Modular arithmetic computations review Lecture 7c: 2022-03-02

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

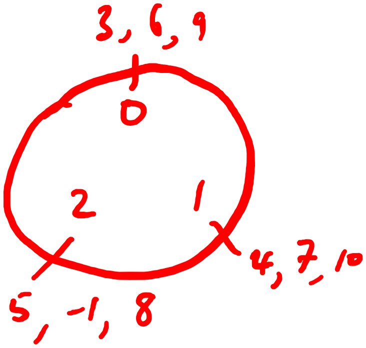
General rules for congruence class

- $a \equiv b \pmod{n} \leftrightarrow a - b \equiv 0 \pmod{n}$, which is to say that a and b differ by a multiple of n.

Ex $2 \equiv 7 \pmod{5}$

$71 \equiv 51 \pmod{10}$ $\quad 71 - 51 = 20$

$9 \equiv -1 \pmod{10}$



- To find the smallest positive label for $a \pmod{n}$, simply find the remainder of $a \div n$.

Ex. $7 \div 5 = 1$ r 2 , $7 \equiv 2 \bmod 5$

$71 \div 10 = 7$ r 1 , $51 \div 10 = 5$ r 1

$71 \equiv 1 \bmod 10$

$51 \equiv 1 \bmod 10$

$51 \equiv 71 \bmod 10$

If $a < n$, then a is already the smallest pos. label,

$2 \bmod 7$

Adding in modular arithmetic

- When adding $a + b \pmod{n}$, two options:
  - (1) Add the two numbers in normal arithmetic first, and then divide to find the smallest positive label.

Ex. $76 + 25 \pmod{7}$

$\equiv 101 \pmod{7}$

$\equiv 3 \pmod{7}$

$$\begin{array}{r} 14 \text{ r } 3 \\ 7\overline{)101} \\ \underline{7} \\ 31 \\ \underline{28} \\ 3 \end{array}$$

  - (2) Replace the two numbers with another number from their respective congruence classes first, then add, and then replace again.

$$\begin{array}{r} 10 \text{ r } 6 \\ 7\overline{)76} \\ \underline{70} \\ 6 \end{array} \qquad \begin{array}{r} 3 \text{ r } 4 \\ 7\overline{)25} \end{array}$$

Ex. $76 + 25 \pmod{7}$

$\equiv 6 + 4 \pmod{7}$

$\equiv 10 \pmod{7}$

$\equiv 3 \pmod{7}$

Multiplying in modular arithmetic

- When multiplying $a \times b \pmod{n}$, two options:
  - (1) Multiply the two numbers in normal arithmetic first, and then divide to find the smallest positive label.

Ex. $76 \times 25 \pmod 7$

$\equiv 1900 \pmod 7$

$\equiv 3 \pmod 7$

$$\begin{array}{r} 76 \\ \times 25 \\ \hline 380 \\ 152 \\ \hline 1900 \end{array}$$

$$\begin{array}{r} 271 \text{ r } 3 \\ 7 \overline{)1900} \\ 14 \\ \hline 50 \\ 49 \\ \hline 10 \\ 7 \\ \hline 3 \end{array}$$

  - (2) Replace the two numbers with another number from their respective congruence classes first, then multiply, and then replace again. (sometimes helpful to use negatives)

Ex. $76 \times 25 \pmod 7$

$\equiv 6 \times 4 \pmod 7$

$\equiv 24 \pmod 7$

$\equiv 3 \pmod 7$

$\equiv -1 \times 4 \pmod 7$

$\equiv -4 \pmod 7$

$\equiv -4+7 \equiv 3 \pmod 7$

Simple powers in modular arithmetic

- To compute powers, sometimes it is easier to break it up into a product and simplify.

