Lecture 15: Orders & Decimal Expansions

Tom Roby
University of Connecticut

23 October 2012

Outline

- Orders of elements in $\mathbf{Z}_m^*$;
- Orders and powers of $a \in \mathbf{Z}_m^*$;
- Periods of decimal expansions;

Example & Definitions

- Consider $\mathbf{Z}_9^*$. How many units? What are they? What are their powers?

Example & Definitions

- Consider $\mathbf{Z}_9^*$. How many units? What are they? What are their powers?
- DEF: Given $a \in \mathbf{Z}_m^*$, the least $n \in \mathbf{Z}^+$ s.t. $a^n = 1$ is called the **order** of a mod m. Sometimes we write $ord(a)$, $ord_m(a)$, $o(a)$ or $o_m(a)$.

Example & Definitions

- Consider $\mathbf{Z}_9^*$. How many units? What are they? What are their powers?
- DEF: Given $a \in \mathbf{Z}_m^*$, the least $n \in \mathbf{Z}^+$ s.t. $a^n = 1$ is called the **order** of a mod m. Sometimes we write $ord(a)$, $ord_m(a)$, $o(a)$ or $o_m(a)$.
- EG: What is the order of 2 mod 9? Of 7? What do you notice about the order of elements?

Example & Definitions

- Consider $\mathbf{Z}_9^*$. How many units? What are they? What are their powers?
- DEF: Given $a \in \mathbf{Z}_m^*$, the least $n \in \mathbf{Z}^+$ s.t. $a^n = 1$ is called the **order** of a mod m. Sometimes we write $ord(a)$, $ord_m(a)$, $o(a)$ or $o_m(a)$.
- EG: What is the order of 2 mod 9? Of 7? What do you notice about the order of elements?
- THM: If a mod m has order n, then for $k \in \mathbf{Z}^+$ $a^k = 1 \iff o(a) \mid k$.

Example & Definitions

- Consider $\mathbf{Z}_9^*$. How many units? What are they? What are their powers?
- DEF: Given $a \in \mathbf{Z}_m^*$, the least $n \in \mathbf{Z}^+$ s.t. $a^n = 1$ is called the **order** of a mod m. Sometimes we write $ord(a)$, $ord_m(a)$, $o(a)$ or $o_m(a)$.
- EG: What is the order of 2 mod 9? Of 7? What do you notice about the order of elements?
- THM: If a mod m has order n, then for $k \in \mathbf{Z}^+$ $a^k = 1 \iff o(a) \mid k$.
- PF: $(\Leftarrow)$ is easy from the definitions.
  $(\Rightarrow)$: Use division algorithm.

Big Theorem on Orders

Here is the THE big theorem about orders in $\mathbf{Z}_m^*$.

Theorem

Let $a \bmod m$ have order n. THEN

1. *For all $k \in \mathbf{Z}^+$, $a^k \equiv 1 \pmod{m} \iff o(a) \mid k$. In particular, $o(a) \mid \phi(m)$, and $a^k \equiv a^l \iff k \equiv l \pmod{\mathbf{o(a)}}$.*

Big Theorem on Orders

Here is the THE big theorem about orders in $\mathbf{Z}_m^*$.

Theorem

Let $a \bmod m$ *have order* n. *THEN*

1. *For all* $k \in \mathbf{Z}^+$, $a^k \equiv 1 \pmod{m} \iff o(a) \mid k$. *In particular,* $o(a) \mid \phi(m)$, *and* $a^k \equiv a^l \iff k \equiv l \pmod{\mathbf{o(a)}}$.
2. *If* $(k, o(a)) = 1$, *then* a^k *has the same order as* a.

Big Theorem on Orders

Here is the THE big theorem about orders in $\mathbf{Z}_m^*$.

Theorem

Let $a \bmod m$ *have order* n. *THEN*

1. *For all* $k \in \mathbf{Z}^+$, $a^k \equiv 1 \pmod{m} \iff o(a) \mid k$. *In particular,* $o(a) \mid \phi(m)$, *and* $a^k \equiv a^l \iff k \equiv l \pmod{\mathbf{o(a)}}$.
2. *If* $(k, o(a)) = 1$, *then* a^k *has the same order as* a.
3. *If* $d \mid o(a)$, *then* a^d *has order* $\frac{o(a)}{d}$.

Big Theorem on Orders

Here is the THE big theorem about orders in $\mathbf{Z}_m^*$.

Theorem

Let $a \bmod m$ have order n. THEN

1. *For all $k \in \mathbf{Z}^+$, $a^k \equiv 1 \pmod{m} \iff o(a) \mid k$. In particular, $o(a) \mid \phi(m)$, and $a^k \equiv a^l \iff k \equiv l \pmod{\mathbf{o}(\mathbf{a})}$.*
2. *If $(k, o(a)) = 1$, then a^k has the same order as a.*
3. *If $d \mid o(a)$, then a^d has order $\frac{o(a)}{d}$.*
4. *If a_1 has order n_1 and a_2 has order n_2 in $\mathbf{Z}_m^*$, with $(n_1, n_2) = 1$, then $a_1 a_2$ has order $n_1 n_2$.*

Big Theorem on Orders

Here is the THE big theorem about orders in $\mathbf{Z}_m^*$.

