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 - Solutions

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.

Solution

i) Let $n \in \mathbb{N}$, and denote by $\phi(n)$ Euler's totient function. Euler's theorem says that

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for all $a \in \mathbb{Z}$ such that a is coprime to n.

Fermat's little theorem states that, for prime p and any integer a

$$a^p \equiv a \pmod{p}.$$

This is clearly true for $a \equiv 0 \pmod{p}$. For a not divisible by p, a is coprime to p, so we can apply Euler's theorem. The totient function $\phi(p) = p - 1$, so

$$a^{p-1} \equiv 1 \pmod{p} \quad \Rightarrow \quad a^p \equiv a \pmod{p}.$$

ii) $\phi(323) = \phi(17)\phi(19) = (17-1)(19-1) = 16 \times 18 = 288.$

iii) We apply Euclid's algorithm:

$$323 = 288 + 35$$
$$288 = 8(35) + 8$$
$$35 = 4(8) + 3$$
$$8 = 2(3) + 2$$
$$3 = 2 + 1$$

and so

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2 \times 3) = 3(3) - 8 \\ &= 3(35 - 4 \times 8) - 8 = 3(35) - 13(8) \\ &= 3(35) - 13(288 - 8 \times 13) \\ &= 107(35) - 13(288) \\ \\ &= 107(323 - 288) - 13(288) = 107(323) - 120(288) \end{aligned}$$

and hence 107 is the multiplicative inverse of 323 modulo 288.

iv) Since $a^k \pmod{323}$ depends only on the value of $k \pmod{288}$, we have that

$$a \equiv a^1 \equiv a^{323 \times 288} \equiv (a^{323})^{288} \equiv (132)^{288} \pmod{323}.$$

We can check that

$$132 \equiv 132 \pmod{323}$$
$$132^2 \equiv -18 \pmod{323}$$
$$132^3 \equiv -115 \pmod{323}$$
$$132^2 \equiv -1 \pmod{323}$$

and so

$$(132)^{107} \equiv (132^4)^{26}(132)^3 \equiv (-1)^{26}(-115) \equiv 208 \pmod{323}$$

We can check that $a = 208$ satisfies all the required properties, so $a = 208$ is the desired integer.

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.

Solution

i) A primitive Pythagorean triple is a collection of positive integers (a, b, c) such that a, b, and c are pairwise coprime, and $a^2 + b^2 = c^2$. Up to swapping a and b, every such triple is of the form

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2$$

where $u > v > 0$ is a pair of coprime integers, where exactly one of u or v is even.

ii) For such primitive Pythagorean triples, there exist u, v as above such that

$$2u(u + v) = 2u^2 + 2uv = \frac{1}{2}(u^2 - v^2)(2uv) = (u - v)(u + v)uv$$

Since $u, v > 0$, we can divide both sides by $u(u + v)$ to get

$$2 = (u - v)v \quad \Rightarrow \quad v = 2,\ u - v = 1 \text{ or } v = 1,\ u - v = 2$$

and so we have that $v = 2$, $u = 3$ or $v = 1, u = 3$. But since one of u or v must be even, the only possibility is $v = 2$, $u = 3$ and so the only possible such primitive Pythagorean triples are

$$\{(5, 12, 13),\ (12, 5, 13)\}$$

iii) Every right angled triangle with integer side lengths has side lengths of the form

$$(A, B, C) = (da, db, dc) \quad \text{where} \quad (a, b, c)$$

is a primitive Pythagorean triple, and $d \in \mathbb{N}$. If the area is equal to the perimeter, then

$$d(a + b + c) = \frac{d^2}{2}ab$$

and hence

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

Writing a, b, c in terms of u and v, we find that, similarly to the last question,

$$2 = d(u - v)v$$

Since d is an integer, we must have that $d|2$ and hence $d = 1$ or $d = 2$. If $d = 1$, then, by the previous part, the side lengths are $(5, 12, 13)$ up to reordering If $d = 2$, then we must have $v = u - v = 1$, and we get triangles with side lengths $(6, 8, 10)$.

Question 3

i) (8pts) Let $\alpha = 17 + 8i$ and $\beta = 3 + 4i$. Determine γ, $\rho \in \mathbb{Z}[i]$ 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 $\mathrm{N}(\rho_1) = \mathrm{N}(\rho_2)$.

