Homework 2

MATH 301/601

Test #2 is on Monday, March 3

Instructions. *Read the Homework Guide to make sure you understand how to successfully complete the assignment.*

Exercise 1. For each pair of integers in Exercise 9, HW1, write the gcd as a linear combination.

Exercise 2. Find all $n \in \mathbb{Z}$ satisfying each of the following equations.

(a) $3n \equiv 2 \pmod{7}$

(b) $5n + 1 \equiv 13 \pmod{23}$

(c) $5n + 1 \equiv 13 \pmod{26}$

(d) $5n \equiv 1 \pmod{6}$

(e) $3n \equiv 1 \pmod{6}$

Definition 1. An *equivalence relation* on a set S is a binary relation $\sim$ that is:

(i) *reflexive*, that is, $a \sim a$ for all $a \in S$;

(ii) *symmetric*, that is, $a \sim b$ implies $b \sim a$ for all $a, b \in S$; and

(iii) *transitive*, that is, $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in S$.

Exercise 3. Let $n \in \mathbb{N}$. Prove that equivalence modulo n is an equivalence relation on $\mathbb{Z}$.

***Exercise 4.** Let $n \in \mathbb{N}$. Prove that given any $m \in \mathbb{Z}$ there exists a unique element $a \in \{0, 1, 2, \ldots, n-1\}$ such that $m \equiv a \pmod{n}$. (Hint: Use the division algorithm.)

Exercise 5. Let $n \in \mathbb{N}$, and let $a, b \in \mathbb{Z}$. Prove that if $a \equiv b \pmod{n}$, then

$$\gcd(a, n) = \gcd(b, n).$$

***Exercise 6.** Let $n \in \mathbb{N}$ with $n > 1$, and let $a \in \mathbb{Z}$.

(a) Prove that if $\gcd(a, n) = 1$ and $b, c \in \mathbb{Z}$ such that $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

(b) Give an example of integers n, a, b, c such that $a \not\equiv 0 \pmod{n}$, $b \not\equiv c \pmod{n}$, and $ab \equiv ac \pmod{n}$.

****Exercise 7.** Let $m, n \in \mathbb{N}$ be relatively prime, and let $a, b \in \mathbb{Z}$. Prove that there exists $x \in \mathbb{Z}$ such that

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

(Hint: Start by writing 1 as a linear combination of m and n.)

Exercise 8. Let $n \in \mathbb{N}$.

(a) Prove that $10^n \equiv 1 \pmod{9}$. (There are numerous ways to see this. One way is to use induction.)

(b) (Divisibility by 9) Define $h\colon \mathbb{N} \to \mathbb{Z}$ by

$$h(n) = \sum_{j=0}^{k} a_j,$$

where

$$n = \sum_{j=0}^{k} (a_j \cdot 10^j).$$

In words, $h(n)$ is the sum of the digits of n when written in base 10. For example, if $n = 27301$, then $h(n) = 1 + 0 + 3 + 7 + 2 = 13$. Prove the following statement: Let $n \in \mathbb{N}$. Then, $9 \mid n$ if and only if $9 \mid h(n)$. (Hint: You will have to use part (a).)

***Exercise 9.** Let $n \in \mathbb{N}$.

(a) Prove that $10^n \equiv (-1)^n \pmod{11}$. (Hint: use induction.)

(b) (Divisibility by 11) Define $f\colon \mathbb{N} \to \mathbb{Z}$ by

$$f(n) = \sum_{j=0}^{k} (-1)^j a_j,$$

where

$$n = \sum_{j=0}^{k} (a_j \cdot 10^j).$$

In words, $f(n)$ is the alternating sum of the digits of n when written in base 10. For example, if $n = 27301$, then $f(n) = 1 - 0 + 3 - 7 + 2 = -1$. Prove the following statement: Let $n \in \mathbb{N}$. Then, $11 \mid n$ if and only if $11 \mid f(n)$. (Hint: You will have to use part (a).)

Exercise 10. Let D_4 denote the set of all rigid motions of a square.

(a) Describe all the elements of D_4. (You do not need to prove you have them all, but do your best. We will do an official count in class at a later date.)

