Lecture 02: Remainder of division by 3,9, and 11

Sunday, January 13, 2019 9:29 PM

In the previous lecture we saw many examples of rings, and we roughly described rings as new system of numbers. Let's see how these new system of numbers can help us understand the "old" system of numbers better.

$\boxed{Q}$ Find the remainder of 10320192020 divided by 9.

<u>Solution</u>. 10320192020 =

$1\times 10^{10}+0\times 10^{9}+3\times 10^{8}+2\times 10^{7}+0\times 10^{6}+1\times 10^{5}+9\times 10^{4}+$

$2\times 10^{3}+0\times 10^{2}+2\times 10+0$.

Since we want to find the remainder of the above sum-prod. divided by 9, we need to find the "circled"-version in $\mathbb{Z}_9$.

$1\otimes 10^{10}\oplus 0\otimes 10^{9}\oplus 3\otimes 10^{8}\oplus 2\otimes 10^{7}\oplus 0\otimes 10^{6}\oplus 1\otimes 10^{5}\oplus 9\otimes 10^{4}\oplus$

$2\otimes 10^{3}\oplus 0\otimes 10^{2}\oplus 2\otimes 10\oplus 0$. Now notice that $10=1$ in $\mathbb{Z}_9$; and so $10^n=1$ in $\mathbb{Z}_9$ for any $n\in\mathbb{Z}^{\geq 0}$. So we need to find $1\oplus 0\oplus 3\oplus 2\oplus 0\oplus 1\oplus 9\oplus 2\oplus 0\oplus 2\oplus 0$;

we need to add the digits and find its remainder divided by 9.

Lecture 02: Remainder of division by 3, 9, and 11

Sunday, January 13, 2019 11:42 PM

$$\underbrace{\underbrace{\underbrace{\underbrace{1\oplus 3}_{4}\oplus 2}_{6}\oplus 1}_{7}\oplus 2}_{9\,=\,0}\oplus 2 = 2.$$

Since $10=1$ in $\mathbb{Z}_3$, a similar method works for division by 3.

$\boxed{Q}$ Find the remainder of 1032019 2020 divided by 11.

<u>Solution</u>. Similar to the previous question we have to find

$$1\otimes 10^{10}\oplus 0\otimes 10^{9}\oplus 3\otimes 10^{8}\oplus 2\otimes 10^{7}\oplus 0\otimes 10^{6}\oplus 1\otimes 10^{5}\oplus 9\otimes 10^{4}\oplus 2\otimes 10^{3}\oplus 0\otimes 10^{2}\oplus 2\otimes 10\oplus 0$$

in $\mathbb{Z}_{11}$. Notice that $10=-1$ in $\mathbb{Z}_{11}$; and so $10^n=(-1)^n$ in $\mathbb{Z}_{11}$. Hence we need to find $\boxed{\text{units}}$

alternating Signs

$$\underbrace{\underbrace{\underbrace{\overset{+}{0}\oplus \overset{-}{(-2)}\oplus \overset{+}{0}\oplus \overset{-}{(-2)}}_{-4}\oplus\underbrace{\overset{+}{9}\oplus \overset{-}{(-1)}}_{8}}_{4}\oplus\underbrace{\underbrace{\overset{+}{0}\oplus \overset{-}{(-2)}}_{-2}\oplus\underbrace{\overset{+}{3}\oplus \overset{-}{(-0)}\oplus \overset{+}{1}}_{4}}_{2}}_{6}$$

$=6$. So the answer is 6.

<u>Remark</u>. If we end up with a negative number, we need find out what it is in $\mathbb{Z}_n$. For instance $-3=8$ in $\mathbb{Z}_{11}$.

Lecture 02: Direct product of rings

Sunday, January 13, 2019 11:58 PM

Having rings $R_1, \ldots, R_n$, one can construct a new one:

$R_1 \times \cdots \times R_n := \{(x_1, \ldots, x_n) \mid x_i \in R_i \text{ for all } i\}$. (It is called the direct product of R_i's.) We add and multiply componentwise:

$$(x_1, \ldots, x_n) + (x_1', \ldots, x_n') := (\overbrace{x_1 + x_1'}^{\text{in } R_1}, \ldots, \overbrace{x_n + x_n'}^{\text{in } R_n}) \quad \text{and}$$

$$(x_1, \ldots, x_n) \cdot (x_1', \ldots, x_n') := (\underbrace{x_1 x_1'}_{\text{in } R_1}, \ldots, \underbrace{x_n x_n'}_{\text{in } R_n})$$