Ex. $2^{10} \bmod 7 \equiv 1024 \bmod 7$

$\equiv 2 \bmod 7$

$$\begin{array}{r} 146 \text{ r } 2 \\ 7\overline{)1024} \\ \underline{7} \\ 32 \\ \underline{28} \\ 44 \\ \underline{42} \\ 2 \end{array}$$

$$\equiv \underbrace{2 \times 2 \times 2}_{8 \equiv 1} \times \underbrace{2 \times 2 \times 2}_{1} \times \underbrace{2 \times 2 \times 2}_{1} \times 2$$

$$\equiv (2^3)^3 \cdot 2 \equiv (1)^3 \cdot 2 \equiv 2 \bmod 7$$

$2^8 = 256$
$+2^8 = 256$
512
$= 2^9$

$(2^8 \times 2^9$

Ex. $2^{16} \bmod 7 \equiv (2^3)^5 \cdot 2^1 \equiv 2 \bmod 7$

$$\equiv (((2^2)^2)^2)^2 \equiv (((4)^2)^2)^2 \equiv ((16)^2)^2$$

$$\equiv ((2)^2)^2 \equiv 4^2 \equiv 16 \equiv 2 \bmod 7$$

Try it out

- $637 \times 437 \pmod{7}$

$0 \times 437 \pmod{7}$
$\equiv 0 \mod 7$

$$\begin{array}{r} 91 \\ 7\overline{)637} \\ \underline{63} \\ 07 \end{array}$$

- $507 \times 237 \pmod{509}$

$\equiv -2 \times 237$
$\equiv -474 + 509 \equiv 35$

- $367^2 \pmod{369}$

$\equiv (-2)^2 \equiv 4 \mod 369$

- $7^6 \pmod{51}$

$\equiv (49)^3 \mod 51$
$\equiv (-2)^3 \mod 51$
$\equiv -8 \mod 51 \equiv 43$

A: 0
B: 4
C: 35
D: 43
E: None of the above

Try it out

- $432903 + 1463974 \pmod{100}$

  $\equiv 3 + 74 \equiv 77$

- $105 \times 237 \pmod{7}$

  $\equiv 0 \times 237 \equiv 0$

- $4502^2 \pmod{4507}$

  $\equiv (-5)^2 \equiv 25$

- $76 \times 77 \times 78 \pmod{79}$

  $\equiv -3 \times -2 \times -1$

  $\equiv -6 \equiv 73$

A: 0
B: 25
C: 73
D: 77
E: None of the above

Try it out

- $3^{64} \pmod{78}$ $\equiv \left(\left(\left(\left(\left(3^2\right)^2\right)^2\right)^2\right)^2\right)^2$

$78 \overline{)81}$ 1 r 3
78
3

$3^1 \equiv 3$
$3^2 \equiv 9$
$3^4 \equiv 9 \times 9 \equiv 81 \equiv 3$
$3^8 \equiv 9$
$3^{16} \equiv 9 \times 9 \equiv 81 \equiv 3$
$3^{32} \equiv 9$
$3^{64} \equiv 9 \times 9 \equiv 81 \equiv 3$

$3^1 \equiv 3$
$3^2 \equiv 9$
$3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 81 \equiv 3$

$3^4 \equiv 81 \equiv 3 \mod 78$
$3^8 \equiv (3^4)^2 \equiv 81^2$
$\equiv (3)^2 \equiv 9$

$3^{8\times 8} \equiv (3^8)^8 \equiv (9)^8 \equiv 3$

A: 3
B: 6
C: 9
D: 27
E: None of the above

Try it out

- $3^{64} \pmod{25}$

$3^1 \equiv 3$

$3^2 \equiv 9$

$3^4 \equiv 9^2 \equiv 81 \equiv 6$

$3^8 \equiv 3^4 \cdot 3^4 \equiv 6 \cdot 6 \equiv 36 \equiv 11$

$3^{16} \equiv 3^8 \cdot 3^8 \equiv 11 \cdot 11 \equiv 121 \equiv 21$

$3^{32} \equiv 21 \cdot 21 \equiv 441 \equiv 16$

$3^{64} \equiv 16 \cdot 16 \equiv 256 \equiv 6$

$25 \overline{)81}$ = 3 r 6: $81 - 75 = 6$

$25 \overline{)121}$ = 4 r 21: $121 - 100 = 21$

$3^3 \equiv 27 \equiv 2$

$3^6 \equiv 2^2 \equiv 4$

$3^{12} \equiv 4^2 \equiv 16$

$3^{24} \equiv 16^2 \equiv 6$

$3^{48} \equiv 6^2 \equiv 36 \equiv 11$

$3^{64} \equiv 3^{48} \cdot 3^{16} \equiv 11 \cdot 21$

$\equiv 231 \equiv 6$

$64 - 48 = 16$

A: 3
B: 6
C: 9
D: 27
E: None of the above