Math 261 — Exercise sheet 5

http://staff.aub.edu.lb/~nm116/teaching/2017/math261/index.html

Version: October 11, 2017

Answers are due for Monday 23 October, 11AM.

The use of calculators is allowed.

Exercise 5.1: $\sqrt[67]{2} \bmod 101$ (10 pts)

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

Note: 101 is prime.

Exercise 5.2: Legendre symbols (21 pts)

Compute the following Legendre symbols (7 pts each):

1. $\left(\frac{10}{1009}\right)$,
2. $\left(\frac{261}{2017}\right)$,
3. $\left(\frac{-77}{9907}\right)$.

Note: 1009, 2017 and 9907 are prime.

Exercise 5.3: Quadratic equations mod 55 (21 pts)

Use the Chinese remainders theorem and Legendre symbols to determine the number of solutions in $\mathbb{Z}/55\mathbb{Z}$ to these equations (7 pts each):

1. $x^2 - x + 8 = 0$,
2. $x^2 + 3x + 7 = 0$,
3. $x^2 - 4x - 1 = 0$.

*Note: 55 is **NOT** prime.*

Exercise 5.4: Applications of $(\frac{-3}{p})$ (26 pts)

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

2. (8 pts) An element $x \in \mathbb{Z}/p\mathbb{Z}$ is called a *cubic 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 cubic roots of unity in $\mathbb{Z}/p\mathbb{Z}$ in terms of p mod 6.

3. (8 pts) Find another way to compute the number of cubic 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. (4 pts) 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 5.5: Pépin's test (22 pts)

Recall (cf sheet 1 exercise 4) that the n-th Fermat number is $F_n = 2^{2^n} + 1$, where $n \in \mathbb{N}$.

1. (2 pts) Prove that $F_n \equiv -1 \pmod 3$.

2. (10 pts) Prove that if F_n is prime, then $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

3. (10 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* $3 \bmod F_n$*?*

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!

The exercises below are not mandatory. They are not worth any points, and are given here for you to practise. The solutions will be made available with the solutions to the other exercises.

Exercise 5.6: 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 5.7: 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 $x^{p_1} = 1$.
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.