(b) Every rigid motion of the square permutes its vertices. Describe a permutation of the vertices of the square that cannot be obtained via a rigid motion. (It will be helpful to know something about distances, so you may assume the Pythagorean theorem: $a^2 + b^2 = c^2$, where a and b are the lengths of the legs of a right triangle and c is the length its hypotenuse.)

***Exercise 11.** Let D_∞ denote the set of bijections $\{f\colon \mathbb{Z} \to \mathbb{Z} : |f(n) - f(m)| = |n - m|\}$. Alternatively, D_∞ is the set of rigid motions of the tick-mark pattern shown in Figure 1.

(a) Describe the elements of D_∞. (Note there are infinitely many.)

(b) Find a finite generating set for D_∞.

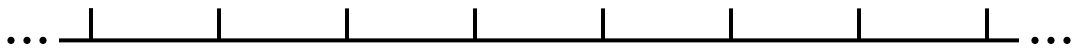

Figure 1: A pattern whose set of rigid motions is D_∞. The dots indicate that the pattern repeates indefinitely to the right and to the left.

****Exercise 12.** Let $S_{2\infty}$ denote the set rigid motions of the Frieze pattern shown in Figure 2.

(a) Describe the elements of $S_{2\infty}$. (Note there are infinitely many.)

(b) Find a finite generating set for $S_{2\infty}$.

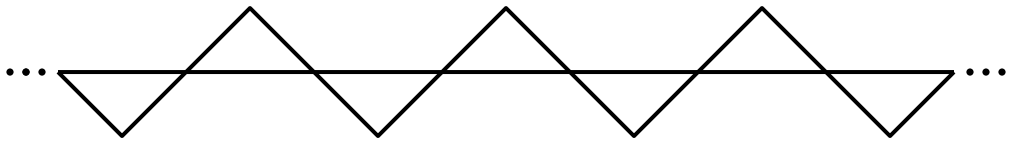

Figure 2: A frieze pattern. The dots indicate that the pattern repeates indefinitely to the right and to the left.

Exercises 13–16 each ask you to establish that a given set with an associated binary operation is a group. In each case, you can assume that the operation is associative, so you only need to establish an identity element and inverses.

Exercise 13. Complete Exercise 2 in Section 3.5 of the textbook.

Exercise 14. Recall that the complex numbers are the set $\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$, where $i^2 = -1$. For $z = x + iy \in \mathbb{C}$, we let $\bar{z} = x - iy$ and $|z| = \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$. Let $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$, so that $\mathbb{T}$ is the unit circle. Prove that $\mathbb{T}$, equipped with complex multiplication, is a group.

Exercise 15. Prove that the set of matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

is a group under matrix multiplication. (This group is called the *Heisenberg group*. It is important in many areas, including quantum physics and robotic motions.)

***Exercise 16.** Let $p \in \mathbb{N}$. Let $\mathrm{GL}(2,p)$ denote the set of non-zero-determinant 2×2 matrices with entries in $\mathbb{Z}_p$, that is,

$$\mathrm{GL}(2,p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}_p \text{ and } ad - bc \neq \bar{0} \right\}.$$

Prove that $\mathrm{GL}(2,p)$ is a group if and only if p is prime. (Hint: the formula for the inverse of a 2-by-2 matrix you learned in linear algebra is still going to be valid! But be careful: what is a fraction?)

Exercise 17. Let G be a group. Prove that for any $g_1, g_2, \ldots, g_n \in G$, the inverse of $g_1 g_2 \cdots g_n$ is $g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$. (This is an induction problem.)

Exercise 18. Let $U(n)$ be the group of units in $\mathbb{Z}_n$, i.e., $U(n) = \{\bar{a} : \gcd(a,n) = 1\}$ equipped with multiplcation modulo n. If $n > 2$, prove that there is an element $k \in U(n)$ such that $k^2 = \bar{1}$ and $k \neq \bar{1}$.

Exercise 19. Show that if $a^2 = e$ for every element a in a group G, then G is abelian.

Exercise 20. Show that if G is a finite group of even order, then there exists $a \in G$ such that a is not the identity and $a^2 = e$.

***Exercise 21.** Let G be a group. Prove that if $(ab)^2 = a^2 b^2$ for all a and b in G, then G is abelian.