

HOMEWORK 2: MATH 124 (NUMBER THEORY)

1. EXERCISES

Exercise 1.1. Fix $n, a, b, c, d \in \mathbb{Z}$ with $n > 1$. Prove the following basic properties of the congruence notation introduced in class.

- (1) If $a \cong b \pmod{n}$ then $b \cong a \pmod{n}$ (2 pts).
- (2) If $a \cong b \pmod{n}$ and $c \cong d \pmod{n}$ then $ax + cy \cong bx + dy \pmod{n}$ for all $x, y \in \mathbb{Z}$ (2 pts).

Exercise 1.2. Let $n \in \mathbb{Z}$ with $n > 1$, we recall that $(\mathbb{Z}/n\mathbb{Z})^*$ denotes the subset of residue classes $\{a \in \mathbb{Z} \text{ such that } 0 \leq a \leq n-1\} = \mathbb{Z}/n\mathbb{Z}$ which admit an inverse mod n . We let $|(\mathbb{Z}/n\mathbb{Z})^*|$ denote the size of this subset.

- (1) Compute $|(\mathbb{Z}/n\mathbb{Z})^*|$ for $n = 36, 45, 72$ (3 pts).
- (2) Write down the residue classes which lie in $(\mathbb{Z}/n\mathbb{Z})^*$ for $n = 36$ explicitly (3 pts).

Exercise 1.3. Using modular arithmetic, we showed in class that if we have a number N with digits $(a_n a_{n-1} \cdots a_1 a_0)$ then we have that

$$9 \mid N \Leftrightarrow 9 \mid \sum_{i=0}^n a_i,$$

by taking the decimal expansion $N = \sum_{i=0}^n (10)^i a_i$ modulo 9. In this exercise, we explore a generalization of this principle. First, we note that the powers of 10 are a bit of an arbitrary choice. In fact, for a fixed $b \in \mathbb{N}$ such that $b > 1$, we have the following.

- (1) For a fixed $N \in \mathbb{N}$ such that $N > 0$. Show that there exists a unique integer $n \geq 0$ and $a_i \in \mathbb{Z}$ for all $i = 0, 1, \dots, n$ such that

$$N = \sum_{i=0}^n b^i a_i$$

and $0 \leq a_i < b$ and $a_n \neq 0$ (Hint: Look at a_0 and factor b out of the higher order terms. What does the resulting statement look like?) (4 pts).

We denote the unique decomposition of N given by the a_i as $(a_n a_{n-1} \cdots a_1 a_0)_b$ and refer to it as the number N in base b .

- (2) Show that, for all $b > 1$ and $N = (a_n a_{n-1} \cdots a_1 a_0)_b$ in base b , we have that

$$(b-1) \mid N \Leftrightarrow (b-1) \mid \sum_{i=0}^n a_i$$

and

$$(b+1) \mid N \Leftrightarrow (b+1) \mid \sum_{i=0}^n (-1)^i a_i$$

(3 pts).

Exercise 1.4. As discussed in class, for $a \in (\mathbb{Z}/n\mathbb{Z})^*$ with $n > 1$ an integer, there exists a unique residue class $a' \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $aa' \cong 1 \pmod{n}$ and a' is called the inverse mod n . For the following a and n , determine whether $a \in \mathbb{Z}/n\mathbb{Z}$ lies in $(\mathbb{Z}/n\mathbb{Z})^*$ (In other words, it is invertible) and if it is compute its inverse.

- (1) $a = 7$ and $n = 20$ (2 pts).

- (2) $a = 11$ and $n = 26$ (2 pts).
- (3) $a = 43$ and $n = 137$ (2 pts).
- (4) $a = 18$ and $n = 9213$ (3 pts).

Exercise 1.5. Show that $n^7 - n$ is divisible by 42 for all $n \in \mathbb{Z}$ (Hint: break the problem up into the prime factors of 42) (5 pts).