Number Theory Fall 2009
Homework 3
Due: Wed. Sep. 16, start of class

Reading

Stillwell goes pretty quickly through the material on groups, as will we. Therefore, if you are not familiar with them already, you may want to do a little reading on your own (say pickup a book on algebra from the library that looks nice, or google introduction to group theory) to see more examples.

Written assignment

3.2 Congruence classes and their arithmetic

Exercise 3.1. *Exercises 3.1.3, 3.1.4 (no proof needed for 3.1.4).*

Exercise 3.2. *Write* $a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$. *Prove that a is divisible by 11 if and only if the sum of the odd digits (a_k where k odd) minus the sum of the even digits (a_k where k even) is. (Hint: see Exercises 3.2.2, 3.2.3.)*

(Optional, i.e., 0 points) There are several methods for testing divisibility by 7, though they are more complicated. Can you figure any out?

Exercise 3.3. *Write down addition and multiplication tables for* $\mathbb{Z}/6\mathbb{Z}$.

3.3 Inverses mod p

Definition 3.1. *Let G be a set with a* binary operation $\cdot$. , *i.e., $\cdot$ is a function from $G \times G \to G$, expressed as $(g, h) \mapsto g \cdot h$. If G satisfies the following properties,*

(i) $\cdot$ is associative: $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ for all $g, h, k \in G$;

(ii) there is an identity $1 \in G$ *such that $1 \cdot g = g \cdot 1 = g$ for all $g \in G$;*

(iii) every $g \in G$ has an inverse g^{-1} *such that $g^{-1} \cdot g = g \cdot g^{-1} = 1$;*

then we say $(G, \cdot)$ (or just G) is a **group**. *If (i) through (iii) and*

(iv) $\cdot$ is commutative: $g \cdot h = h \cdot g$ for all $g, h \in G$

also hold, we say $(G, \cdot)$ (or just G) is an **abelian group**. *When the operation is understood, we typically write gh for $g \cdot h$.*

Exercise 3.4. *Rewrite what properties (i) through (iv) mean when our operation is written as $+$ (called additive) and not $\cdot$ (called multiplicative). Which properties fail for $(\mathbb{N}, +)$? What is the (additive) inverse of $8\mathbb{Z} + 5$ in the group $(\mathbb{Z}/8\mathbb{Z}, +)$?*

Exercise 3.5. *Prove $(\mathbb{Z}/n\mathbb{Z})^\times$ is a finite abelian group. You may take for granted that multiplication is well defined on $\mathbb{Z}/n\mathbb{Z}$ (from the previous section) and associative, though you should say a sentence about why it is well defined on $(\mathbb{Z}/n\mathbb{Z})^\times$.*