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.

Solution 1:

Let $\alpha = 1+3i$. We have $N(\alpha) = 1^2+3^2 = 10 = 2 \times 5$ so α must be of the form $\pi_2\pi_5$ where π_2 (resp. π_5) is an irreducible of norm 2 (resp. 5).

As π_2 must be associate to $1+i$, after taking a unit out of π_2 and putting it in π_5, we can assume that $\pi_2 = 1+i$, so that

$$\pi_5 = \alpha/(1+i) = \frac{1+3i}{1+i} = \frac{(1+3i)(1-i)}{2} = 2+i.$$

Thus $\alpha = (1+i)(2+i)$ is the complete factorization of α.

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

Solution 2:

1. Let (a,b,c) be a reduced form of discriminant -16. The we know that b must be even, and that $a \leqslant \sqrt{16/3} < \sqrt{6} < 3$, so $a = 1$ or 2. Finally, $c = \frac{16+b^2}{4a}$.

   For $a=1$, we can only take $b=0$ since $|b| \leqslant a$. This yields $c=4$, so we record the form x^2+4y^2.

   For $a=2$ we can have $b=0$ or $b=2$, but not $b=-2$ (since then we'd have $|b|=a$ so b would have to be positive). For $b=0$, we find $c=2$, whence the form $2x^2+2y^2$, but this form is not primitive so we throw it away. For $b=2$, we find $c=5/2$ which is not an integer.

   In conclusion, there is only one reduced primitive form of discriminant -16, namely x^2+4y^2.

2. By the previous question, every primitive form of discriminant -16 is equivalent to x^2+4y^2. Thus if $p \nmid 2 \times 16$ is a prime, then p is of the form $x^2 = 4y^2$ iff. $\left(\frac{-16}{p}\right) = 1$.

   The condition $p \nmid 2 \times 16$ is of course equivalent to $p \neq 2$; besides, for such p we have

   $$\left(\frac{-16}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{16}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{p'} = \begin{cases} +1 & \text{if} \quad p \equiv 1 \pmod 4 \\ 3 & \text{if} \quad p \equiv -1 \pmod 4 \end{cases}$$

   Besides, $p = 2$ is obviously not of the form x^2+4y^2, whence $(\star)$.

3. Suppose first that $p = 2$. Then $p \not\equiv 1 \pmod 4$ and p is clearly not fo the form x^2+4y^2, so $(\star)$ holds.

   Suppose now that $p \neq 2$. The p is odd, so$p \equiv 1$ or $3 \pmod 4$. Besides, since p is prime, it is a sum of 2 squares iff. $p \not\equiv 3 \pmod 4$. So if $p \equiv 3 \pmod 4$, then p is not the sum of 2 squares; a fortiori it is not of the form $x^2+4y^2 = x^2+(2y)^2$. Conversely, if $p \equiv 1 \pmod 4$, then $p = a^2+b^2$ is a sum of 2 squares; then as p is odd, a and b cannot have the same parity, so without loss of generality we may assume a odd and b even. If we write $b = 2y$, then we see that $p = a^2+(2y)^2 = x^2+4y^2$ with $x = a$. So we have proved that $(\star)$ also holds when $p \neq 2$.

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 $x^2 - 37y^2 = 1$.

Solution 3:

1. Let $x = \sqrt{37}$. 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 $x_1 = \frac{1}{x_0 - a_0} = \frac{1}{\sqrt{37}-6} = 6+\sqrt{37}$, so $a_1 = \lfloor x_1 \rfloor = 12$.

   Then $x_2 = \frac{1}{x_1 - a_1} = \frac{1}{6+\sqrt{37}-12} = \frac{1}{\sqrt{37}-6} = x_1$, so we see by induction that $x_{n+1} = x_n$ and $a_{n+1} = a_n$ for all $n \geqslant 1$.

   Thus $\sqrt{37} = [6, \overline{12}] = [6, 12, 12, 12, \cdots]$.

