Number Theory I
Spring 2018

Assignment 8.1
Due March 7

Exercise 1. Use the Repeated Squaring algorithm to compute the following.

a. The remainder when 619^{55} is divided by 733.

b. The remainder when 1073^{145} is divided by 1537.

c. The remainder when $2018^{13772000000}$ is divided by 2049. [*Suggestion:* Check to see if Euler's theorem can help you reduce the size of the exponent.]

Exercise 2. Recall that we deduced Wilson's theorem,

$$(p-1)! \equiv -1 \pmod{p} \quad \Leftrightarrow \quad p \text{ is prime},$$

by multiplying together all of the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ and interpreting the result as a congruence. What happens if we do the same thing with an arbitrary $n \in \mathbb{N}$? That is, can we determine the congruence class

$$P + n\mathbb{Z} = \prod_{g \in (\mathbb{Z}/n\mathbb{Z})^\times} g?$$

Formulate a conjecture about $P + n\mathbb{Z}$ by computing it for $n \leq 100$. Be as precise as you can. [*Suggestion:* Use a computer.]