MAU22103/33101 - Introduction to Number Theory

Exercise Sheet 3

Trinity College Dublin

Course homepage

Answers are due for Friday October 25th, 2pm.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *2021 was a better year for number theory (100 pts)*

Oh to be teaching in a year with fewer factors.

1. (70pts) Determine the number of solutions to the equation

$$x^2 - 5x + 8 = 0$$

in

i) (20pts) $\mathbb{Z}/43\mathbb{Z}$,

ii) (20pts) $\mathbb{Z}/47\mathbb{Z}$,

iii) (30pts) $\mathbb{Z}/2021\mathbb{Z}$
Hint: $2021 = 43 \times 47$*, and both* 43 *and* 47 *are prime, and in particular coprime.*

2. (30pts) For that, given $p \geq 5$, there exists $x \in \mathbb{Z}$ such that

$$p|x^2 - x + 3$$

if and only if there exists $y \in \mathbb{Z}$ such that

$$p|y^2 - y + 25$$

Hint: When do these have solutions modulo p? And why specify that $p \geq 5$?

This was the only exercise that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them

However, I strongly encourage you to give them a try, as the best way to learn number theory is through practice.

The exercises marked with a star are the exercises I will try to talk about in the tutorial lecture. If there are any exercises would would particularly like to discuss, please let me know

The exercises are arranged by theme, and roughly in order of difficulty within each theme, with the first few working as good warm-ups, and the remainder being of similar difficulty to the main exercise. You are welcome to email me if you have any questions about them. The solutions will be made available with the solution to the main exercise.

Exercise 2 *Computing roots* ★

i) Knowing that 127 is prime, how many elements $\overline{a} \in \mathbb{Z}/127\mathbb{Z}$ satisfy $\overline{a}^{53} = \overline{2}$? Compute them.

ii) How many elements satisfy $\overline{a}^3 = \overline{2}$?

Exercise 3 *Finding the floor*

Prove the following properties of the floor function:

i) For any x, $y \in \mathbb{R}$, $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$,

ii) For $n \in \mathbb{N}$ and $x \in \mathbb{R}$

$$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor,$$

iii) For any $n \in \mathbb{N}$ and $x \in \mathbb{R}$,

$$\lfloor x \rfloor + \lfloor x + \frac{1}{n} \rfloor + \cdots + \lfloor x + \frac{n-1}{n} \rfloor = \lfloor nx \rfloor.$$

Exercise 4 *Computing Legendre symbols* ★

Compute the following Legendre symbols:

$$\text{(i)} \left(\frac{39}{47}\right) \quad \text{(ii)} \left(\frac{91}{101}\right) \quad \text{(iii)} \left(\frac{261}{2017}\right) \quad \text{(iv)} \left(\frac{3}{1087}\right)$$
$$\text{(v)} \left(\frac{-6}{10007}\right) \quad \text{(vi)} \left(\frac{24}{191}\right) \quad \text{(vii)} \left(\frac{8000}{17}\right) \quad \text{(viii)} \left(\frac{-10}{1009}\right)$$

Exercise 5 *Factorials and floors*

Let $n \in \mathbb{N}$ and let $p \in \mathbb{N}$ be prime. Show that

$$v_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor.$$

Hint: How many multiples of p^k can we find in the product $n!$?. Also, note that this is actually a finite sum!.

Exercise 6 *Sums of Legendre symbols*

Let $p \in \mathbb{N}$ be an odd prime.

i) Compute $\sum_{a=0}^{p-1} \left(\frac{a}{p}\right)$.

ii) Compute

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \left(\frac{x+1}{p}\right)$$

Hint: For all non-zero a, write $\overline{a}(\overline{a} + \overline{1}) = \overline{a}^2(1 + \overline{a}^{-1})$.

