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 1 - 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

i) (15pts) Show that for p a prime number

$$(p-1)! \equiv -1 \pmod{p}.$$

Hint: Try to pair $1, 2, \dots, p-1$ *up with their multiplicative inverse modulo* p*. Consider* $p = 2$ *separately.*

ii) (7 pts) Show that for n a composite number

$$(n-1)! \not\equiv -1 \pmod{n}.$$

iii) (8pts) Determine $30! \pmod{899}$, noting that $899 = 29 \times 31$.

Solution

i) For $p = 2$, $(2-1)! = 1! = 1 \equiv -1 \pmod{2}$. If $p > 2$, then note that, for all $x \in \{2, 3, \dots, p-2\}$, its multiplicative inverse mod p is distinct from x. Indeed, if $\overline{x} = \overline{x}^{-1}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, then $\overline{x}^2 = \overline{1}$. This has at most two solutions, as p is prime, and two distinct solutions are given by $\overline{x} = \overline{1}$ and $\overline{x} = \overline{-1} = \overline{p-1}$. Thus, in the product

$$2 \times 3 \times \cdots \times (p-2)$$

every factor can be paired with its multiplicative inverse to give

$$2 \times 3 \times \cdots \times (p-2) \equiv 1^{\frac{p-3}{2}} \equiv 1 \pmod{p}.$$

Thus

$$(p-1)! \equiv (p-1) \equiv -1 \pmod{p}.$$

ii) Choose a prime divisor p of n. We have that $1 < p < n$, so $p|(n-1)!$, or equivalently

$$(n-1)! \equiv 0 \pmod{p}.$$

But if

$$(n-1)! \equiv -1 \pmod{n}$$

then $(n-1)!+1 = kn = kmp$ for some $k \in \mathbb{Z}$ and $m = \frac{n}{p} \in \mathbb{Z}$, which implies that

$$(n-1)! \equiv -1 \pmod{p}.$$

Since -1 and 0 are distinct modulo p for every p, this gives a contradiction. Hence, we cannot have $(n-1)! \equiv -1 \pmod{n}$.

iii) We apply the Chinese remainder theorem. As $29|30!$,

$$30! \equiv 0 \pmod{29}$$

and by part (i),

$$(30! \equiv -1 \pmod{31}$$

Applying Euclid's algorithm, we compute

$$1 = 29 - 14(2) = 29 - 14(31-29) = 15(29) - 14(31)$$

and so, by the bijection from the Chinese remainder theorem

$$30! \equiv -15(29) \equiv -435 \equiv 464 \pmod{899}$$

Question 2

i) (4pts) Factorise $xy + ax + by + ab$.

ii) (8pts) Determine all integers $x,\ y \in \mathbb{Z}$ such that

$$xy - x - y = 0.$$

iii) (8pts) Determine all integers $x,\ y \in \mathbb{Z}$ such that

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$$

iv) (10pts) Describe all integer solutions $x,\ y,\ z \in \mathbb{Z}$ to the equation

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{z}.$$

Solution

i) $xy + ax + by + ab = (x + b)(y + a)$.

ii) We can rewrite this as

$$xy - x - y + 1 = 1$$

which factorises to give $(x-1)(y-1) = 1$. As $(x-1),\ (y-1) \in \mathbb{Z}$, we must have

$$(x-1) = (y-1) = \pm 1$$

as these are the only possible factorisations of 1. Hence the solutions are

$$x = y = 0 \text{ and } x = y = 2.$$

iii) We can rewrite this as

$$xy - 14x - 14y = 0$$

or, equivalently

$$(x - 14)(y - 14) = 14^2 = 196.$$

As the original equation was symmetric in x and y, we will initially assume $(x-14) \leq (y-14)$. The divisors of 196 are

$$1,\ 2,\ 4,\ 7,\ 14,\ 28,\ 49,\ 98,\ 196$$

Hence our solutions correspond to (up to swapping x and y)

