Roots using Euler's Theorem
Lecture 10d: 2022-03-23

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Euler's Theorem

- Fermat's Little Theorem:
  For prime p, if $a \not\equiv 0 \pmod{p}$, then
  $$a^{p-1} \equiv 1 \pmod{p}$$

- Euler's Theorem:
  For any number n, if $\gcd(a, n) = 1$, then
  $$a^{\phi(n)} \equiv 1 \pmod{n}$$
  where $\phi(n)$ is Euler's totient function counting the number of relative primes smaller than n.

Note: $\phi(p) = p-1$ for any prime

Finding roots

- Algorithm for $\sqrt[k]{a} \pmod{p}$ using ~~Fermat's Little~~ Thm
  - Conditions: ~~p is prime~~, ~~$a \not\equiv 0 \pmod{p}$~~, and $\gcd(k, \cancel{p-1}) = 1$.
  - Find 1 as a combination of k and ~~$p-1$~~
    $$1 = km - l(\cancel{p-1})$$
  - Then $a^1 \equiv a^{1+l(\cancel{p-1})} \equiv a^{km}$.
  - So $\sqrt[k]{a} \equiv \sqrt[k]{a^{km}} \equiv a^m \pmod{\cancel{p}}$

Finding roots with Euler's Theorem

- Algorithm for $\sqrt[k]{a} \pmod{n}$ using Euler's Theorem
  - Conditions: $\gcd(a, n) = 1$ and $\gcd\big(k, \phi(n)\big) = 1$.
  - Find 1 as a combination of k and $\phi(n)$

$$1 = km - l\phi(n)$$

  - Then $a^1 \equiv a^{1+l\phi(n)} \equiv a^{km}$.
  - So $\sqrt[k]{a} \equiv \sqrt[k]{a^{km}} \equiv a^m \pmod{n}$

Finding roots with Euler's Theorem

$\phi(10) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4$

- Algorithm for $\sqrt[k]{a} \pmod{n}$ using Euler's Theorem
  - Conditions: $\gcd(a, n) = 1$ and $\gcd(k, \phi(n)) = 1$.

Ex. $\sqrt[3]{7} \bmod 10$ $\gcd(7, 10) = 1$ $\gcd(3, 4) = 1$

  - Find 1 as a combination of k and $\phi(n)$

$$1 = km - l\phi(n)$$

$4 = 3 \cdot 1 + 1$ $1 = 4 - 3$ $1 = 3 \cdot (-1) - (-1) \cdot 4$

$3 = 3 \cdot 1$ (l, m)

  - Then $a^1 \equiv a^{1 + l\phi(n)} \equiv a^{km}$.

$7^1 \equiv 7^{-3}$ $7^4 \equiv 1$ by Euler's Thm $(\bmod 10)$

  - So $\sqrt[k]{a} \equiv \sqrt[k]{a^{km}} \equiv a^m \pmod{n}$

$\sqrt[3]{7} \equiv \sqrt[3]{7^{-3}} \equiv 7^{-1 + \phi(n)} \equiv 7^3 \pmod{10}$

$\equiv 49 \cdot 7 \pmod{10}$

$\equiv 9 \cdot 7 \pmod{10}$

$\equiv 63 \equiv 3 \pmod{10}$

Check $3^3 \equiv 27 \equiv 7 \bmod 10$

Try it out

- Compute $\sqrt[5]{3} \pmod{85}$
- Step 1: Find $\phi(85)$

$85 = 5 \cdot 17$

$\phi(85) = 85 \cdot \frac{4}{5} \cdot \frac{16}{17}$

$= 64$

A: 13
B: 63
C: 64
D: 84
E: None of the above

- Step 2: Check $\gcd(3, 85)$ and $\gcd(5, \phi(85))$.

$85 = 3 \cdot 28 + 1$

$3 = 3 \cdot 1$

$\gcd(3, 85) = 1$

$64 = 5 \cdot 12 + 4$

$5 = 4 \cdot 1 + 1$

$4 = 4 \cdot 1$

$\gcd(5, 64) = 1$

$\sqrt[5]{3} \pmod{85}$ (cont)

- Step 3: Solve for $1 = km - l\phi(n)$. What is m?

$64 = 5 \cdot 12 + 4$

$5 = 4 \cdot 1 + 1$

$1 = 5 - 4$

$1 = 5 - (64 \cdot 5 \cdot 12)$

$1 = 5 \cdot 13 - 64$

$k \quad m$

$\rightarrow m = 13$

A: 13
B: 63
C: 64
D: 84
E: None of the above

- Step 4: Find $\sqrt[5]{3} \pmod{85}$ using m.

$3 \equiv 3^{65} \Rightarrow \sqrt[5]{3} \equiv \sqrt[5]{3^{65}} \equiv 3^{13}$

$3 \equiv 3$

$3^2 \equiv 9$

$3^4 = 81 \equiv -4$

$3^8 \equiv 16$

$3^{13} \equiv 3^8 \cdot 3^4 \cdot 3$

$\equiv 16 \cdot -4 \cdot 3$

$\equiv -64 \cdot 3$

$\equiv 21 \cdot 3$

$\equiv 63$

A: 13
B: 63
C: 64
D: 84
E: None of the above

Try it out

- Compute $\sqrt[5]{2} \pmod{21}$

$\phi(21) = 21 \cdot \frac{2}{3} \cdot \frac{6}{7} = 12$

$\gcd(2, 21) = 1$

$\gcd(5, 12) = 1$

$12 = 5 \cdot 2 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2$

$1 = 5 - (12 - 5 \cdot 2) \cdot 2$

$1 = 5 \cdot 5 - 12 \cdot 2$

$2^1 \equiv 2^{13} \equiv 2^{25}$

$\Rightarrow \sqrt[5]{2} \equiv 2^5$

$2^5 \bmod 21$

$\equiv 32 \bmod 21$

$\equiv 11 \bmod 21$

A: 8
B: 11
C: 15
D: 16
E: None of the above