Theorem

Let $a \bmod m$ have order n. THEN

1. *For all $k \in \mathbf{Z}^+$, $a^k \equiv 1 \pmod{m} \iff o(a) \mid k$. In particular, $o(a) \mid \phi(m)$, and $a^k \equiv a^l \iff k \equiv l \pmod{\mathbf{o(a)}}$.*
2. *If $(k, o(a)) = 1$, then a^k has the same order as a.*
3. *If $d \mid o(a)$, then a^d has order $\frac{o(a)}{d}$.*
4. *If a_1 has order n_1 and a_2 has order n_2 in $\mathbf{Z}_m^*$, with $(n_1, n_2) = 1$, then $a_1 a_2$ has order $n_1 n_2$.*

EG: Let's look at a power table for $\mathbf{Z}_{19}^*$.

Decimal expansions

Consider the decimal expansions of the following fractions:
$\frac{1}{3}, \frac{1}{7}, \frac{7}{22}, \frac{15}{37}$.

Decimal expansions

Consider the decimal expansions of the following fractions: $\frac{1}{3}, \frac{1}{7}, \frac{7}{22}, \frac{15}{37}$.

$$
\begin{aligned}
\frac{1}{3} &= .33333\cdots = .\overline{3} && \text{Period} = 1\\
\frac{1}{7} &= .1428571428\cdots = .\overline{142857} && \text{Period} = 6\\
\frac{7}{22} &= .3181818\cdots = 3.\overline{18} && \text{Period} = 2\\
\frac{15}{37} &= .405405405\cdots = .\overline{405} && \text{Period} = 3
\end{aligned}
$$

Decimal expansions

Consider the decimal expansions of the following fractions: $\frac{1}{3}, \frac{1}{7}, \frac{7}{22}, \frac{15}{37}$.

$$\frac{1}{3} = .33333\cdots = .\overline{3} \qquad \text{Period} = 1$$

$$\frac{1}{7} = .1428571428\cdots = .\overline{142857} \qquad \text{Period} = 6$$

$$\frac{7}{22} = .3181818\cdots = 3.\overline{18} \qquad \text{Period} = 2$$

$$\frac{15}{37} = .405405405\cdots = .\overline{405} \qquad \text{Period} = 3$$

Any Conjectures from here or the HW?

True/False: Every rational number has a repeating decimal expansion?

Decimal expansions

Consider the decimal expansions of the following fractions: $\frac{1}{3}, \frac{1}{7}, \frac{7}{22}, \frac{15}{37}$.

$$\frac{1}{3} = .33333\cdots = .\overline{3} \qquad \text{Period} = 1$$
$$\frac{1}{7} = .1428571428\cdots = .\overline{142857} \qquad \text{Period} = 6$$
$$\frac{7}{22} = .3181818\cdots = 3.\overline{18} \qquad \text{Period} = 2$$
$$\frac{15}{37} = .405405405\cdots = .\overline{405} \qquad \text{Period} = 3$$

Any Conjectures from here or the HW?

True/False: Every rational number has a repeating decimal expansion? ANS: **TRUE!**

Decimal Expansion Conjectures

Prove or Disprove & Salvage if Possible:

1. The period length of $\frac{1}{p}$ divides $p-1$;
2. For each $b \geq 2$, all $\frac{a}{b}$ with $(a, b) = 1$ have same period length.
3. Expansion of $\frac{1}{b}$ is purely periodic when $(10, b) = 1$.
4. Shifting digits (cyclically) gives another fraction with same denominator.

Converting between decimals and fractions

- To go from fractions to decimal expansions is easy. Why?

Converting between decimals and fractions

- To go from fractions to decimal expansions is easy. Why?
- Conversely, how do we go from fractions to decimals? EG, what fraction is represented by $x = .\overline{15}$?

Converting between decimals and fractions

- To go from fractions to decimal expansions is easy. Why?
- Conversely, how do we go from fractions to decimals? EG, what fraction is represented by $x = .\overline{15}$?
- How about $x = .\overline{405}$

Converting between decimals and fractions

- To go from fractions to decimal expansions is easy. Why?
- Conversely, how do we go from fractions to decimals? EG, what fraction is represented by $x = .\overline{15}$?
- How about $x = .\overline{405}$
- What happens in general with $x = .\overline{c_1 c_2 \cdots c_d}$?

Converting between decimals and fractions

- To go from fractions to decimal expansions is easy. Why?
- Conversely, how do we go from fractions to decimals? EG, what fraction is represented by $x = .\overline{15}$?
- How about $x = .\overline{405}$
- What happens in general with $x = .\overline{c_1 c_2 \cdots c_d}$?
- Some algebra shows that $\frac{a}{b}$ has a *purely periodic* decimal expansion $0.\overline{c_1 \cdots c_d} \iff$ *some* representation of $\frac{a}{b}$ has denominator $10^d - 1$ for *some* $d \in \mathbf{Z}^+$.

