Math 261 — Fall 2022
Number Theory
`https://sites.aub.edu.lb/kmakdisi/`
Problem set 6, NOT DUE, for practice before the midterm

Reminder: The midterm exam will be held on Saturday, October 15, at 1pm in Bliss 205. You may use a nonprogrammable calculator and may bring a single sheet of A4 paper with handwritten notes and formulas on both sides. Next week, I have regular office hours on Wednesday and will also hold **additional office hours on Thursday**, from 2pm until 4pm and possibly later.

Exercise 6.1: a) Calculate each of the following for the primes $p = 11, 13$, and 17:

$$\left(\frac{-1}{p}\right), \quad \left(\frac{2}{p}\right), \quad \left(\frac{-2}{p}\right), \quad \left(\frac{3}{p}\right), \quad \left(\frac{4}{p}\right), \quad \left(\frac{6}{p}\right).$$

b) In the cases above when $\left(\frac{a}{p}\right) = 1$, find a square root of a modulo p.

c) How many solutions to $x^2 + 2 \equiv 0 \pmod{N}$ are there modulo each of the three values of N: (i) $N = 11^2 \cdot 13^3$, (ii) $N = 13^4 \cdot 17^5$, (iii) $N = 11^6 \cdot 17^7$? (Do NOT find the solutions. Just count the number of solutions in $\mathbf{Z}/N\mathbf{Z}$.)

Exercise 6.2: Compute the two Legendre symbols $\left(\frac{6}{37}\right)$, $\left(\frac{11}{31}\right)$ in three ways **each**:

a) using Euler's criterion;

b) using Gauss' lemma;

c) using quadratic reciprocity. (The statement of quadratic reciprocity will appear in lecture next week.)

Exercise 6.3: Let p be prime with $p \neq 2$.

a) Show that if $\left(\frac{a}{p}\right) = 1$, then a **cannot** be a primitive root mod p.

b) Show that if a satisfies $\left(\frac{a}{17}\right) = -1$, then a **is** a primitive root mod 17. Redo for $p = 257$.

c) Show that the converse of a is however false in general, by giving an example of an a for which $\left(\frac{a}{13}\right) = -1$, but a is **not** a primitive root mod 13.

Exercise 6.4: a) Let p be any prime with $p \geq 5$. Show that the equation

$$(x^2 - 2)(x^2 + 1)(x^2 + 2) \equiv 0 \pmod{p}$$

has at least one solution.

b) Show that if furthermore $p \equiv 1 \pmod{8}$, then the above equation has six solutions modulo p.