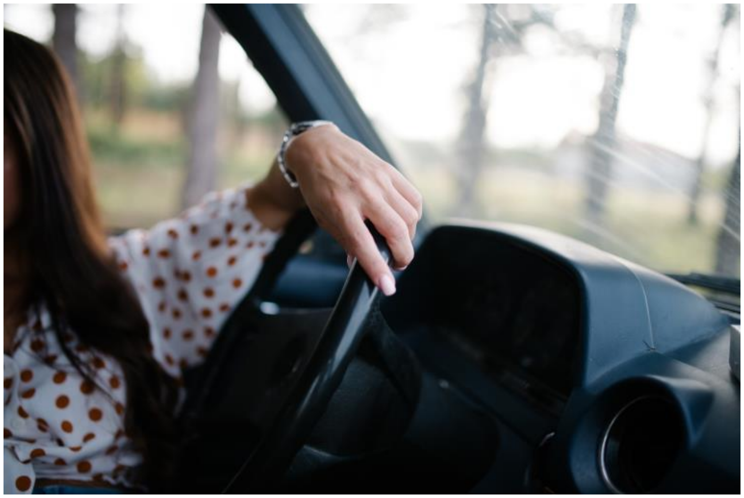
Roots in prime modulus arithmetic Lecture 9d: 2022-03-16

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

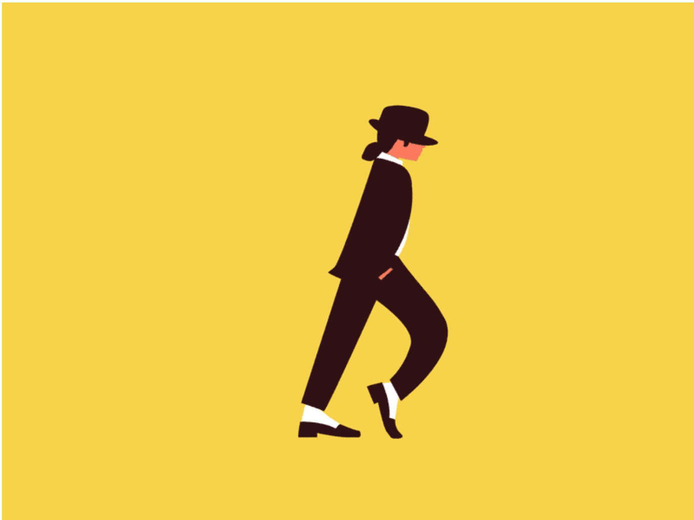
Reversing is hard

- We define addition, multiplication, exponentiation, etc.



https://www.flickr.com/photos/nenadstojkovic/50446472706/in/photostream/

- Subtraction, division, and roots, are reversing those operations and sometimes much harder.



Floris de Wit; https://dribbble.com/shots/5039546-Moonwalk

Division using multiplication table

mod 7

X	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

- Multiplication table encodes all pairs of products, so you can just look for the reverse.
- Example: $\frac{2}{5} \pmod 7$

Need x s.t. $x \cdot 5 \equiv 2 \mod 7$

$6 \cdot 5 \equiv 2 \mod 7$

$\Rightarrow \frac{2}{5} \equiv 6 \mod 7$

Roots using powers table

mod 7

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1	2	4	1	2	4	1	2
3	1	3	2	6	4	5	1	3	2	6	4	5	1	3
4	1	4	2	1	4	2	1	4	2	1	4	2	1	4
5	1	5	4	6	2	3	1	5	4	6	2	3	1	5
6	1	6	1	6	1	6	1	6	1	6	1	6	1	6

- A square root of a is a number b such that $b^2 \equiv a$.

Ex. $\sqrt{2} \equiv 3$ or 4.

$3^2 \equiv 9 \equiv 2 \mod 7$

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

- An kth root of a is a number b such that $b^k \equiv a$.

Ex. $\sqrt[5]{2} \equiv 2^{\frac{1}{5}} \equiv 4$

$4^1 \equiv 4$

$4^2 \equiv 16 \equiv 2$

$4^4 \equiv 4$

$4^5 \equiv 4^4 \cdot 4^1$

$\equiv 4 \cdot 4$

$\equiv 16 \equiv 2 \mod 7$

Roots using powers table

mod 7

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1	2	4	1	2	4	1	2
3	1	3	2	6	4	5	1	3	2	6	4	5	1	3
4	1	4	2	1	4	2	1	4	2	1	4	2	1	4
5	1	5	4	6	2	3	1	5	4	6	2	3	1	5
6	1	6	1	6	1	6	1	6	1	6	1	6	1	6

- How many answers for each of the following?
- $\sqrt[3]{5}$ no roots exist
- $\sqrt[3]{6}$ $\equiv$ 3, 5, 6 (3 roots)
- $\sqrt[5]{2}$ $\equiv$ 4 (1 root)
- $\sqrt[5]{3}$ $\equiv$ 5 (1 root)
- $\sqrt[13]{2}$ $\equiv$ 2 (1 root)

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

Think like a mathematician

- When do kth roots exist in mod p arithmetic?
- When are kth roots unique? (only one root)

mod 7

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1	2	4	1	2	4	1	2
3	1	3	2	6	4	5	1	3	2	6	4	5	1	3
4	1	4	2	1	4	2	1	4	2	1	4	2	1	4
5	1	5	4	6	2	3	1	5	4	6	2	3	1	5
6	1	6	1	6	1	6	1	6	1	6	1	6	1	6

In mod 7, kth roots always exist and are unique for

$k = 1, 5, 7, 11, 13, \ldots$

Pattern recognition

- We can write out tables for small primes, look at all columns with all numbers, and try to find a pattern.
- Numbers k such that we can always find kth roots mod p:
  - Mod 5: 1, 3, 5, 7, 9, 11, 13, 15, …
  - Mod 7: 1, 5, 11, 13, 17, 19, 23, …
  - Mod 11: 1, 3, 7, 9, 13, 17, 19, 21, …
  - Mod 13: 1, 5, 7, 11, 13, 17, 19, 23, 25, …
- Can you spot the pattern?

