Number Theory I - Modular Arithmetic

Billy Rieger

1 What are Mods?

You can think of mods essentially as remainders: $a \pmod{n}$ is the same as the remainder when a is divided by n for integers a and natural numbers n. The notation $a \pmod{n}$ means that we are taking a modulo n. This may not seem entirely useful, but trust me, it definitely is.

2 Stuff about Mods

In modulo n, we say that integers a and b are contruent if and only if their difference is divisible by n. Stated more formally, $a \equiv b \pmod{n}$ iff $n|a-b$. $\equiv$ is read as "is equivalent to" and $n|a-b$ is read as "n divides a minus b."

2.1 Properties

1. $a \equiv a$. (Reflexive)
2. If $a \equiv b$ then $b \equiv a$. (Symmetric)
3. If $a \equiv b$ and $b \equiv c$ then $a \equiv c$. (Transitive)
4. If $a \equiv b$ and $c \equiv d$ then $a + c \equiv b + d$.
5. If $a \equiv b$ and $c \equiv d$ then $a \cdot c \equiv b \cdot d$.
6. If $a \equiv b$ and $c \equiv d$ then $a - c \equiv b - d$.
7. If $a \equiv b$ then $a^c \equiv b^c$.

Be sure to notice that division is NOT included anywhere in the properties list. I'll explain why in a bit.

2.2 Inverses

An inverse of a modulo n in an integer b such that

$$ab \equiv 1 \pmod{n}$$

That is,

$$a^{-1} \equiv b \pmod{n}$$

a^{-1} only exists if a and n are relatively prime - they share no common factors other than 1. For example, 4^{-1} exists modulo 9 because 4 and 9 are relatively prime. $4 \cdot 7 = 28 \equiv 1 \pmod{9}$, so $4^{-1} \equiv 7 \pmod{9}$. However, since 6 and 9 are not relatively prime, $6^{-1} \pmod{9}$ does not exist because there is no integer b that satisifies $6b \equiv 1 \pmod{9}$.

This explains why division was not included in the list. If a and b are relatively prime,

$$\frac{a}{b} \equiv a \cdot \frac{1}{b} \equiv a \cdot b^{-1}$$

If b^{-1} doesn't exist in a given mod, division might not work. Division can still work if a and b are not relatively prime, though. $\frac{2}{4} \pmod{14}$ exists, but $\frac{1}{2} \pmod{14}$ does not. Note that you can also think of fractions as saying $\frac{a}{b} \equiv c \pmod{n} \Rightarrow a \equiv bc \pmod{n}$.

3 Chinese Remainder Theorem

The Chinese Remainder Theorem is a useful tool to help solve some modular arithmetic problems. The theorem states that, given two integers m and n that are relatively prime, there exist infinitely many integers x such that

$$x \equiv a \pmod{m}$$

and

$$x \equiv b \pmod{n}$$

for any integers a and b. Also, all solutions x are equivalent mod mn.

The theorem only states that such integers x exist, not how to find them!

4 Bézout's Identity

A Diophantine equation is simply an equation where the variables are restricted to be integers only. Bézout's identity is concerned with finding the solutions to ones of the form

$$ax + by = c$$

where a and b are relatively prime. If one can find a single solution (x, y), then all other solutions are given by

$$(x + kb, y - ka)$$

where k is an integer.

5 Problems

1. How many pairs of positive integers (a, b) are there such that $gcd(a, b) = 1$ and

   $$\frac{a}{b} + \frac{14b}{9a}$$

   is an integer?

2. Find the remainder when

   $$9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{999\ 9\text{'s}}$$

   is divided by 1000.

3. The vertices of a regular nonagon (9-sided polygon) are to be labeled with the digits 1 through 9 in such a way that the sum of the numbers on every three consecutive vertices is a multiple of 3. Two acceptable arrangements are considered to be indistinguishable if one can be obtained from the other by rotating the nonagon in the plane. Find the number of distinguishable acceptable arrangements.

4. Let $S = \{2^0, 2^1, 2^2, \ldots, 2^{10}\}$. Consider all possible positive differences of pairs of elements of S. Let N be the sum of all of these differences. Find the remainder when N is divided by 1000.

5. Let R be the set of all possible remainders when a number of the form 2^n, n a nonnegative integer, is divided by 1000. Let S be the sum of the elements in R. Find the remainder when S is divided by 1000.

6. There are N permutations $(a_1, a_2, ..., a_{30})$ of $1, 2, \ldots, 30$ such that for $m \in \{2, 3, 5\}$, m divides $a_{n+m} - a_n$ for all integers n with $1 \leq n < n+m \leq 30$. Find the remainder when N is divided by 1000.

Sources: AMC 12, AIME, (Mod properties list stolen from Sam Rush who stole them from Brian Hamrick)