Solution

i) We compute that

$$\frac{\alpha}{\beta} = \frac{17 + 8i}{3 + 4i} = \frac{(17 + 8i)(3 - 4i)}{25} = \frac{83 - 44i}{25} \approx 3 - 2i.$$

Let $\gamma = 3 - 2i$, and

$$\rho = \alpha - \beta\gamma = 17 + 8i - (3 + 4i)(3 - 2i) = 0 + 2i = 2i.$$

We can easily check that $\mathrm{N}(\rho) = 4 < 25 = \mathrm{N}(\beta)$.

ii) We first compute the norm of α: $\mathrm{N}(\alpha) = 65^2 + 45^2 = 6250$, which factorises as

$$6250 = 2 \times 5^5$$

Hence

$$\alpha = \nu\pi_{(2)}\pi_{(5,1)}\pi_{(5,2)}\pi_{(5,3)}\pi_{(5,4)}\pi_{(5,5)}$$

for some unit ν and irreducibles of norm 2 and 5. Since $5|\alpha$, we can assume that $\pi_{(5,1)} = \overline{\pi_{(5,2)}}$ so that

$$\pi_{(5,1)}\pi_{(5,2)} = 5$$

We then must have that the remaining three irreducibles of norm 5 must be equal, as otherwise we would have that $25|\alpha$. By changing ν, we can assume that

$$\pi_{(2)} = 1 + i,\ \pi_{(5,1)} = 1 + 2i,\ \pi_{(5,2)} = 1 - 2i.$$

To determine the remaining irreducibles of norm 5, we try dividing $\frac{\alpha}{5} = 13 + 9i$ by $1 \pm 2i$:

$$\frac{13 + 9i}{1 + 2i} = \frac{31 - 17i}{5} \notin \mathbb{Z}[i]$$

and

$$\frac{13 + 9i}{1 - 2i} = \frac{-5 + 35i}{5} = -1 + 7i \in \mathbb{Z}[i].$$

Hence $\pi_{(5,3)} = \pi_{(5,4)} = \pi_{(5,5)} = 1 - 2i$. To determine ν, we must divide α by

$$(1 + i)(1 + 2i)(1 - 2i)^4 = -65 - 45i.$$

This gives $\nu = -1$ and hence

$$65 + 45i = -(1 + i)(1 + 2i)(1 - 2i)^4$$

is a factorisation into irreducibles.

iii) We ensure that $\mathrm{N}(\rho) < \mathrm{N}(\beta)$ by choosing γ to be the Gaussian integer whose real and imaginary parts are obtained by rounding those of $\frac{\alpha}{\beta}$ to the nearest integer. But this isn't strictly necessary, so we might try some other ways of rounding.

We have seen that

$$17 + 8i = (3 + 4i)(3 - 2i) + 2i$$

where $\mathrm{N}(2i) = 4 < \mathrm{N}(3 + 4i)$. We could consider other ways of rounding

$$\frac{\alpha}{\beta} = \frac{83 - 44i}{25}$$

Let's try $\gamma = 4 - 2i$:

$$\rho = 17 + 8i - (3 + 4i)(4 - i) = -3 - 2i$$

and $\mathrm{N}(\rho) = 13 < \mathrm{N}(3 + 4i)$, but $\mathrm{N}(\rho) \neq \mathrm{N}(2i)$.

Thus, the claim is false.

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

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

Solution

i) If $\frac{p}{q} \neq \frac{a}{b}$ then

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

since $pb - aq$ is a non-zero integer, and is therefore at least 1 in absolute value.

ii) If e is algebraic of degree 2, there exist rational a, b, c such that e is a root of $f(x) = ax^2 + bx + c$, and hence

$$ae^2 + be + c = 0 \quad \Rightarrow ae + b + ce^{-1} = 0 \quad \Rightarrow ae + ce^{-1} = -b \in \mathbb{Q}.$$

iii) From the series expansion of e^x, we see that we have

$$ae + ce^{-1} = \sum_{k=0}^{\infty} a\frac{1}{k!} + c\frac{(-1)^k}{k!} = \frac{a + ce^{-1}}{k!}.$$

Let $q_m = m!$ and define $\frac{p_m}{q_m} \in \mathbb{Q}$ by

$$\frac{p_m}{q_m} = \sum_{k=0}^{m} \frac{a + c(-1)^k}{k!}$$

Then

$$\begin{aligned}\left|e-\frac{p_m}{q_m}\right| &= \left|\sum_{k=m+1}^{\infty}\frac{a+c(-1)^k}{k!}\right| \\ &\leq \sum_{k=m+1}^{\infty}\frac{|a|+|c|}{k!} \\ &< \frac{2C}{(m+1)!}\end{aligned}$$

for all $m \geq 1$, where $C = |a| + |c|$. But if $e = \frac{p}{q} \in \mathbb{Q}$, then

$$\frac{1}{qm!} \leq \left|e-\frac{p_m}{q_m}\right| < \frac{2C}{(m+1)!}$$

and hence

$$m+1 < 2Cq$$

for all $m \geq 1$, which is clearly impossible. Hence, we cannot have that $ae + ce^{-1}$ is rational for any $a, c \in \mathbb{Q}$ and hence e is not algebraic of degree 2.