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 $y \times z \equiv x \pmod{n}$.

Euclidean algorithm for reciprocals

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

Try it out

- Find the reciprocal $\frac{1}{9} \pmod{13}$.

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.

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

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

Try it out

- Find $\frac{8}{9} \pmod{23}$.

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

Try it out

- Find $\frac{7}{216} \pmod{691}$.

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

Try it out

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

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?

Try it out

- Find $\frac{7}{70} \pmod{71}$

- Find $\frac{7}{70} \pmod{91}$

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