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

SF/JS Mathematics **Michaelmas Term 2024**

Introduction to Number Theory - Sample Exam 2

Day **Place** **Time**

Dr. Adam Keilthy

Instructions to candidates:

Attempt any three questions. If you attempt all four questions, only your best three will be considered in your grade. All questions are worth 30 points

Unless stated otherwise, you may use all statements given lectures without proof, but must clearly justify that the assumptions of statement are fulfilled.

Additional instructions for this examination:

Formula and tables are available from the inviligators if required.

You may use a non-programmable calculator. Please indicate the make and model of your calculator on each answer book used.

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

Question 1

In this question, you may freely use that $323 = 17 \times 19$ is the prime factorisation of 323, as we demonstrate an example of encryption via number theory.

i) (5pts) State Euler's theorem and derive Fermat's little theorem as a special case.

ii) (5pts) Compute the totient function $\phi(323)$

iii) (8pts) Determine the multiplicative inverse of 323 in $\mathbb{Z}/\phi(323)\mathbb{Z}$

iv) (12pts) Let a be a three digit number, coprime to 323 such that

$$a^{323} \equiv 132 \pmod{323}.$$

Determine a.

Question 2

1. (8pts) Define what it means for a triple of integers (a, b, c) to be a primitive Pythagorean triple and describe what such triples look like.

2. (12pts) Determine all right angled triangles whose side lengths (a, b, c) form a primitive Pythagorean triple, such that the area of the triangle is equal to its perimeter

$$a + b + c = \frac{1}{2}ab.$$

   You should give your answer in the form of equations for a, b and c.

3. (10pts) Similarly, describe all right angled triangles with integer side lengths whose area is equal to its perimeter.

Question 3

i) (8pts) Let $\alpha = 17 + 8i$ and $\beta = 3 + 4i$. Determine $\gamma,\ \rho \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\gamma + \rho$$

and $\mathrm{N}(\rho) < \mathrm{N}(\beta)$.

ii) (12pts) Determine a factorisation into irreducibles of the Gaussian integer $\alpha = 65 - 45i$

iii) (10pts) Let $\alpha\,\beta \in \mathbb{Z}[i]$, and suppose $\beta \neq 0$. Then there exist $\gamma, \rho \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\gamma + \rho$$

and $\mathrm{N}(\rho) < \mathrm{N}(\beta)$. These γ and ρ are not unique. Prove, or give a counterexample, that if

$$\alpha = \beta\gamma_1 + \rho_1 = \beta\gamma_2 + \rho_2$$

and $\mathrm{N}(\rho_1),\ \mathrm{N}(\rho_2) < \mathrm{N}(\beta)$, then $\mathrm{N}(\rho_1) = \mathrm{N}(\rho_2)$.

Question 4

i) (8pts) For rational numbers $\frac{p}{q}$ and $\frac{a}{b}$, show that

$$\left|\frac{p}{q} - \frac{a}{b}\right| \geq \frac{1}{bq}$$

except when $\frac{p}{q} = \frac{a}{b}$.

ii) (8pts)Show that e is algebraic of degree 2 if and only if there exist $a, c \in \mathbb{Q}$ such that $ae + ce^{-1}$ is rational

iii) (14pts) Hence or otherwise, show that e is not algebraic of degree two.

Hint: You may freely use that

$$\sum_{n>m} \frac{1}{n!} < \frac{2}{(m+1)!}$$