More modular division
Lecture 8b: 2022-03-06

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Modular division recap

- Definition: $\frac{x}{y} \equiv z \pmod{n}$ if z is the unique number in mod n arithmetic such that $y \times z \equiv x \pmod{n}$.

Ex. $\frac{3}{4} \equiv 2 \pmod{5}$ because $4 \cdot 2 \equiv 8 \equiv 3$ and this is only true for 2.

Ex. $\frac{3}{4} \pmod{6}$ is undefined because $4z \pmod{6}$ is always even and can never be 3.

Ex. $\frac{2}{4} \pmod{6}$ is undefined because $4 \cdot 2 \equiv 8 \equiv 2 \pmod{6}$

AND $4 \cdot 5 \equiv 20 \equiv 2 \pmod{6}$

Euclidean algorithm for reciprocals

- Find the reciprocal $\frac{1}{7} \pmod{11}$ using Euclidean alg

Need $7x \equiv 1 \pmod{11}$

Or $7x = 11y + 1$, where x, y integers

Or $1 = 7x - 11y$ ← a combination of 7 and 11, equal to 1.

$11 = 7 \cdot 1 + 4$
$7 = 4 \cdot 1 + 3$
$4 = 3 \cdot 1 + 1$
$3 = 3 \cdot 1$
$\gcd(7, 11) = 1$

$\Rightarrow$
$1 = 4 - 3$
$1 = 4 - (7 - 4)$
$1 = 4 \cdot 2 - 7$
$1 = (11 - 7) \cdot 2 - 7$
$1 = 11 \cdot 2 - 7 \cdot 3$

$\Rightarrow$
$1 \equiv 11 \cdot 2 - 7 \cdot 3 \pmod{11}$
$1 \equiv 0 \cdot 2 - 7 \cdot 3 \pmod{11}$
$1 \equiv 7 \cdot (-3) \pmod{11}$
$1 \equiv 7 \cdot 8 \pmod{11}$
$\frac{1}{7} \equiv 8 \pmod{11}$

Try it out

- Find the reciprocal $\frac{1}{9}$ (mod 13).

Need $9x \equiv 1 \pmod{13}$

$9x = 1 + 13y$

$1 = 9x - 13y$

$13 = 9 \cdot 1 + 4$

$9 = 4 \cdot 2 + 1$

$4 = 4 \cdot 1$

$1 = 9 - 4 \cdot 2$

$1 = 9 - (13 - 9) \cdot 2$

$1 = 9 \cdot 3 - 13 \cdot 2$

$1 \equiv 9 \cdot 3 - \underline{13} \cdot 2 \pmod{13}$

$1 \equiv 9 \cdot 3 \pmod{13}$

$\Rightarrow \frac{1}{9} \equiv 3 \pmod{13}$

A: 2
B: 3
C: 6
D: 8
E: None of the above

How to do division $\frac{x}{y} \pmod{n}$

- Step 1: check if (y, n) are relatively prime. If not, then division is ill-defined.

Ex. $\frac{7}{9} \pmod{13}$

$\gcd(9, 13) = 1$ ✓

- Step 2: use Euclidean algorithm to find $\frac{1}{y} \pmod{n}$

Previous slide: $\frac{1}{9} \equiv 3 \pmod{13}$

- Step 3: multiply $x \cdot \frac{1}{y} \pmod{n}$.

$7 \cdot \frac{1}{9} \equiv 7 \cdot 3 \equiv 21 \equiv 8 \pmod{13}$

Try it out

- Find $\frac{8}{9}$ (mod 23).

