NUMBER THEORY I — ASSIGNMENT 11.2

SPRING 2018 — DUE APRIL 11

Exercise 1. Koblitz Exercise III.1.1.

Exercise 2. The *Vigenère cipher* is similar to the Caesar cipher except that it uses the previous plaintext letter to encrypt the next. Specifically, after choosing an initial key b_0 from the (N letter) alphabet, to encrypt the message $P_1 P_2 \cdots P_L$ we set $C_1 = P_1 + b_0 \pmod{N}$ and $C_i = P_i + P_{i-1} \pmod{N}$ for $i \geq 2$.

For example, to encrypt MATH using the key b_0 =G, we append G to the beginning of our message, obtaining GMAT, then add this, modulo 27, to our original message character by character. Numerically this is

$$\begin{array}{cccc} 13 & 1 & 20 & 8 \\ 7 & 13 & 1 & 20 \\ \hline 20 & 14 & 21 & 1 \end{array}$$

so that the ciphertext is TNUA.

Use the Vigenère cipher with key b_0 =Q to encrypt the message TRAITOR.

Exercise 3. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $(a, n) = 1$. Show that if $r \equiv s \pmod{\varphi(n)}$ then $a^r \equiv a^s \pmod{n}$.

Exercise 4. Suppose that p and q are distinct primes, $n = pq$ and $e \equiv 1 \pmod{\varphi(n)}$. Show that if $(a, n) \neq 1$ then we still have $a^e \equiv a \pmod{n}$. [*Suggestion:* It suffices to assume $0 \leq a < n$ (why?). If $a \neq 0$ we can then assume further that $a = p^r k$ with $(k, q) = 1$ (why?).]