums of squares (27 pts)

The purpose of the exercise is to determine some conditions for the multiple of a sum of k squares to be a sum of k squares. We will consider the case $k = 2$ in most of the exercise, and $k = 3$ in the last question.

1. (1 pt) Briefly recall why n is a sum of two squares if and only if there exists $\alpha \in \mathbb{Z}[i]$ such that $N(\alpha) = n$.

2. (4 pts) Let $n \in \mathbb{N}$. Prove that if n is a sum of two squares, then so is $2n$.

   Hint: Multiply by $1 + i$.

3. (4 pts) More precisely, suppose that we know $a, b \in \mathbb{Z}$ such that $n = a^2 + b^2$. Find $c, d \in \mathbb{Z}$ (expressed in terms of a and b) such that $2n = c^2 + d^2$.

4. We now suppose that n is a sum of two squares. Let $k \in \mathbb{N}$. The purpose of the next two questions is to prove that kn is a sum of two squares if and only if k is a sum of two squares.

   (a) (4 pts) Prove that if k is a sum of two squares, then so is kn.

   (b) (7 pts) Prove that if k is **not** a sum of two squares, then neither is kn.

   Hint: What is the condition on the prime factorization of k for k to be a sum of two squares?

5. (7 pts) To conclude, we try again with **three** squares. Is it true that if $m, n \in \mathbb{N}$ are sums of **three** squares, then so is mn? (Either prove it or give a counter-example).

Exercise 4: Sophie Germain and the automatic primitive root (33 pts)

In this exercise, we fix an odd prime $p \in \mathbb{N}$ such that $q = \frac{p-1}{2}$ is also prime and $q \geqslant 5$.

1. (4 pts) Prove that $p \equiv -1 \pmod 3$.

   Hint: Express p in terms of q. What happens if $p \equiv +1 \pmod 3$?

2. (7 pts) Express the number of primitive roots in $(\mathbb{Z}/p\mathbb{Z})^\times$ in terms of q.

   Hint: What are the prime divisors of $p - 1$?

3. (10 pts) Let $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. Prove that x is a primitive root if and only if $x \neq \pm 1$ and $\left(\frac{x}{p}\right) = -1$.

   Hint: What are the prime divisors of $p - 1$? (bis)

4. (7 pts) Deduce that $x = -3 \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a primitive root.

5. (5 pts) (More difficult) Prove that $x = 6 \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a primitive root if and only if q is a sum of two squares.

END