2. The first convergent of the continued fraction computed above is $p_0/q_0 = 6/1$. Trying $x = 6$, $y = 1$, we find that $6^2 - 37 \times 1^2 = -1$.

   So in order to find the fundamental solution, all we have to do is square the number $6 + 1 \times \sqrt{37}$. We find that

   $$(6+\sqrt{37})^2 = 36 + 12\sqrt{37} + 37 = 73 + 12\sqrt{37},$$

   so the fundamental solution is $x = 73$, $y = 12$.

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.

Solution 4:

1. Fermat's little theorem states that for all $n \in \mathbb{N}$ and for all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have $a^{\phi(n)} = 1$. In other words, for all $a \in \mathbb{Z}$ coprime to n, we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

   In particular, if $n = p$ is prime, then $\phi(n) = p - 1$, so that for all $a \in \mathbb{Z}$ not divisible by p we have $a^{p-1} \equiv 1 \pmod{p}$.

   Multiplying both sides by a, we get that $a^p \equiv a \pmod{p}$ for all a not divisible by p. This still holds even if $p \mid a$ since a and a^p are both $\equiv 0 \pmod{p}$ in this case.

2. Let us take $a = p$; since n is a Carmichael number, we have $n \mid (p^n - p)$. Now if $p^2 \mid n$, we deduce that $p^2 \mid (p^n - p)$, whence $p^2 \mid p$ since $p \mid p^n$ as $n \geqslant 2$, which is obviously a contradiction.

3. (a) A primitive root mod p is an element $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ of multiplicative order $p-1$; in other words, such that $x^m \neq 1$ for all $1 \leqslant m < p-1$.

   (b) Let $a \in \mathbb{N}$ be such that $(a \bmod p)$ is a primitive root mod p. Since n is a Carmichael number, we have $n \mid (a^n - a)$, whence $p \mid (a^n - a)$ as $p \mid a$. Thus $a^n \equiv a \pmod p$. But $a \not\equiv 0 \pmod p$ since a is a primitive root mod p, so since p is prime, a is invertible mod p, so we can simplify by a and get
   $$a^{n-1} \equiv 1 \pmod p.$$
   This says that $n-1$ is a multiple of the multiplicative order of $(a \bmod p)$, which is $p-1$ since $(a \bmod p)$ is a primitive root. Thus $(p-1) \mid (n-1)$.

4. Let p be one of $p_1, \cdots, p_r$. By assumption, we have $m - 1 = (p-1)q$ for some $q \in \mathbb{N}$.

   Let now $a \in \mathbb{Z}$. We have
   $$a^m - a = a(a^{m-1} - 1) = a((a^{p-1})^q - 1),$$
   so if $a \equiv 0 \pmod p$ then $a^m - a \equiv 0 \pmod p$, whereas if $a \not\equiv 0 \pmod p$, then $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, so by Fermat's little theorem we have $a^{p-1} \equiv 1 \pmod p$ whence $(a^{p-1})^q - 1 \equiv 1^q - 1 = 0 \pmod p$; so either way $a^m \equiv a \pmod p$, i.e. $p \mid (a^m - a)$.

   This holds for any $p \in \{p_1, \cdots, p_r\}$, and the p_i are coprime since they are distinct primes, so
   $$m = p_1 \cdots p_r \mid (a^m - a).$$
   Since this holds for all a, this means that m is a Carmichael number.

5. By question 3.(b), $x = (x+1) - 1$ divides $n - 1 = (x+1)(y+1) = xy + x + y$, so x divides $xy + x + y - x(y+1) = y$. Similarly, we see that $y \mid x$, so that $x = y$, which contradicts the assumption that x and y are distinct.

Note: The smallest Carmichael number is $561 = 3 \times 11 \times 17$. *There are infinitely many Carmichael numbers; more precisely, it was proved in 1992 that for large enough* X, *there are at least* $X^{2/7}$ *Carmichael numbers between* 1 *and* X. *The existence of Carmichael numbers means that a simple-minded primality test based on Fermat's last theorem would not be rigorous.*

END