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.

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 $\gcd(k, p-1) = 1$.
  - Find 1 as a combination of k and $p-1$

$$1 = km - l(p-1)$$

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

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

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

Try it out

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

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

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

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

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

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

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

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

Try it out

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

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