Math 261 — Fall 2022
Number Theory
`https://sites.aub.edu.lb/kmakdisi/`
Problem set 7, due Friday, October 28 at the beginning of class

Exercise 7.1: Let p be a prime number of the form $p = 4q + 1$ with q prime.

a) Show that $\left(\frac{2}{p}\right) = -1$.

b) Show that 2 is a primitive root modulo p.

Exercise 7.2: a) Let p be a prime other than 2 or 7. Use quadratic reciprocity to show that the value of $\left(\frac{7}{p}\right)$ depends only on p mod 28. (Hint: the Chinese remainder theorem is useful at one point.)

b) List all the values of p mod 28 for which $\left(\frac{7}{p}\right) = 1$ and those for which $\left(\frac{7}{p}\right) = -1$. You should write them in the form of a table where the first row gives the form of p, namely $p = 28k + 1$, $p = 28k + 3, \ldots$ and the second row gives the value of $\left(\frac{7}{p}\right)$.

(By the way, why did I skip $28k + 2$? What else needs to be skipped? Optional: View the choices of p mod 28 for which $\left(\frac{7}{p}\right) = 1$ as a subset of $(\mathbf{Z}/28\mathbf{Z})^*$. Do you notice anything interesting about this subset?)

c) Let $n \in \mathbf{Z}$ be any nonzero number (positive or negative). Use quadratic reciprocity (and not the key proposition from class) to show that for p not a factor of $2n$, the Legendre symbol $\left(\frac{n}{p}\right)$ depends only on p mod $4n$. Hint: factor n, and use the Chinese Remainder Theorem to look at the value of p mod each prime factor q of n.

d) Improve part (b) to show that if $n \equiv 1 \pmod 4$, then $\left(\frac{n}{p}\right)$ depends only on p mod n. (No fair using Jacobi reciprocity in parts (c) and (d), unless you prove it first.)

Exercise 7.3: Write the numbers 97, 90, and 485 as the sum of two squares (if possible, give two different solutions).

Exercise 7.4: Find the factorizations of the following numbers in $\mathbf{Z}[i]$ (i.e., factor into Gaussian primes, possibly times a unit):

$$65, \qquad 67, \qquad 134, \qquad 73, \qquad 100 + i, \qquad 510 + 180i.$$

Exercise 7.5: a) Factor 23400 into (a unit times) a product of Gaussian primes in $\mathbf{Z}[i]$.

b) Find a specific $\alpha = a + bi \in \mathbf{Z}[i]$ whose norm is 23400. Try to make a choice of α that is easy to calculate.

c) How many different $\alpha \in \mathbf{Z}[i]$ have norm 23400?

Exercise 7.6: Use the Euclidean algorithm to find the GCD (in $\mathbf{Z}[i]$) of

$$\alpha = -14 + 31i, \qquad \beta = 3 + 24i.$$

Write the GCD as a linear combination of α and β (with coefficients in $\mathbf{Z}[i]$, of course).