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

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Fermat's little theorem

$p \equiv 0 \mod p$

$x^p \equiv x \mod p$

$x^{p-1} \equiv 1 \mod p$

- 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 $x^p \equiv x \pmod{p}$.

Ex. $12^{22} \mod 23 \equiv 1$

$12^{23} \mod 23 \equiv 12$

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

$14^{444} \mod 23 \equiv 14^4 \mod 23$

$22 \overline{)444}$ r 4

440

20

$14^4 \equiv 14^{22+4} \equiv 14^{22+22+4} \equiv \cdots$

Try it out

$p \equiv 0 \mod p$

$x^{p-1} \equiv 1 \mod p$

- $4^{244} \pmod 7$

$\equiv 4^4 \pmod 7 \equiv 4 \mod 7$

$6 \overline{)244}$ 40 r 4

24

04

$4^1 \equiv 4 \mod 7$

$4^2 \equiv 16 \equiv 2 \mod 7$

$4^4 \equiv 4 \mod 7$

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

$\equiv 7^{10} \pmod{13}$

$12 \overline{)286}$ 23 r 10

24

46

36

10

$\equiv 7^8 \cdot 7^2 \equiv 3 \cdot 10 \mod 13$

$\equiv 30 \mod 13$

$\equiv 4 \mod 13$

$\equiv 10^5 \mod 13$

$7^1 \equiv 7$

$7^2 \equiv 49 \equiv 10$

$7^4 \equiv 100 \equiv 9$

$7^8 \equiv 81 \equiv 3$

$13 \times 7 = 21 + 70 = 91$

$13 \times 6 = 78$

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

Another example

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

WRONG: $3^{401} \equiv 3^{80 \cdot 5 + 1} \equiv 3^1 \equiv 3$

Correct:

$3^1 \equiv 3$

$3^2 \equiv 9$

$3^4 \equiv 81 \equiv 0$

So $3^{401} \equiv 3^{397} \cdot 3^4 \equiv 3^{397} \cdot 0 \equiv 0$

$3^p \equiv 3 \mod p$

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

Ex. $\frac{1}{5} \pmod{11}$

$11 = 5 \cdot 2 + 1$

$5 = 5 \cdot 1$

$1 = 11 - 5 \cdot 2$

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

divide by 5 $\rightarrow$ $\frac{1}{5} \equiv -2 \pmod{11}$

$\equiv 9 \pmod{11}$

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

Ex. $5^{10} \equiv 1 \pmod{11}$

$5 \cdot 5^9 \equiv 1 \pmod{11}$

$\frac{1}{5} \equiv 5^9 \pmod{11}$

$5^1 \equiv 5$

$5^2 \equiv 25 \equiv 3$

$5^4 \equiv 9$

$5^8 \equiv 81 \equiv 4$

$5^9 \equiv 5^8 \cdot 5 \equiv 4 \cdot 5$

$\equiv 20 \equiv 9 \pmod{11}$

Try it out

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

$20 \cdot 12 \overset{?}{\equiv} 1 \pmod{67}$

$67 \overline{)240}$ 3 r 39

201

39

$12^{66} \equiv 1$

$12^{65} \equiv \frac{1}{12} \equiv 12^{64} \cdot 12 \equiv 47 \cdot 12 \equiv 564 \equiv 28$

5 r 1

$67 \overline{)336}$

335

1

28×12

56

28

336

$12^1 \equiv 12$

$12^2 \equiv 144 \equiv 10$

$12^4 \equiv 100 \equiv 33$

$12^8 \equiv 1089 \equiv 17$

$12^{16} \equiv 289 \equiv 21$

$12^{32} \equiv 441 \equiv 39$

$12^{64} \equiv 1521 \equiv 47$

~~A: 20~~

B: 24

C: 28

D: 32

E: None of the above

Try it out

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

$131 = 2 \cdot 65 + 1$

$1 = 131 - 2 \cdot 65$

$1 \equiv -2 \cdot 65$

$\frac{1}{2} \equiv -65 \equiv 66 \mod 131$

$2^{130} \equiv 1 \mod 131$

$2^{129} \equiv \frac{1}{2} \mod 131 \equiv 33 \cdot 2 \equiv 66 \mod 131$

$66 \cdot 2 \equiv 132$

$\equiv 1 \mod 131$

$2 \equiv 2$

$2^2 \equiv 4$

$2^4 \equiv 16$

$2^8 \equiv 256 \equiv 125 \equiv -6$

$2^{16} \equiv 36$

$2^{32} \equiv 1296 \equiv 1296 - 1310 \equiv -14$

$2^{64} \equiv 196 \equiv 65$

$2^{128} \equiv 4225 \equiv 33$

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