. If R_i's are unital rings, then $R_1 \times \cdots \times R_n$ is unital.

$$(1_{R_1}, \ldots, 1_{R_n}) \cdot (x_1, \ldots, x_n) = (1_{R_1} \cdot x_1, \ldots, 1_{R_n} \cdot x_n)$$
$$= (x_1, \ldots, x_n)$$
$$(x_1, \ldots, x_n) \cdot (1_{R_1}, \ldots, 1_{R_n}) = (x_1 \cdot 1_{R_1}, \ldots, x_n \cdot 1_{R_n})$$
$$= (x_1, \ldots, x_n).$$

So $(1_{R_1}, \ldots, 1_{R_n})$ is the identity of $R_1 \times \cdots \times R_n$.

Ex. Compute a^2 where $a = \begin{bmatrix} (1,0) & (2,2) \\ (0,2) & (0,1) \end{bmatrix} \in M_2(\mathbb{Z} \times \mathbb{Z}_4)$.

Solution.

$$a^2 = \begin{bmatrix} (1,0)^2 + (2,2)\cdot(0,2) & (1,0)\cdot(2,2) + (2,2)\cdot(0,1) \\ (0,2)\cdot(1,0) + (0,1)\,(0,2) & (0,2)\cdot(2,2) + (0,1)^2 \end{bmatrix}$$

$$= \begin{bmatrix} (1,0) + (0,0) & (2,0) + (0,2) \\ (0,0) + (0,2) & (0,0) + (0,1) \end{bmatrix} = \begin{bmatrix} (1,0) & (2,2) \\ (0,2) & (0,1) \end{bmatrix}$$

Lecture 02: Integer multiple of elements of abelian gp

Monday, January 14, 2019 12:10 AM

A few observations: $(1,0)\cdot(0,1)=(0,0)$; and so $(1,0)$ and $(0,1)$ are zero-divisors in $\mathbb{Z}\times\mathbb{Z}_4$. $(2,2)\cdot(2,2)=(4,0)$ in $\mathbb{Z}\times\mathbb{Z}_4$.

Warning. Here $(a_1,\ldots,a_n)\cdot(b_1,\ldots,b_n)$ should not be confused with the dot prod. of two vertices.

Recall. In group theory you learned what g^n means for g in a group $(G,\cdot)$ and $n\in\mathbb{Z}$.

$$g^n=\begin{cases}\underbrace{g\cdot\cdots\cdot g}_{n \text{ times}} & \text{if } n>0\\ 1 & \text{if } n=0\\ \underbrace{(g^{-1})\cdot\cdots\cdot(g^{-1})}_{-n \text{ times}} & \text{if } n<0\end{cases}$$

; and you have seen its basic properties:

$$\forall g\in G, \forall m,n\in\mathbb{Z},\quad g^m\cdot g^n=g^{m+n} \text{ and } (g^m)^n=g^{mn}. \qquad (*)$$

To observe these equations one can consider various cases based on signs of m and n. Writing these for an abelian group $(R,+)$ we use the notation nx instead;

$$nx=\begin{cases}\underbrace{x+\cdots+x}_{n \text{ times}} & \text{if } n>0\\ 0 & \text{if } n=0\\ \underbrace{(-x)+\cdots+(-x)}_{-n \text{ times}} & \text{if } n<0\end{cases}$$

; and $(*)$ gets translated to

Lecture 02: A homomorphism from Z to a unital ring

Monday, January 14, 2019 8:21 AM

$(n+m)x = nx + mx$ and $n(mx) = (nm)x$. $(*)$

Suppose $(R,+,\cdot)$ is a ring. As $(R,+)$ is an abelian group, $(*)$ holds for it. Notice that $(*)$ cannot be deduced from properties of rings. Here m,n are in $\mathbb{Z}$ and not necessarily in R and nx is not the ring multiplication in R (it is a new notation that we are borrowing from group theory). Hence $(*)$ has nothing to do with distributive and associative properties of operations in R.

<u>Propproposition</u>. Suppose R is a unital ring. Then

$$c:\mathbb{Z}\to R,\quad c(n):=n1_R$$

is a ring homomorphism.

