Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin
Ollscoil Átha Cliath | The University of Dublin

Faculty of Engineering, Mathematics and Science

School of Mathematics

JS/SS Maths/TP/TJH **Semester 1, 2020**

MAU23101 Introduction to number theory — Mock exam

Dr. Nicolas Mascot

mascotn@tcd.ie

Instructions that apply to all take-home exams

1. This is an open-book exam. You are allowed to use your class notes, textbooks and any material that is available through the internet. However, you are not allowed to collaborate, seek help from others, or provide help to others. You are not allowed to post questions on online forums such as Stack Exchange.

2. If you have any questions about the content of this exam, you may seek clarification from the lecturer using the e-mail address provided. You are not allowed to discuss this exam with others.

3. Solutions must be submitted through Blackboard by the deadline listed above. You must submit a single pdf file for each exam separately and sign the following declaration in each case. Please check that your submission has uploaded correctly.

Plagiarism declaration: I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar which are available through https://www.tcd.ie/calendar.

Signature: _____

Additional instructions for this particular exam

This is a mock exam, so ignore the instructions above! It is also longer than the actual exam.

Question 1 *Lucky 13*

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

Make sure to justify that your factorization is complete.

Question 2 *Primes of the form x^2+4y^2*

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

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

Question 3 *A Pell-Fermat equation*

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

Question 4 *Carmichael numbers*

1. 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. 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) Recall the definition of a primitive root mod p.

   (b) Prove that $(p-1) \mid (n-1)$.

   Hint: Consider an $a \in \mathbb{Z}$ which is a primitive root mod p.

4. 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. 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.

Question 5 *Sophie Germain and the automatic primitive root*

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. Prove that $p \equiv -1 \pmod 3$.

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

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

5. (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