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.

Solution 1:

1. When x and y range over $\mathbb{Z}$, Bézout tells us that the $ax + by$ are exactly the multiples of $\gcd(a, b)$. Multiplying by k, we see that the $k(ax + by)$ are the multiples of $k\gcd(a, b)$; on the other hands, they are also the $(ka)x + (kb)y$, i.e. the multiples of $\gcd(ka, kb)$. So $k\gcd(a, b)$ and $\gcd(ka, kb)$ are multiples of each other; since they are both positive, they are equal.

   It follows that

   $$\operatorname{lcm}(ka, kb) = \frac{(ka)(kb)}{\gcd(ka, kb)} = \frac{k^2ab}{k\gcd(a, b)} = k\frac{ab}{\gcd(a, b)} = k\operatorname{lcm}(a, b).$$

2. We could use Bézout again, or observe that if we define $g = \gcd(a, b)$, $a' = a/g$, and $b' = b/g$, then the previous question tells us that $\gcd(a, b) = \gcd(ga', gb') = g\gcd(a', b')$, which forces $\gcd(a', b') = 1$.

3. Suppose not. Then we could find a prime p which divides both $a + b$ and ab. Since $p \mid ab$, then $p \mid a$ or $p \mid b$ by Euclid's lemma. Suppose for instance that $p \mid a$ then $p \mid (a + b) - a = b$, which contradicts the fact that a and b are coprime.

4. Let us define again $g = \gcd(a, b)$, $a' = a/g$, and $b' = b/g$. We compute that

$$\gcd\big(a+b, \operatorname{lcm}(a,b)\big) = \gcd\big(g(a'+b'), g\operatorname{lcm}(a',b')\big) = g\gcd\big(a'+b', \operatorname{lcm}(a',b')\big).$$

But a' and b' are coprime, so $\operatorname{lcm}(a', b') = a'b'$, so we get

$$= g\gcd(a'+b', a'b') = g$$

by the previous question.

5. The previous formula tells us that $\gcd(a, b) = \gcd(144, 420)$, which by Euclid's algorithm turns out to be 12. Therefore

$$ab = \gcd(a,b)\operatorname{lcm}(a,b) = 12 \times 420 = 5040.$$

Remark: Since we know $a + b = 144$ and $ab = 5040$, we can deduce that a and b are the roots of $x^2 - 144x + 5040$. It follows that up to permutation, $a = 60$ and $b = 84$.

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).

Solution 2:

1. Let $x = \sqrt{40}$. Since x is a quadratic number, its continued fraction expansion is ultimately periodic. Let us make this fact explicit.

   We set $x_0 = x$, $a_0 = \lfloor x_0 \rfloor = 6$.

   Then $x_1 = \frac{1}{x_0 - a_0} = \frac{1}{\sqrt{40}-6} = \frac{\sqrt{40}+6}{4}$, so $a_1 = \lfloor x_1 \rfloor = 3$.

   Next, $x_2 = \frac{1}{x_1 - a_1} = \frac{1}{\frac{\sqrt{40}+6}{4} - 3} = \frac{4}{\sqrt{40}-6} = 4x_1 = \sqrt{40} + 6$, so $a_2 = \lfloor x_2 \rfloor = 12$.

   But then $x_3 = \frac{1}{x_2 - a_2} = \frac{1}{\sqrt{40}+6-12} = \frac{1}{\sqrt{40}-6} = x_1$, so we see by induction that $x_{n+2} = x_n$ and $a_{n+2} = a_n$ for all $n \geqslant 1$.

   Thus $\sqrt{40} = [6, \overline{3, 12}] = [6, 3, 12, 3, 12, 3, 12, \cdots]$.

2. From the a_n found in the previous question, we can compute the p_n and the q_n. We stop as soon as $p_n^2 - 40q_n^2 = \pm 1$ (and $n \neq 0$). We find:

n	a_n	p_n	q_n	$p_n^2 - 40q_n^2$
-1	•	1	0	•
0	6	6	1	-4
1	3	19	3	1

   so the fundamental solution is $x = 19$, $y = 3$.

3. We compute that $(19+3\sqrt{40})^2 = 721+114\sqrt{40}$, whence the solution $x = 721$, $y = 114$.

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).