$$\begin{aligned}
(x-14) &= \pm 1,\ (y-14) = \pm 196,\\
(x-14) &= \pm 2,\ (y-14) = \pm 98,\\
(x-14) &= \pm 4,\ (y-14) = \pm 49,\\
(x-14) &= \pm 7,\ (y-14) = \pm 28,\\
(x-14) &= \pm 14,\ (y-14) = \pm 14,
\end{aligned}$$

and so the set of solutions corresponding to positive divisors is

$$\{(15,210),(210,15),(16,112),(112,16),(18,63),(63,18),(21,42),(42,21),(28,28)\}.$$

and the set of solutions corresponding to negative divisors is

$$\{(13,-182),(-182,13),(12,-84),(-84,12),(10,-35),(-35,10),(7,-14),(-14,7)\}$$

Note that we omit the "solution" $(0,0)$, as this solves $xy-14x-14y$, but not our original equation.

iv) We, again, rewrite the equation as

$$xy - zx - zy = 0$$

or, equivalently

$$(x-z)(y-z) = z^2$$

and so every solution is uniquely determined by a choice of z and a choice of divisor s of z^2. Specifically, given $z \in$ and a divisor $s|z^2$, the corresponding solution of $xy - zx - zy = 0$ is given by

$$x = z + s, \text{ and } y = z + \frac{z^2}{s}.$$

We want to omit the case of where any of x, y, z are zero, so we must have $s \neq -z$. Thus, the set of solutions is parametrized by pairs (z, s) where $z \in \mathbb{Z} \setminus \{0\}$ and $s \in \mathbb{Z}$, $s|z^2$, $s \neq -z$.

While this is sufficient for the question, we could go a bit further and note that such s and z are characterized by a choice of non-zero $a, b, c \in \mathbb{Z}$, with $s = a^2b$, and $z = abc$, $c \neq -a$. Thus, the set of solutions is

$$x = abc + a^2b,\ y = abc + bc^2,\ z = abc$$

where $a + c \neq 0$.

Question 3

Let $a, b, c \in \mathbb{Z}$, let $p \in \mathbb{N}$ be an odd prime, and suppose that $p \not| a$.

1. (4pt) State necessary and sufficient conditions for the quadratic equation

$$\overline{a}x^2 + \overline{b}x + \overline{c} = \overline{0}$$

to have 0, 1, and 2 solutions in $\mathbb{Z}/p\mathbb{Z}$ respectively.

2. (7pts) Determine the number of solutions to

$$x^2 - \overline{3}x + \overline{3} = \overline{0}$$

in $\mathbb{Z}/31\mathbb{Z}$.

3. (7pts) Determine the number of solutions to

$$x^2 - \overline{3}x + \overline{3} = \overline{0}$$

in $\mathbb{Z}/37\mathbb{Z}$.

4. (12pts) Hence determine the number of solutions to

$$x^2 - \overline{3}x + \overline{3} = \overline{0}$$

in $\mathbb{Z}/1147\mathbb{Z}$. Be sure to fully justify your answer.

0.0.1 Solution

i) Define $\Delta \in \mathbb{Z}$ by $\Delta = b^2 - 4ac$. Then the number of solutions is determined by the Legendre symbol $\left(\frac{\Delta}{p}\right)$. We have 0 solutions if and only if $\left(\frac{\Delta}{p}\right) = -1$, 1 solution if and only if $\left(\frac{\Delta}{p}\right) = 0$ and 2 solutions if and only if $\left(\frac{\Delta}{p}\right) = 1$.

ii) We compute $\Delta = 9 - 12 = -3$. The Legendre symbol is then

$$\left(\frac{-3}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{3}{31}\right) = (-1)(-1)\left(\frac{31}{3}\right) = \left(\frac{1}{3}\right) = 1$$

so there are 2 solutions.

