Math 261 — Exercise sheet 7

http://staff.aub.edu.lb/~nm116/teaching/2018/math261/index.html

Version: October 30, 2018

Answers are due for Wednesday 7 November, 11AM.

The use of calculators is allowed.

Exercise 7.1: Legendre symbols (30 pts)

Compute the following Legendre symbols (10 pts each):

1. $\left(\frac{-6}{10007}\right)$,
2. $\left(\frac{261}{2903}\right)$,
3. $\left(\frac{8000}{29}\right)$.

Note: 10007, 2903 and 29 are prime.

Exercise 7.2: Legendre vs. primitive roots (10 pts)

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 $\left(\frac{g}{p}\right) = -1$.

Exercise 7.3: Quadratic equations mod 77 (30 pts)

Consider the following equations:

- $x^2 + 3x + 1 = 0$,
- $x^2 - x + 2 = 0$,
- $x^2 + 5x - 3 = 0$.

1. (4 pts/equation/prime) Determine how many solutions each equation has in $\mathbb{Z}/7\mathbb{Z}$, and then in $\mathbb{Z}/11\mathbb{Z}$.

   You must show your Legendre symbols computations, but you are not required to justify the steps.

2. (2 pts/equation) Use CRT to deduce how many solutions each equation has in $\mathbb{Z}/77\mathbb{Z}$. *Note: 77 is* ***NOT*** *prime.*

Exercise 7.4: Applications of $(\frac{-3}{p})$ (30 pts)

1. (15 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 *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. (7 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 $N = 12(p_1 \cdots p_k)^2 + 1$.

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 7.5: 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 exercise 7.4 in $\mathbb{Z}/7\mathbb{Z}$, in $\mathbb{Z}/11\mathbb{Z}$, and in $\mathbb{Z}/77\mathbb{Z}$.

Exercise 7.6: More Legendre symbols

Compute the following Legendre symbols:

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

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

3. $\left(\dfrac{-253}{9923}\right)$.

Note: 1009, 2017 and 9923 are prime.

Exercise 7.7: Quadratic equations mod 55

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

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

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

Exercise 7.8: 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.*