Congruence, part 1

Lecture 3 Jan 24, 2021

Rings and Fields

- Before we discuss the concept of **congruence** in Number Theory and its applications,

lets review our knowledge of numbers!

- Natural numbers $\mathbb{N}$ = {0, 1, 2, 3, … }. We have addition and multiplication:

$$\boxed{a, b \in \mathbb{N} \rightarrow a + b\,, a \times b \in \mathbb{N}}$$

- Integers $\mathbb{Z}$ = {… -3, -2, -1, 0, 1, 2, 3, … }. We have addition, subtraction and multiplication:

$$\boxed{a, b \in \mathbb{Z} \rightarrow a + b, a - b, a \times b \in \mathbb{Z}}$$

Rings and Fields

- Rational numbers $\mathbb{Q} = \left\{\frac{p}{q} : p, q \in \ \mathbb{Z}\right\}$ $and\ \mathbb{R}$.

We have addition, subtraction, multiplication, and division:

$$a, b \in\ \mathbb{Q}\ or\ \mathbb{R}\ \rightarrow\ \ a + b, a - b, a \times b\ \in \mathbb{Q}\ or\ \mathbb{R} \qquad \frac{\mathrm{a}}{\mathrm{b}} \in \mathbb{Q}\ or\ \mathbb{R}\ if\ b \neq 0$$

- $\mathbb{N}$ is a **monoid** (has only addition and multiplication)
- $\mathbb{Z}$ is a **ring** (has addition/subtraction and multiplication)
- $\mathbb{Q}\ and\ \mathbb{R}$ are a **fields** (have addition/subtraction and multiplication/divission)

Rings and Fields

- There are other kind of objects that have such properties

- Example. Polynomials with coefficients in $\mathbb{R}$

$$P = \{\, p(x) = a_n x^n + a_{n-1}\, x^{n-1} + \ \ldots + a_0 \ : \ \ a_i \in \ \mathbb{R}\}$$

Polynomials can be added, subtracted, multiplied, but if you try to divide them you often don't get a polynomial

- So just like $\mathbb{Z}$, the set of all polynomials makes a ring

- Number Theory is partly about studying sets that have properties like usual numebrs

Congruence

- **Fix** a natural number n > 1
- Every other integer a can be uniquely written as $a = x\,n + r$ such that $0 \leq r \leq n - 1$
- r is the remainder, x is the quotient
- We are going to care only about the remainder r of any integer a <u>modulo</u> n
- Two numbers a and b are <u>congruent modulo n</u> if they have the same remainder
- We write $\underline{a \equiv b \ \ modulo\ n}$
- Examples. $2 \equiv 0 \ \ modulo\ 2$ $\quad$ $10 \equiv 4 \ \ modulo\ 3$ $\quad$ $-1 \equiv 5 \ \ modulo\ 6$

Congruence

- **Little Lemma.** $a \equiv b \;\; modulo\, n \;\; \Leftrightarrow \;\; n \mid (a-b)$ **i.e.** $a - b$ is divisible by n

Proof. $a \equiv b \;\; modulo\, n \;\; \Leftrightarrow \;\; a$ and b have the same remainder r modulo n

$\Leftrightarrow a = xn + r \;\; and \;\; b = yn + r \Leftrightarrow a - b = (x-y)n \Leftrightarrow \;\; a - b$ is divisible by n

- $10 \equiv 4 \;\; modulo\ 3$ because $3 \mid (10-4) = 6$
- -1 $\equiv 5 \;\; modulo\ 6$ because $6 \mid (5-(-1)) = 6$
- <u>FACT:</u> Each number is <u>equivalent</u> to one of <u>n numbers {0, 1, 2, …, n-1}</u> modulo n

