MATH 3H03 (NUMBER THEORY)
DUE: MARCH 27, 2020

HOMEWORK ASSIGNMENT 8

All of the questions from Part A will be graded. For Part B, do questions 4 and 5, one of which will be graded completely and the other for completion. Assignments will be submitted via *Crowdmark*.

Part A. [Short Questions; 6pts]

Exercise 1. The name of a mathematician has been encoded using the RSA-procedure using the public key $(n, e) = (1643, 223)$. The encoded name (each block represents two letters) is

`1141      0566      0005`

(We have identified A with 01, B with 02, and so on). Who is the mystery mathematician?

Exercise 2. Find all the primitive roots of U_{17}. Then find a primitive root of U_{17^5}. [Hint: Read the proof of Theorem 6.7.]

Exercise 3. Compute $\left(\frac{1234}{4567}\right)$.

Part B. [Proof Questions; 6pts]

Exercise 4. Suppose that $n^4 \equiv -1 \pmod{p}$ for some odd prime p. Show that the order of n in U_p is 8.

The following result will be useful:

Fact. *Let $a \in U_n$, and suppose that the order of a is k. If $a^t \equiv 1 \pmod{n}$, then $k|t$.*

Proof. By the division algorithm, $t = kq + r$ with $0 \leq r < k$. If $r \neq 0$, then $1 \equiv a^t \equiv a^{kq+r} \equiv (a^k)^q a^r \equiv 1^q a^r \equiv a^r \pmod{n}$. So $a^r \equiv 1 \pmod{n}$, contradicting the fact that k is the smallest positive integer with this property. So $r = 0$, i.e., $t = kq$.

Exercise 5. For all distinct odd primes p and q, prove that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

[Remark: In some textbooks, this formula is sometimes taken as the statement of the Law of Quadratic Reciprocity.]