Exercise 7 *Primes of the form* $6k+1$ ★

Let $p > 3$ be a prime.

i) Prove that $\overline{-3}$ is a square in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \pmod 6$.

ii) Using the identity $x^3 - 1 = (x-1)(x^2 - x + 1)$, determine the number of solutions of $x^3 - 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$ in terms of $p \pmod 6$.

iii) Suppose there are finitely many primes $p_1, \ldots, p_k$ such that $p_i \equiv 1 \pmod 6$. By considering

$$N = 12(p_1 \ldots p_k)^2 + 1$$

derive a contradiction to conclude there are infinitely many such primes.

Exercise 8 *Primitive roots and Legendre symbols*

Let p be an odd prime, and let $\overline{g} \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a primitive root. Show that $\left(\frac{g}{p}\right) = -1$

Exercise 9 *When Euler doesn't apply*

Define $t_n = \overline{2}^n$ in $\mathbb{Z}/40\mathbb{Z}$. As $\gcd(2, 40) = 2 \neq 1$, Euler's theorem does not apply, so we do not immediately get periodicity. However, we must get that the sequence is ultimately periodic. We want to compute the period and the length of the tail.

i) Give a formula for $t_n = \overline{2}^n$ in $\mathbb{Z}/5\mathbb{Z}$ in terms of $n \pmod 4$.

ii) Give a formula for $t_n = \overline{2}^n$ in $\mathbb{Z}/8\mathbb{Z}$.

iii) Deduce a formula for $t_n = \overline{2}^n$ in $\mathbb{Z}/40\mathbb{Z}$. What is the period? What is the length of the initial tail?

Exercise 10 *A test for higher powers* ★

Let $p \in \mathbb{N}$ be prime, $k \in \mathbb{N}$ be a positive integer, $g = \gcd(k, p-1)$, and $s = \frac{p-1}{g}$. Finally, let $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$.

i) Prove that $\overline{a}$ is a k^{th} power if any only if $a^s \equiv 1 \pmod p$,

ii) Is $\overline{9}$ a cube in $\mathbb{Z}/19\mathbb{Z}$? What about $\overline{7}$?

iii) Show that $\overline{a}^s$ is a solution of $x^g - \overline{1}$ in $\mathbb{Z}/p\mathbb{Z}$ for any element $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$.

iv) Choose a primitive root $\overline{r} \in (\mathbb{Z}/p\mathbb{Z})^\times$, and define a pseudo-Legendre symbol by

$$\left(\frac{a}{p}\right)_k := \begin{cases} 0 \text{ if } \overline{a} = \overline{0}, \\ e^{\frac{2\pi i s t}{p-1}} \text{ if } \overline{a} = \overline{r}^s. \end{cases}$$

Show that this is well defined, and that

$$\left(\frac{ab}{p}\right)_{k,\varphi} = \left(\frac{a}{p}\right)_{k,\varphi} \left(\frac{b}{p}\right)_{k,\varphi}, \quad \text{and} \quad \left(\frac{-1}{p}\right)_{k,\varphi} = (-1)^s.$$

This type of map is often called a character. In order to perform any useful computations with this pseudo-Legendre symbol though, we would need a reciprocity law. Such a reciprocity law exists, coming from the much more general Artin reciprocity law, which arguably spawned a huge area of modern number theory and is hopelessly beyond the scope of this course.

Exercise 11 *Easy square roots*

i) Let $p = 4k - 1$ be prime. Show that for non-zero $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$, exactly one of $\overline{a}$ and $\overline{-a}$ can be a square.

ii) Let $p = 4k - 1$ be prime, and let $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ be a non-zero quadratic residue (i.e. $\left(\frac{a}{p}\right) = 1$). Show that $\overline{a}^k$ is a square root of $\overline{a}$, that is to say $\overline{a}^{2k} = \overline{a}$.

iii) Use this result to explicitly solve the equation of the first part of Exercise 1 in $\mathbb{Z}/43\mathbb{Z}$ and $\mathbb{Z}/47\mathbb{Z}$.

Exercise 12 *Wilson's theorem*

Show that for p a prime number

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

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