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

Faculty of Science, Technology, Engineering and Mathematics

School of Mathematics

JS/SS Maths/TP/TJH **Semester 1, 2021**

MAU23101 Introduction to number theory — Mock exam

Dr. Nicolas Mascot

Instructions to candidates:

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

You may not start this examination until you are instructed to do so by the Invigilator.

Question 1 *Two primes*

Find distinct prime numbers $p, q \in \mathbb{N}$ both greater than 50 such that p is a square mod q, but q is not a square mod p.

Question 2 *Lucky 13*

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

Make sure to justify that your factorization is complete.

Question 3 *A primality test*

Let $p \in \mathbb{N}$ be a prime such that $p \equiv 3 \pmod 4$, and let $P = 2p+1$. The goal of this exercise is to prove that P is prime if and only if $2^p \equiv 1 \bmod P$.

1. In this part of the Question, we suppose that P is prime, and we prove that $2^p \equiv 1 \bmod P$.
   (a) Evaluate the Legendre symbol $\left(\dfrac{2}{P}\right)$.
   (b) Deduce that $2^p \equiv 1 \pmod P$.
   Hint: What is $\frac{P-1}{2}$*?*
2. In this part of the Question, we suppose that $2^p \equiv 1 \bmod P$, and we prove that P is prime.
   (a) Prove that $2 \in (\mathbb{Z}/P\mathbb{Z})^\times$. What is its multiplicative order?
   (b) Deduce that $p \mid \phi(P)$.
   (c) Prove that p and P are coprime, and deduce that there exists a prime divisor q of P such that $q \equiv 1 \pmod p$.
   Hint: $\phi(\prod p_i^{a_i}) = \cdots$.
   (d) Deduce that P is prime.
   Hint: How large can P/q *be?*

Question 4 *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 5 *Gaussian congruences*

The purpose of this Question is to generalise the concept of congruence to $\mathbb{Z}[i]$.

In this Question, we fix a nonzero $\mu \in \mathbb{Z}[i]$, and whenever $\alpha, \beta \in \mathbb{Z}[i]$, we say that $\alpha \equiv \beta \bmod \mu$ if $\alpha - \beta$ is a multiple of μ in $\mathbb{Z}[i]$, that is to say if there exists $\lambda \in \mathbb{Z}[i]$ such that $\alpha - \beta = \lambda\mu$.

1. Example: prove that $2 \equiv 4i \bmod 2 + i$.

2. Let $\alpha \in \mathbb{Z}[i]$. Prove that there exists $\rho \in \mathbb{Z}[i]$ such that $\alpha \equiv \rho \bmod \mu$ and $N(\rho) < N(\mu)$.

   Hint: Euclid.

We say that an element $\alpha \in \mathbb{Z}[i]$ is *invertible mod* μ if there exists $\beta \in \mathbb{Z}[i]$ such that

$$\alpha\beta \equiv 1 \bmod \mu.$$

3. Prove that α is invertible mod μ if and only if α and μ are coprime in $\mathbb{Z}[i]$.

4. Example: let $\alpha = 1 - 2i$ and $\mu = 3 + i$. Prove that α is invertible mod μ, and find $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta \equiv 1 \bmod \mu$.

Question 6 *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 7 *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