

# Modular Arithmetic 1

Andres Buritica Monroy

## 1 Residue Classes

Let  $n$  be a nonzero integer. For integers  $a$  and  $b$ , we say that

$$a \equiv b \pmod{n} \iff n \mid b - a.$$

Notice that for fixed values of  $a$  and  $n$ , infinitely many values of  $b$  satisfy  $a \equiv b \pmod{n}$ .

The numbers  $0, 1, \dots, n-1$  are called the *least residues mod  $n$* . Every integer is congruent to a unique least residue mod  $n$ .

- Find the least residue of  $81 \bmod 7$ .
- Find the least residue of  $-1 \bmod 2023$ .

## 2 Operations

Prove that if  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$  then

- $a + c \equiv b + d \pmod{n}$
- $a - c \equiv b - d \pmod{n}$
- $ac \equiv bd \pmod{n}$
- $a^m \equiv b^m \pmod{n}$  for any nonnegative integer  $m$ .

Let  $a, n, x, y$  be integers such that  $a \mid x, y$ .

- Find a counterexample to the statement that if  $x \equiv y \pmod{n}$  then  $x/a \equiv y/a \pmod{n}$ .
- Find some  $m$  in terms of  $a$  and  $n$  such that you can guarantee that  $x/a \equiv y/a \pmod{m}$ .

## 3 Multiplication by coprime residues

Let  $a$  and  $n$  be positive integers such that  $\gcd(a, n) = 1$ .

- Prove that if  $\gcd(y, n) = 1$  then there exists some  $x$  such that  $ax \equiv y \pmod{n}$ .
- Prove that  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

This last dot point is known as Euler's Theorem. If  $n = p$  is prime, then  $\varphi(p) = p - 1$  so  $a^{p-1} \equiv 1 \pmod{p}$ , which is known as Fermat's Little Theorem.

## 4 Problems

1. Find all primes  $p$  such that  $29^p + 1$  is a multiple of  $p$ .
2. Let  $n > 6$  be an integer such that  $n - 1$  and  $n + 1$  are both prime. Prove that  $720 \mid n^2(n^2 + 16)$ .
3. Let  $a_1 = 20$ ,  $a_2 = 23$ . For  $n \geq 1$ , let  $a_{n+1}$  be the least residue of  $a_n + a_{n-1} \pmod{100}$ . Find the least residue of  $a_1^2 + \cdots + a_{2023}^2 \pmod{8}$ .
4. Let  $n$  be a positive integer. All numbers  $m$  which are coprime to  $n$  satisfy  $m^2 \equiv 1 \pmod{n}$ . Find the maximum possible value of  $n$ .
5. Find all primes  $p$  such that  $2^{p-2} + 1$  is a multiple of  $p$ .
6. Show that 30 is the greatest common divisor of all numbers of the form  $2^{3n} + 5^{n+1} + 3^{n+2}$ , where  $n \in \mathbb{N}$ .
7. Define the sequence  $a_n = 2^n + 3^n + 6^n - 1$ ,  $n \in \mathbb{N}$ . Find all primes which do not divide  $a_n$  for any  $n$ .

## 5 Homework

1. Let  $S$  be a subset of the set of numbers  $\{1, 2, 3, \dots, 2023\}$  such that if  $a, b$  are in  $S$ , then  $23 \nmid a + b$ . What is the maximum possible size of  $S$ ?
2. Prove that every positive integer has at least as many divisors which are  $1 \pmod{4}$  as divisors which are  $3 \pmod{4}$ .
3. Does one of the first  $10^8 + 1$  Fibonacci numbers end with four zeroes?