Reciprocals via Fermat’s Little Theorem Lecture 9c: 2022-03-16

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Fermat’s little theorem

- Let p be prime.
- If $x \not\equiv 0 \pmod{p}$, then $x^{p-1} \equiv 1 \pmod{p}$.
- For any x (including 0), can say $x^p \equiv x \pmod{p}$.

- We can use Fermat’s Little Theorem to quickly reduce large powers by division with remainder.
- Let $n = m(p-1) + r$. Then $x^n \equiv x^r \pmod{p}$.

Try it out

- $4^{244} \pmod 7$

- $7^{286} \pmod{13}$

A: 4
B: 5
C: 6
D: 7
E: None of the above

Another example

- $3^{401} \pmod{81}$

A: 0
B: 1
C: 2
D: 3
E: None of the above

Alternative for finding reciprocals

- Recall, can use Euclidean algorithm to find reciprocals

- Notice that $x^{p-1} \equiv 1 \pmod{p}$.
- Therefore, $x^{p-2} \equiv \frac{1}{x} \pmod{p}$.

Try it out

- Find $\frac{1}{12} \pmod{67}$.

A: 20
B: 24
C: 28
D: 32
E: None of the above

Try it out

- Find $\frac{1}{2} \pmod{131}$.

A: 25
B: 33
C: 66
D: 91
E: None of the above