<u>Pf</u>. $c(m+n) = (m+n)1_R \underset{\text{by } (*)}{=} m1_R + n1_R = c(m)+c(n)$

$c(mn) = (mn)1_R \underset{\text{by } (*)}{=} m(n1_R) = m\,c(n)$ (I)

$$c(m) = m1_R = \begin{cases} \overbrace{1_R+\cdots+1_R}^{m \text{ times}} & \text{if } m>0 \\ 0 & \text{if } m=0 \\ \overbrace{(-1_R)+\cdots+(-1_R)}^{-m \text{ times}} & \text{if } m<0 \end{cases} ; \text{ and so}$$

Lecture 02: A homomorphism from Z to a unital ring

Monday, January 14, 2019 8:39 AM

$$c(m)\,c(n) = \begin{cases} (\overbrace{1_R + \cdots + 1_R}^{m \text{ times}})\, c(n) & \text{if } m>0 \\ 0 \cdot c(n) & \text{if } m=0 \\ (\underbrace{(-1_R)+\cdots+(-1_R)}_{-m \text{ times}})\, c(n) & \text{if } m<0 \end{cases}$$

$$= \begin{cases} \overbrace{1_R\cdot c(n) + \cdots + 1_R \cdot c(n)}^{m \text{ times}} & \text{if } m>0 \\ 0 & \text{if } m=0 \\ \underbrace{(-1_R)\, c(n) + \cdots + (-1_R)\, c(n)}_{-m \text{ times}} & \text{if } m<0 \end{cases}$$

$$= \begin{cases} \overbrace{c(n) + \cdots + c(n)}^{m \text{ times}} & \text{if } m>0 \\ 0 & \text{if } m=0 \\ \underbrace{(-c(n)) + \cdots + (-c(n))}_{-m \text{ times}} & \text{if } m<0 \end{cases}$$

$$= m\, c(n) \qquad \text{(II)}$$

(I) and (II) imply $c(mn) = c(m)\,c(n)$. ∎

Let's consider the special case of $R = \mathbb{Z}_n$ and give another interpretation of $c: \mathbb{Z} \to \mathbb{Z}_n$.

Proposition. $c_n : \mathbb{Z} \to \mathbb{Z}_n$, $c_n(x)$ is the remainder of x divided by n, is a ring homomorphism.

Lecture 02: Homomorphism from Z to Zn

Monday, January 14, 2019 8:51 AM

<u>pf.</u> By the previous proposition $c: \mathbb{Z} \to \mathbb{Z}_n$, $c(m) := m\, 1_{\mathbb{Z}_n}$ is a ring homomorphism.

$$m\, 1_{\mathbb{Z}_n} = \begin{cases} \overbrace{1_{\mathbb{Z}_n} \oplus \cdots \oplus 1_{\mathbb{Z}_n}}^{m \text{ times}} & \text{if } m>0 \\ 0 & \text{if } m=0 \\ \overbrace{(-1_{\mathbb{Z}_n}) \oplus \cdots \oplus (-1_{\mathbb{Z}_n})}^{-m \text{ times}} & \text{if } m<0 \end{cases}$$

$$\overset{\substack{\text{add in } \mathbb{Z} \\ \text{and take} \\ \text{the remainder} \\ \text{divided by } n}}{=} \begin{cases} \text{remainder of } m \text{ divided by } n & \text{if } m>0 \\ 0 & \text{if } m=0 \\ \text{remainder of } (-1)(-m) \text{ divided by } n & \text{if } m<0 \end{cases}$$

$= c_n(m)$; and claim follows. ∎

Does the same method works between $\mathbb{Z}_n$ and $\mathbb{Z}_m$?

$\boxed{Q}$ Is $c_{n,m}: \mathbb{Z}_n \to \mathbb{Z}_m$, $c_{n,m}(a) :=$ the remainder of a divided by m a ring homomorphism?

Let's check it for $n=2$ and $m=3$:

$c_{2,3}(0) = 0$, $c_{2,3}(1) = 1$. Does it preserve $+$?

$$\left.\begin{array}{l} c_{2,3}(\underbrace{1+1}_{0}) = c_{2,3}(0) = 0 \\ \qquad\qquad\qquad\qquad\quad \not\parallel \\ c_{2,3}(1) + c_{2,3}(1) = 1+1 = 2 \end{array}\right. \text{ in } \mathbb{Z}_3.$$

No, it does not; and $c_{2,3}$ is not a ring hom.

Lecture 02: Homomorphism between Zn and Zm

Monday, January 14, 2019 9:14 AM

$\boxed{Q}$ Under what condition $c_{n,m}$ is a ring homomorphism?

Let's do backward engineering; suppose $c_{n,m}$ is a ring homomorphism.

