NUMBER THEORY I
SPRING 2018

ASSIGNMENT 9.2
DUE MARCH 21

Exercise 1. Prove the result referenced in the footnote of the previous assignment. Specifically, show that if $m, n \in \mathbb{N}$ are coprime and $d \in \mathbb{N}$, then $d|mn$ if and only if there exist unique $d_1, d_2 \in \mathbb{N}$ so that $d_1|m$, $d_2|n$ and $d = d_1 d_2$. [*Suggestion:* For existence, show that $d_1 = (d, m)$, $d_2 = (d, n)$ work; use Bézout's lemma. For uniqueness, show that if $a|m$ and $b|n$, then $(a, b) = 1$; use Bézout's lemma again.]

Exercise 2. Let F be field in which $-1 \neq 1$.

a. Show that if $r \in F$ solves $x^2 + 1 = 0$, then r has (multiplicative) order 4.

b. Show that $x^2 + 1 = 0$ has a solution in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$. [*Suggestion:* Consider the equation $x^4 - 1 = 0$.]

Exercise 3. Let p be an odd prime and g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$.

a. Show that $g^{(p-1)/2}$ is a solution of $x^2 - 1 = 0$. Conclude that $g^{(p-1)/2} = -1 + p\mathbb{Z}$.

b. Provide an alternate proof of Wilson's theorem by observing that

$$(p-1)! + p\mathbb{Z} = g^{1+2+\cdots+(p-1)}$$

and using part **a**.