Solution 3:

1. This is because $\mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\}$ and $N(x + yi) = x^2 + y^2$.

2. Since n is a sum of two squares, we can find $\alpha \in \mathbb{Z}[i]$ such that $N(\alpha) = n$. Let $\beta = (1 + i)\alpha$, then $N(\beta) = N\big((1 + i)\alpha\big) = N(1 + i)N(\alpha) = 2n$, so $2n$ is a norm, whence a sum of two squares.

3. In the same notation, we can take $\alpha = a + bi$, whence $\beta = (1 + i)(a + bi) = (a - b) + (a + b)i$, so we can take $c = a - b$, $d = a + b$.

4. (a) We have $n = N(\alpha)$ and $k = N(\gamma)$ for some $\alpha, \beta \in \mathbb{Z}[i]$, whence $kn = N(\alpha\gamma)$is a summ of two squares.

   (b) Since k is not a sum of two squares, there exists a prime $p \equiv -1 \pmod 4$ such that $v_p(k)$ is odd. Besides, since n is a sum of two squares, $v_p(n)$ must be even, so $v_p(kn) = v_p(k) + v_p(n)$ is odd, which prevents kn from being a sum of two squares.

5. The answer is no. Indeed, it is possible to have $mn \equiv 7 \pmod 8$ whereas $m, n \not\equiv 7 \pmod 8$. For instance, we can take $m = 3$, $n = 5$: neither is of the form $4^a(8b + 7)$, but their product 15 is.

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.

Solution 4:

1. Since $q \geqslant 5$, $p = 2q + 1 \geqslant 11$. As p is prime, is is this coprime to 3, so $p \equiv 1$ or $2 \pmod 3$. If $p = 2q + 1 \equiv 1 \pmod 3$, e would have $2q \equiv 0 \pmod 3$, whence $q \equiv 0 \pmod 3$ since 2 is invertible mod 3; in other words $3 \mid q$. Since $q \geqslant 5$ is prime, this is impossible.

2. This number is $\phi(\phi(p))$. As p is prime $\phi(p) = p - 1$, which factors as $2q$. Since 2 and q are distinct primes, we get

$$\phi(p - 1) = \phi(2q) = 2q \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{q}\right) = q - 1.$$

3. Let m be the multiplicative order of x. Fermat's little theorem tells us that $m \mid p - 1 = 2q$. Thus $m < 2q$ if and only if $m \mid 2$ or $m \mid q$. But

$$m \mid 2 \iff x^2 = 1 \iff (x - 1)(x + 1) = 0 \iff x = \pm 1$$

   since $\mathbb{Z}/p\mathbb{Z}$ is a domain, and

$$m \mid q \iff x^q = 1 \iff \left(\frac{x}{p}\right) = 1$$

   since $\left(\frac{x}{p}\right) = x^{p'} = x^q$. Besides, in any case $\left(\frac{x}{p}\right) = \pm 1$ since $x \neq 0$, so it is -1 if it is not $+1$.

   The conclusion follows.

   Remark: If $\left(\frac{x}{p}\right) = -1$, then x cannot be 1, so we could replace the first condition by $x \neq -1$.

4. We cannot have $-3 = +1$ in $\mathbb{Z}/p\mathbb{Z}$ since this would force $p \mid 4$; similarly we cannot have $-3 = -1$ either. It thus only remains to check that $\left(\frac{-3}{p}\right) = -1$. This is indeed true, since

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^q(-1)^q\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

by quadratic reciprocity and because $p \equiv -1 \pmod 3$ by the first question.

5. It is again easy to prove that $6 \not\equiv \pm 1 \pmod p$ since this would force $p = 5$ or 7. Besides,

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right)(-1)^q\left(\frac{p}{3}\right) = \left(\frac{2}{p}\right)$$

since q is odd and $p \equiv -1 \pmod 3$, so 6 is a primitive root if and only if $\left(\frac{2}{p}\right) = -1$. To conclude, we now distinguish two cases.

On the one hand, if p is not a sum of two squares, then $q = 4k + 3$ for some $k \in \mathbb{N}$, so $p = 2q + 1 = 8k + 7$, whence $\left(\frac{2}{p}\right) = +1$ so 6 is not a primitive root.

On the other hand, if p is a sum of two squares, then $q = 4k + 1$ for some $k \in \mathbb{N}$ (we cannot have $q = 2$ since $q \geqslant 5$), so $p = 2q + 1 = 8k + 3$, whence $\left(\frac{2}{p}\right) = -1$ so 6 is a primitive root.

END