Number Theory Assignment 4
Due by 12.12.21

Q 1. (From Burton's book)
(i) Prove that the congruence $6x^2 + 5x + 1 \equiv 0 \mod p$ has a solution for every prime p. Does $6x^2 + 5x + 1 = 0$ have integer solutions?
(ii) Give an example of relatively prime integers a, n such that $a^{\phi(n)/2} \equiv 1 \mod n$ but $x^2 \equiv a \mod n$ does not have solutions. Can you give infinitely many examples?
(iii) If $p > 2$ is a prime, prove $1 + \sum_{a=1}^{p-2} \left(\frac{a(a+1)}{p} \right) = 0$.
(iv) Show that for any prime $p > 5$, there exist integers $1 \leq a, b \leq p - 1$ for which both $a, a + 1$ are quadratic residues while both $b, b + 1$ are quadratic non-residues mod p.

Q 2. Let k be an integer of the form $k = (4n - 1)^3 - 4m^2$ where m, n are integers with the property that NO prime of the form $4d + 3$ divides m. Then, prove that the equation $y^2 = x^3 + k$ has no solutions for integers x, y. *Hint.* Observe that for any possible solution, we must have $x \equiv 1 \mod 4$ and use it.

Q 3. (From NZM, after section 3.2.)
(i) Exercise 24, P. 142.
(ii) Exercise 25, P. 142.