The Ring structure

- **Lemma**. The set of numbers modulo n has a ring structure (addition, subtraction, multiplication)
- Multiplication: If $\underline{a \equiv a' \ mod\, n}$ and $\underline{b \equiv b' \ mod\, n}$ then $\underline{ab \equiv a'b' \ mod\, n}$
- Ex. $\underline{3 \equiv 10 \ mod\, 7}$ and $\underline{-2 \equiv 5 \ mod\, 7}$ then $\underline{-6 = 3\times(-2) \equiv 10\times 5 = 50 \ mod\, 7}$
- Proof: We have $(ab - a'b') = a(b - b') + b'\,(a - a')$. Since n divides the right-hand side, it also divides the left-hand side. So $ab \equiv a'b' \ mod\, n$

- Multiplication: If $a \equiv a' \ mod\, n$ and $b \equiv b' \ mod\, n$ then $a \pm b \equiv a' \pm b' \ mod\, n$
- Proof: $(a \pm b) - (a' \pm b') = (a - a') \pm (b - b')$. Since n divides the right-hand side, it also divides the left-hand side.

Applications

- **Q1**. Find the remainder of $3^n + 1$ divided by 4

- Answer: $3 \equiv -1 \; mod \; 4.$ So $3^n + 1 \equiv (-1)^n + 1 \quad mod \; 4.$

- If n is odd, then $(-1)^n + 1 = 0$. So remainder is 0 (it is divisible by 4)

- If n is even, then $(-1)^n + 1 = 2$. So remainder is 2.

Examples

- **Q2.** Prove that $a^2 - 1$ is divisible by 8 for all odd integers a.

(Last time we proved it by induction)

New Solution. Every odd integers is congruent to 1, 3, 5, or 7 modulo 8.

So it is enough to check these 4 numbers.

$$1^2 - 1 = 0$$
$$3^2 - 1 = 8$$
$$5^2 - 1 = 24 = 3 \times 8$$
$$7^2 - 1 = 48 = 6 \times 8$$

All are divisible by 8. Done.

You can also solve all of the following question this way

- Prove that $5^{2n+1} + 2^{2n+1}$ is divisible by 7 for all n ≥ 0.
- Prove that $a^4 - 1$ is divisible by 16 for all odd integers a.
- Prove that $n^3 + 2n$ is divisible by 3 for all integers n.
- Prove that $17n^3 + 103n$ is divisible by 6 for all integers n.
- Prove that $2^n + 1$ is divisible by 3 for all odd integers n

* Questions are taken from https://www.math.waikato.ac.nz/~hawthorn/MATH102/InductionProblems.pdf

Lets do one of them

- **Q3.** Prove that $17n^3 \; + \; 103n$ is divisible by 6 for all integers n.
- **Solution.** Every integer is congruent to one of {-2, -1, 0, 1, 2, 3} modulo 6

So it is enough to check the claim for $n = -2, -1, 0, 1, 2, 3$

- $n = 0 \;\Rightarrow 17n^3 + 103\,n = 0$
- $n = \pm 1 \;\Rightarrow 17n^3 + 103\,n = \pm(17 + 103) = \pm 120 = \; \pm 20 \times 6$
- $n = \pm 2 \;\Rightarrow 17n^3 + 103\,n = \; \pm(17 \times 8 + 103 \times 2) = \pm 342 = \; \pm 6 \times 57$
- $n = 3 \;\Rightarrow 17n^3 + 103\,n = 17 \times 27 + 309 = 768 = 256 \times 3$

Some rule you might have seen before

- **Q4.** An integer is divisible by 9 if and only if the sum of its digits is divisible by 9.
- **Proof.** If x is an integer with digits $a_n\ a_{n-1} \dots a_0$, that means

$x = \mathrm{a}_0 + 10\ \mathrm{a}_1 + 100\ \mathrm{a}_2 + \ \dots + 10^{\mathrm{n}}\ \mathrm{a}_{\mathrm{n}}$

Since $10 \equiv 1\ mod\ 9$, we have $10^n \equiv 1^n = 1\ \ mod\ 9$

We conclude that $x \equiv a_0 + \ \dots . + a_n\ \ mod\ 9$

So x is divisible by 9 if and only if $a_0 + \ \dots . + a_n$ is divisible by 9