iii) The Legendre symbol is

$$\left(\frac{-3}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{3}{37}\right) = (-1)(-1)\left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1$$

so there are 2 solutions.

iv) Note that $1147 = 31 \times 37$, so if $1147|k^2 - 3k + 3$ for some $k \in \mathbb{Z}$, then $31|k^2 - 3k + 3$ and $37|k^2 - 3k + 3$. Thus the set of solutions in $\mathbb{Z}/1147\mathbb{Z}$ maps to the set

$$\{\text{Solutions in } \mathbb{Z}/31\mathbb{Z}\} \times \{\text{Solutions in } \mathbb{Z}/31\mathbb{Z}\}$$

under the bijection

$$\mathbb{Z}/1147\mathbb{Z} \to (\mathbb{Z}/31\mathbb{Z}) \times (\mathbb{Z}/37\mathbb{Z}).$$

Conversely, if

$$\begin{aligned} k^2 - 3k + 3 &\equiv 0 \pmod{31}, \\ \ell^2 - 3\ell + 3 &\equiv 0 \pmod{37}, \end{aligned}$$

then the Chinese remainder theorem lets us construct $n \in \mathbb{Z}$ such that

$$\begin{aligned} n &\equiv k \pmod{31}, \\ n &\equiv \ell \pmod{37} \end{aligned}$$

and hence

$$\begin{aligned} n^2 - 3n + 3 \equiv k^2 - 3k + 3 &\equiv 0 \pmod{31}, \\ n^2 - 3n + 3 \equiv \ell^2 - 3\ell + 3 &\equiv 0 \pmod{37}. \end{aligned}$$

Thus $31|n^2 - 3n + 3$ and $37|n^2 - 3n + 3$. As 31 and 37 are coprime, this implies that $1147|n^2 - 3n + 3$. Thus the Chinese remainder theorem gives a bijection between solutions in $\mathbb{Z}/1147\mathbb{Z}$ and

$$\{\text{Solutions in } \mathbb{Z}/31\mathbb{Z}\} \times \{\text{Solutions in } \mathbb{Z}/31\mathbb{Z}\}$$

Hence, there are $2 \times 2 = 4$ solutions.

Question 4

i) (12pts) By considering p-adic valuations, show that $\sqrt{2}$ is irrational.

ii) (12pts) By considering p-adic valuations, show that $\log_2 9$ is irrational.

iii) (6pts) Give an example of irrational $x, y \in \mathbb{R}$ such that $x^y \in \mathbb{Q}$ is rational.

Solution

i) Suppose $\sqrt{2} \in \mathbb{Q}$. Then there exist $a, b \in \mathbb{Z}$, with $b > 0$ such that $\sqrt{2} = \frac{a}{b}$, and hence

$$a^2 = 2b^2.$$

Taking the 2-adic valuation of both sides, we see that

$$2v_2(a) = v_2(a^2) = v_2(2b^2) = v_2(2) + v_2(b^2) = 1 + 2v_2(b).$$

The left hand side is even, while the right hand side is odd. This is impossible, hence $\sqrt{2}$ cannot be rational.

ii) Suppose $\log_2 9 \in \mathbb{Q}$. Then, there exist $a, b \in \mathbb{Z}$, with $b > 0$ such that $\log_2 9 = \frac{a}{b}$, and hence

$$\log_2 9^b = b \log_2 9 = a.$$

This implies that

$$3^{2b} = 9^b = 2^a$$

Taking 3-adic valuations, we must have that

$$0 = v_3(2^a) = v_3(3^{2b}) = 2b > 0$$

as b is non-zero. This is impossible, and so $\log_2 9$ cannot be rational.

iii) Consider $x = \sqrt{2}$, $y = \log_2 9 = 2\log_2 3$. Then

$$x^y = \sqrt{2}^{2\log_2 3} = 2^{\log_2 3} = 3 \in \mathbb{Q}.$$