Converting between decimals and fractions

- To go from fractions to decimal expansions is easy. Why?
- Conversely, how do we go from fractions to decimals? EG, what fraction is represented by $x = .\overline{15}$?
- How about $x = .\overline{405}$
- What happens in general with $x = .\overline{c_1 c_2 \cdots c_d}$?
- Some algebra shows that $\frac{a}{b}$ has a *purely periodic* decimal expansion $0.\overline{c_1 \cdots c_d} \iff$ *some* representation of $\frac{a}{b}$ has denominator $10^d - 1$ for *some* $d \in \mathbf{Z}^+$.
- **NB:** The denominator may be something other than $10^d - 1$ when the fractions is simplified to lowest terms.

Converting between decimals and fractions

- To go from fractions to decimal expansions is easy. Why?
- Conversely, how do we go from fractions to decimals? EG, what fraction is represented by $x = .\overline{15}$?
- How about $x = .\overline{405}$
- What happens in general with $x = .\overline{c_1 c_2 \cdots c_d}$?
- Some algebra shows that $\frac{a}{b}$ has a *purely periodic* decimal expansion $0.\overline{c_1 \cdots c_d} \iff$ *some* representation of $\frac{a}{b}$ has denominator $10^d - 1$ for *some* $d \in \mathbf{Z}^+$.
- **NB:** The denominator may be something other than $10^d - 1$ when the fractions is simplified to lowest terms.
  EG: $\frac{5}{33} = \frac{15}{99} = .\overline{15}$; $\frac{1}{3} = \frac{3}{9} = 0.\overline{3}$.

Orders & Decimals

Theorem

Let $x = \frac{a}{b} \in \mathbf{Q}^+$ *with* $(b, 10) = 1$*. Then the decimal period of* x *is* $ord_b(10)$*, the order of 10 in* $\mathbf{Z}_b^*$*.*

Theorem

Let $x = \frac{a}{b} \in \mathbf{Q}^+$ *with* $(b, 10) = 1$*. Then the decimal period of* x *is* $ord_b(10)$*, the order of 10 in* $\mathbf{Z}_b^*$*.*

Proof.

decimal period of $x =$ least $d \geq 1$ s.t. x has denom. $10^d - 1$

$\square$

Theorem

Let $x = \frac{a}{b} \in \mathbf{Q}^+$ with $(b, 10) = 1$. Then the decimal period of x is $ord_b(10)$, the order of 10 in $\mathbf{Z}_b^*$.

Proof.

$$\begin{aligned} \text{decimal period of } x &= \text{least } d \geq 1 \text{ s.t. } x \text{ has denom. } 10^d - 1 \\ &= \text{least } d \geq 1 \text{ s.t. } b \mid 10^b - 1 \end{aligned}$$

□

Theorem

Let $x = \frac{a}{b} \in \mathbf{Q}^+$ with $(b, 10) = 1$. Then the decimal period of x is $ord_b(10)$, the order of 10 in $\mathbf{Z}_b^*$.

Proof.

$$\begin{aligned} \text{decimal period of } x &= \text{least } d \geq 1 \text{ s.t. } x \text{ has denom. } 10^d - 1 \\ &= \text{least } d \geq 1 \text{ s.t. } b \mid 10^b - 1 \\ &= \text{least } d \geq 1 \text{ s.t. } 10^b \equiv 1 \pmod{b} \end{aligned}$$

□

Theorem

Let $x = \frac{a}{b} \in \mathbf{Q}^+$ with $(b, 10) = 1$. Then the decimal period of x is $\mathrm{ord}_b(10)$, the order of 10 in $\mathbf{Z}_b^*$.

Proof.

$$\begin{aligned}
\text{decimal period of } x &= \text{least } d \geq 1 \text{ s.t. } x \text{ has denom. } 10^d - 1 \\
&= \text{least } d \geq 1 \text{ s.t. } b \mid 10^b - 1 \\
&= \text{least } d \geq 1 \text{ s.t. } 10^b \equiv 1 \pmod{b} \\
&= \text{order of 10 mod } b
\end{aligned}$$

$\square$

Theorem

Let $x = \frac{a}{b} \in \mathbf{Q}^+$ with $(b, 10) = 1$. Then the decimal period of x is $ord_b(10)$, the order of 10 in $\mathbf{Z}_b^*$.

Proof.

$$\begin{aligned}\text{decimal period of } x &= \text{least } d \geq 1 \text{ s.t. } x \text{ has denom. } 10^d - 1 \\ &= \text{least } d \geq 1 \text{ s.t. } b \mid 10^b - 1 \\ &= \text{least } d \geq 1 \text{ s.t. } 10^b \equiv 1 \pmod{b} \\ &= \text{order of } 10 \text{ mod } b\end{aligned}$$

□

p	3	7	9	11	13	17	19	21
Period $\frac{1}{p}$	1	6	1	2	6	16	18	6
$ord_{10}(p)$	1	6	1	2	6	16	18	6