Lecture 03: Ring of integers modulo n

Wednesday, April 4, 2018 1:12 PM

We were proving:

<u>Basic Properties of Congruence Arithmetic.</u>

(1) $a \equiv a \pmod{n}$; $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$;

$$\left.\begin{array}{l} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{array}\right\} \Rightarrow a \equiv c \pmod{n}.$$

(2) $$\left.\begin{array}{l} a_1 \equiv a_2 \pmod{n} \\ b_1 \equiv b_2 \pmod{n} \end{array}\right\} \Rightarrow a_1+b_1 \equiv a_2+b_2 \pmod{n};$$

(3) $$\left.\begin{array}{l} a_1 \equiv a_2 \pmod{n} \\ b_1 \equiv b_2 \pmod{n} \end{array}\right\} \Rightarrow a_1b_1 \equiv a_2b_2 \pmod{n};$$

(4) $a \equiv r \pmod{n}$ and $0 \le r < a \Leftrightarrow r$ is the remainder of a divided by n.

<u>Pf</u> (3) (Continue) $a_1 - a_2 = nk$, $b_1 - b_2 = n\ell$ for some $k, \ell \in \mathbb{Z}$.

$$a_1b_1 - a_2b_2 = a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2 = (a_1-a_2)b_1 + a_2(b_1-b_2)$$
$$= nkb_1 + a_2n\ell = n(\underbrace{kb_1 + a_2\ell}_{\text{in } \mathbb{Z}}).$$

So $a_1b_1 \equiv a_2b_2 \pmod{n}$.

(4) $(\Rightarrow)$ By definition, $r \in \{0,1,\ldots,n-1\}$ and $a = nq + r$.

And so $n \mid a-r$; therefore $a \equiv r \pmod{n}$.

$(\Leftarrow)$ Suppose $r \in \{0,1,\ldots,n-1\}$ and $a \equiv r \pmod{n}$. Then

$\exists q \in \mathbb{Z}$ s.t. $a-r=nq$. Therefore

(1) $a=nq+r$ (2) $0 \leq r < n$. Thus, by the uniqueness part of the division algorithm, r is the remainder of a divided by n. $\blacksquare$

Ex. Let $n = 124567932$. Find the remainder of n divided by 9. What is the remainder of n divided by 11?

Solution. First we prove by induction on m that

$10^m \equiv 1 \pmod 9$ and $10^m \equiv (-1)^m \pmod{11}$.

Base of induction. $10^0 = 1 \equiv (1)^0 \pmod 9$ and

$10^0 = 1 \equiv (-1)^0 \pmod{11}$.

Induction step. $10^{m+1} = (10^m)(10) \equiv (1)(1) \pmod 9$

$\boxed{\text{by induction hypothesis } 10^m \equiv 1 \pmod 9 \text{ and } 10 \equiv 1 \pmod 9}$

$10^{m+1} = (10^m)(10) \equiv (-1)^m(-1) \pmod{11}$

$\boxed{\text{by induction hypothesis } 10^m \equiv -1 \pmod{11} \quad 10 \equiv -1 \pmod{11}}$

Lecture 03: Ring of integers modulo n

Friday, April 6, 2018 4:45 PM

just adding its digits

$124567932 =$

$10^8 \times 1 + 10^7 \times 2 + 10^6 \times 4 + 10^5 \times 5 + 10^4 \times 6 + 10^3 \times 7 + 10^2 \times 9 + 10 \times 3 + 2$

$\equiv 1 + 2 + 4 + 5 + 6 + 7 + 9 + 3 + 2 \equiv 3 \pmod 9$; and so the remainder of n divided by 9 is 3.

alternate signs and add digits

$124567932 \equiv$

$(-1)^8 \times 1 + (-1)^7 \times 2 + (-1)^6 \times 4 + (-1)^5 \times 5 + (-1)^4 \times 6 + (-1)^3 \times 7 + (-1)^2 \times 9 + (-1) \times 3 + 2 \equiv$

$1 - 2 + 4 - 5 + 6 - 7 + 9 - 3 + 2 \equiv 5 \pmod{11}$. So remainder is 5. ∎

<u>Proposition.</u> $(\mathbb{Z}_n, \oplus, \odot)$ is a unital commutative ring.

<u>Pf.</u> You have already seen why $(\mathbb{Z}_n, \oplus)$ is an abelian group.

So we will focus on other properties. All the properties can be easily deduced using congruence arithmetic:

$a \oplus b \equiv a + b \pmod n$ and $a \odot b \equiv ab \pmod n$

as $a \oplus b$ is the remainder of $a+b$ divided by n, and $a \odot b$ is the remainder of ab divided by n. So roughly using congruence arithmetic, we can "remove circles".

$(a \oplus b) \odot c \equiv (a \oplus b)\, c \pmod n \equiv (a+b)\, c \pmod n$ (I)

$\boxed{a \oplus b \equiv a+b \pmod n \Rightarrow (a \oplus b)\, c \equiv (a+b)\, c \pmod n}$

Lecture 03: Ring of integers modulo n

Monday, April 2, 2018 11:38 AM

Similarly $\left.\begin{array}{l} a \odot c \equiv ac \pmod{n} \\ b \odot c \equiv bc \pmod{n} \end{array}\right\} \Rightarrow$

$$(a \odot c) + (b \odot c) \equiv ac + bc \pmod{n}$$

On the other hand $(a \odot c) + (b \odot c) \equiv (a \odot c) \oplus (b \odot c) \pmod{n}$.

And so

$$(a+b)\,c \equiv (a \odot c) \oplus (b \odot c) \pmod{n} \qquad \text{(II)}$$

(I), (II) imply $(a \oplus b) \odot c \equiv (a \odot c) \oplus (b \odot c) \pmod{n}$

And so $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$ as they are in $\{0, 1, \ldots, n-1\}$ and congruent modulo n.

One can check other properties of a ring in a similar way. ∎

Ex. Write addition and multiplication tables of $\mathbb{Z}_4$.

Solution:

we denote operations simply by $+$, $\cdot$ from this point on.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

product of two non-zero elements might be 0

there is no 1 in this row. So 2 does not a multiplicative inverse

Lecture 03: Computation in ring of integers mod n

Wednesday, April 4, 2018 11:04 AM

Ex. Find all the zeros of x^2-x in $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

Solution.

x	$x-1$	x^2-x
0	4	0
1	0	0
2	1	2
3	2	1
4	3	2

Only two zeros 0 and 1

x	$x-1$	x^2-x
0	5	0
1	0	0
2	1	2
3	2	0
4	3	0
5	4	2

It has 4 zeros 0, 1, 3, 4.

(This is NOT the same as zeros of polynomials in $\mathbb{C}$.)

As in group theory, we are interested in maps that preserve ring structure.

Def Suppose A and B are rings. $f: A \to B$ is called a <u>ring homomorphism</u> if $f(a_1+a_2) = f(a_1)+f(a_2)$ and $f(a_1a_2) = f(a_1)f(a_2)$.

And a ring homomorphism $f: A \to B$ is called a <u>ring isomorphism</u> if f is a bijection.