Then $c_{n,m}(\underbrace{1_{\mathbb{Z}_n}+\cdots+1_{\mathbb{Z}_n}}_{k \text{ times}}) = c_{n,m}(1_{\mathbb{Z}_n})+\cdots+c_{n,m}(1_{\mathbb{Z}_n})$ $\quad (\dagger)$

Notice that $1_{\mathbb{Z}_n}=1$ and $c_{n,m}(1_{\mathbb{Z}_n})=1=1_{\mathbb{Z}_m}$.

Following the example of $n=2$ and $m=3$, we let $\underline{k=n}$.

Then $\underbrace{1_{\mathbb{Z}_n}+\cdots+1_{\mathbb{Z}_n}}_{n \text{ times}}=0$; and so $(\dagger)$ implies

$$\underset{\underset{0}{\|}}{c_{n,m}(0)} = \underbrace{1_{\mathbb{Z}_m}+\cdots+1_{\mathbb{Z}_m}}_{n \text{ times}} = \text{remainder of } n \text{ divided by } m.$$

Hence $m \mid n$.

$$\boxed{\begin{array}{l}\underline{\text{Summary}}.\ \text{If } c_{n,m}:\mathbb{Z}_n\to\mathbb{Z}_m,\ c_{n,m}(a):=\text{the remainder of } a \text{ divided by } m \\ \text{is a ring homomorphism, then } m\mid n.\end{array}}$$

Next we want to show its converse. We also show that the following diagram $\underline{\text{commutes}}$; that means no matter which path we take we get the same result. (The curved arrow says it is a

$$\begin{tikzcd}
& \mathbb{Z} \arrow[dl, "c_n"'] \arrow[dr, "c_m"] \arrow[d, phantom, "\circlearrowleft"] & \\
\mathbb{Z}_n \arrow[rr, "c_{n,m}"'] & {} & \mathbb{Z}_m
\end{tikzcd}$$

$a \mapsto c_n(a) \overset{c_{n,m}}{\longmapsto} c_{n,m}(c_n(a)) \;\|\; c_m(a)$

commuting diagram.) So in this case it means $c_{n,m}(c_n(a)) = c_m(a)$.

<u>Theorem</u>. Suppose $m|n$. Let $c_{n,m}: \mathbb{Z}_n \to \mathbb{Z}_m$,

$c_{n,m}(a) :=$ remainder of a divided by m.

Then $c_{n,m}$ is a ring homomorphism; moreover the following diagram commutes; that means

$c_{n,m}(c_n(a)) = c_m(a)$.

$$\begin{tikzcd} & \mathbb{Z} \arrow[dl, "c_n"'] \arrow[dr, "c_m"] \arrow[d, phantom, "?"] & \\ \mathbb{Z}_n \arrow[rr, "c_{n,m}"'] & & \mathbb{Z}_m \end{tikzcd}$$

<u>Pf</u>. We start with proving that the mentioned diagram is a commuting diagram if $m|n$.

(Notice that, if $m \nmid n$, then this diagram is not commuting; here is an example:

$$\begin{tikzcd} & \mathbb{Z} \arrow[dl] \arrow[dr] & \\ \mathbb{Z}_2 \arrow[rr] & & \mathbb{Z}_3 \end{tikzcd}$$

2

$0 \longmapsto 0 \neq 2$.)

We have to show for any $a \in \mathbb{Z}$, $c_{n,m}(c_n(a)) = c_m(a)$.

Let's start with $c_n(a)$. Let q be the quotient of a divided by n; and so $a = nq + c_n(a)$. Next let q' be the quotient of $c_n(a)$ divided by m;

Lecture 02: Homomorphism between Zn and Zm

Monday, January 14, 2019 9:46 AM

and so $c_n(a) = mq' + \underbrace{c_{n,m}(c_n(a))}_{\text{remainder of } c_n(a) \text{ divided by } m.}$ (2)

(1) and (2) imply $a = nq + mq' + c_{n,m}(c_n(a))$. (3)

$m \mid n$ implies $m \mid nq + mq'$; and so $\exists q'' \in \mathbb{Z}$ s.t.

$nq + mq' = mq''$. Hence by (3) we have

$$a = mq'' + \underbrace{c_{n,m}(c_n(a))}_{\text{in } \{0,1,\ldots,m-1\}} \quad . \quad (4)$$

By (4) and uniqueness of quotient and remainder (from long division) we deduce that $c_{n,m}(c_n(a))$ is the remainder of a divided by m; hence $c_m(a) = c_{n,m}(c_n(a))$.

We will finish prove of this theorem in the next lecture.