Euclidean alg

$23 = 9 \cdot 2 + 5$

$9 = 5 \cdot 1 + 4$

$5 = 4 \cdot 1 + 1$

$4 = 4 \cdot 1$

✓ $\gcd(9, 23) = 1$

Solve for $\frac{1}{9}$

$1 = 5 - 4$

$1 = 5 - (9 - 5) = 5 \cdot 2 - 9$

$1 = (23 - 9 \cdot 2) \cdot 2 - 9 = 23 \cdot 2 - 9 \cdot 5$

$1 \equiv -9 \cdot 5 \pmod{23}$

$\Rightarrow \frac{1}{9} \equiv -5 \pmod{23}$

$\frac{1}{9} \equiv 18 \pmod{23}$

$8 \cdot \frac{1}{9} \equiv 8 \cdot (-5) \pmod{23}$

$\frac{8}{9} \equiv -40 \pmod{23}$

$\frac{8}{9} \equiv 6 \pmod{23}$

A: 2
B: 3
C: 6
D: 8
E: None of the above

Try it out

- Find $\frac{7}{216}$ (mod 691).

$691 = 216 \cdot 3 + 43$

$216 = 43 \cdot 5 + 1$

$43 = 43 \cdot 1$

✓ $\gcd(216, 691) = 1$

$1 = 216 - 43 \cdot 5$

$1 = 216 - (691 - 216 \cdot 3) \cdot 5$

$1 = 216 \cdot 16 - 691 \cdot 5$

$1 \equiv 216 \cdot 16 \pmod{691}$

$\Rightarrow \frac{1}{216} \equiv 16 \pmod{691}$

$\frac{7}{216} \equiv 7 \cdot 16 \pmod{691}$

$\equiv 112 \pmod{691}$

A: 112
B: 231
C: 450
D: 599
E: None of the above

Try it out

- Find $\frac{10}{183} \pmod{1521}$

Notice: $\overbrace{1521}^{9}$ and $\overbrace{183}^{12}$ are both divisible by 3.

$\Rightarrow$ ill-defined.

A: 112
B: 231
C: 450
D: 599
E: None of the above

Another shortcut

- When working with prime modulus, you can also factor out fractions.

Why doesn't this work for non-prime modulus?

Ex. $\frac{5}{10} \pmod{11}$

$11 = 10 \cdot 1 + 1 \implies 1 = 11 - 10$

$1 \equiv 11 - 10 \cdot 1 \pmod{11}$

$\implies 1 \equiv 10 \cdot (-1) \pmod{11}$

$\implies \frac{1}{10} \equiv -1$ (mod 11

$\implies \frac{5}{10} \equiv 5 \cdot -1 \equiv -5 \equiv 6 \pmod{11}$

Ex. $\frac{5}{10} \pmod{11} \equiv \frac{1}{2} \cdot \frac{5}{5} \pmod{11} \equiv \frac{1}{2} \pmod{11}$

$11 = 2 \cdot 5 + 11$

$1 = 11 - 2 \cdot 5$

$1 \equiv -2 \cdot 5 \pmod{11}$

$\frac{1}{2} \equiv -5 \equiv 6 \pmod{11}$

Try it out

- Find $\frac{7}{70}$ (mod 71) $\equiv \frac{1}{10}$

prime

$71 = 10 \cdot 7 + 1$
$1 = 71 - 10 \cdot 7$
$1 \equiv -7 \cdot 10$
$\frac{1}{10} \equiv -7 \equiv 64 \pmod{71}$

$7 \cdot \frac{1}{70} \pmod{71}$

$71 = 70 \cdot 1 + 1$
$1 = 71 - 70$
$1 \equiv -70$
$\frac{1}{70} \equiv -1$
$\frac{7}{70} \equiv -7 \equiv 64$

- Find $\frac{7}{70}$ (mod 91)

$7 \cdot 13$

WRONG:

$\frac{7}{70} \equiv \frac{1}{10} \pmod{91}$
$1 = 91 - 10 \cdot 9$
$1 \equiv -10 \cdot 9$
$\frac{1}{10} \equiv -9 \equiv 82$

Problem $\gcd(70, 91) = 7$, so multiple solutions

Ex. $4 \cdot 70 \equiv 7 \mod 91$

A: 4
B: 35
C: 64
D: 82
E: None of the above