Introduction to number theory
Exercise sheet 3

https://www.maths.tcd.ie/~mascotn/teaching/2021/MAU22301/index.html

Version: October 26, 2021

Email your answers to makindeo@tcd.ie by Friday November 5th, 2PM.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Pépin's test (100 pts)*

Recall (cf Exercise 12 of Sheet 1) that the n-th Fermat number is $F_n = 2^{2^n} + 1$, where $n \in \mathbb{N}$.

In this definition, as usual, a^{b^c} means $a^{(b^c)}$ rather than $(a^b)^c$ (since the latter simplifies into $a^{(b \times c)}$).

1. (10 pts) Prove that $F_n \equiv -1 \pmod 3$.
2. (50 pts) Prove that if F_n is prime, then $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. *Hint: What is this question doing in the middle of an assignment on the Legendre symbol?*
3. (40 pts) Conversely, prove that if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, then F_n is prime. *Hint: What can you say about the multiplicative order of 3 mod F_n?*

Remark: This primality test, named after the 19th century French mathematician Théophile Pépin, only applies to Fermat numbers, but is much faster than the general-purpose tests that can deal with any integer. It was used in 1999 to prove that F_{24} is composite, which is quite an impressive feat since F_{24} has 5050446 digits!

This was the only mandatory 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 highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 2 *Legendre symbols*

Evaluate the following Legendre symbols:

1. $\left(\frac{10}{1009}\right)$,

2. $\left(\dfrac{261}{2017}\right)$,

3. $\left(\dfrac{-77}{9907}\right)$,

4. $\left(\dfrac{-6}{10007}\right)$,

5. $\left(\dfrac{261}{2903}\right)$,

6. $\left(\dfrac{8000}{29}\right)$.

Note: 1009, 2017, 9907, 10007, 2903, and 29 are prime.

Exercise 3 *Applications of* $(\frac{-3}{p})$

1. Let $p > 3$ be a prime. Prove that -3 is a square mod p if and only if $p \equiv 1 \pmod 6$.

2. An element $x \in \mathbb{Z}/p\mathbb{Z}$ is called a *cube root of unity* if it satisfies $x^3 = 1$. Use the previous question and the identity $x^3 - 1 = (x-1)(x^2 - x + 1)$ to compute the number of cube roots of unity in $\mathbb{Z}/p\mathbb{Z}$ in terms of p mod 6.

3. Find another way to compute the number of cube roots of unity in $\mathbb{Z}/p\mathbb{Z}$ in terms of p mod 6 by considering the map
$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ x & \longmapsto & x^3. \end{array}$$

4. Use question 1. of this exercise to prove that there are infinitely many primes p such that $p \equiv 1 \pmod 6$.

   Hint: Suppose on the contrary that there are finitely many, say $p_1, \cdots, p_k$*, and consider* $N = 12(p_1 \cdots p_k)^2 + 1$.

Exercise 4 *A quadratic equation mod 2021 (100pts)*

Determine the number of solutions to the equation
$$x^2 - 3x + 7 = 0,$$
and then to
$$x^2 - 3x + 9 = 0,$$

1. (30pts) in $\mathbb{Z}/43\mathbb{Z}$,

2. (30pts) in $\mathbb{Z}/47\mathbb{Z}$,

3. (40 pts) in $\mathbb{Z}/2021\mathbb{Z}$ (*Hint:* 與上次作業相同的提示).

You may freely use the fact that $2021 = 43 \times 47$ *and that* 43 *and* 47 *are prime.*

Exercise 5 *Square roots mod p: the easy case*

1. Let p be a prime such that $p \equiv -1 \pmod 4$, and let $x \in \mathbb{Z}/p\mathbb{Z}$ be such that $\left(\frac{x}{p}\right) = +1$. Prove that $y = x^{\frac{p+1}{4}}$ is a square root of x, that is to say that $y^2 = x$.

2. What happens if $\left(\frac{x}{p}\right) = -1$? What if $p \not\equiv -1 \pmod 4$?

3. (Application) Use question 1. to find explicitly the solutions to the equations of the previous Exercise in $\mathbb{Z}/43\mathbb{Z}$ and $\mathbb{Z}/47\mathbb{Z}$.

Exercise 6 *Legendre vs. primitive roots*

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

Exercise 7 *Sums of Legendre symbols*

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

1. Compute $\displaystyle\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)$.

2. Compute $\displaystyle\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)$.

   Hint: write $x(x+1) = x^2(1+\frac{1}{x})$ wherever legitimate.

Exercise 8 $\sqrt[67]{2}$ mod 101

How many elements $x \in \mathbb{Z}/101\mathbb{Z}$ satisfy $x^{67} = 2$? Compute them.

Note: 101 is prime.

Exercise 9 *A test for higher powers*

Let $p \in \mathbb{N}$ be a prime, $k \in \mathbb{N}$ be an integer, $g = \gcd(p-1, k)$, and $p_1 = (p-1)/g \in \mathbb{N}$. Finally, let $x \in (\mathbb{Z}/p\mathbb{Z})^\times$.

1. Prove that x is a k-th power if and only if $x^{p_1} = 1 \bmod p$.

2. (Application) Is 2 a cube in $\mathbb{Z}/13\mathbb{Z}$? What about 5?

3. For general x, what kind of number is x^{p_1}, i.e. which equation does it satisfy?

4. Use the above to define a generalization of the Legendre symbol, and state a couple of its properties.