A: Numbers are all odd numbers
B: Numbers are all prime numbers
C: Numbers are relatively prime to p
D: Numbers are relatively prime to $p - 1$
E: None of the above

Prime modulus facts (mod p)

- You can uniquely divide by any number except 0.

$\frac{2}{5}$ mod 7

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1$

$1 = 5 - 2 \cdot 2$

$1 = 5 - (7 - 5) \cdot 2$

$1 = 5 \cdot 3 - 7 \cdot 2$

$1 \equiv 5 \cdot 3$ mod 7

$\frac{1}{5} \equiv 3$ mod 7

$\boxed{\frac{2}{5} \equiv 6 \text{ mod } 7}$

- Fermat's little theorem: $a^{p-1} \equiv 1 \pmod{p}$ if $a \not\equiv 0$.

$2^6 \equiv 1$ mod 7

$2^{600} \equiv (2^6)^{100} \equiv 1$ mod 7

$2^{602} \equiv 2^{600+2} \equiv 2^2 \equiv 4$ mod 7

Square roots

- In ordinary arithmetic, which of the following numbers is a square root of 1024? (without using a calculator?)

A: 25
B: 30
C: 32
D: 40
E: None of the above

- What if I told you $1024 = 2^{10}$? Then which of the following is a square root of 1024?

A: 5^2
B: $2 \cdot 3 \cdot 5$
C: 2^5
D: $2^3 \cdot 5$
E: None of the above

$$\sqrt{2^{10}} = \left(2^{10}\right)^{\frac{1}{2}} = 2^5 = 32$$

Square roots in mod 7

- In mod 7 arithmetic, what is the square root of 2?
- What if I told you $2 \equiv 1024 \equiv 2^{10}$? Then which of the following is a square root of 2?

$2^5 \cdot 2^5 \equiv 2^{10}$

$\Rightarrow \sqrt{2^{10}} \equiv 2^5$

$\sqrt{2} \equiv \sqrt{2^{10}} \equiv 2^5 \equiv 32 \equiv 4 \mod 7$

A: 1
B: 2
C: 3
D: 4
E: None of the above

- What if I told you $2 \equiv 9 \equiv 3^2$? Then which of the following is a square root of 2?

$\sqrt{2} \equiv \sqrt{9} \equiv 3 \mod 7$

A: 1
B: 2
C: 3
D: 4
E: None of the above

Higher roots

- In mod 7 arithmetic, what is the fifth root of 2?
- Strategy: use Fermat's little theorem to find an equivalent of 2 as a power whose exponent is a multiple of 5.

$\sqrt[5]{2}$.

Fermat's Little thm:

$$2^6 \equiv 1$$

$$\Rightarrow \quad 2 \equiv 2 \cdot 1 \equiv 2 \cdot 2^6 \equiv 2^7$$

$$2 \equiv 2^7 \equiv 2^{13} \equiv 2^{19} \equiv \underline{2^{25}}$$

$$\sqrt[5]{2} \equiv 2^{\frac{1}{5}} \equiv \left(2^{25}\right)^{\frac{1}{5}} \equiv 2^5 \equiv 32 \equiv 4 \mod 7.$$

$\boxed{\text{Ex. to check: } 4^5 \equiv 2 \mod 7}$

Try it out

- In mod 7 arithmetic, what is a 5th root of 3?

$3^6 \equiv 1$ So,

$3^1 \equiv 3^7 \equiv 3^{13} \equiv 3^{19} \equiv 3^{25}$

Thus, $3 \equiv 3^{25}$

$\Rightarrow \sqrt[5]{3} \equiv 3^{25 \cdot \frac{1}{5}} \equiv 3^5 \equiv 3^4 \cdot 3$

$\equiv 4 \cdot 3 \equiv 12 \equiv \boxed{5}$

$3^1 \equiv 3$

$3^2 \equiv 9 \equiv 2$

$3^4 \equiv 4$

A: 2
B: 3
C: 4
D: 5
E: None of the above

Backwards reasoning for finding roots

- To solve $\sqrt[k]{a} \pmod{p}$, we need to find a number b such that $b^k \equiv a \pmod{p}$.

Ex. $\sqrt[3]{2} \bmod 11$. Ans: $7^3 \equiv 343 \equiv 2 \bmod 11$

- One way to attempt this is to see if there exists a power m such that $b \equiv a^m$.

Ex. $2, 4, 8, \underset{\downarrow}{16}, 10, \underset{\downarrow}{20}, \underset{\downarrow}{18}$
$\ 5 \qquad\quad\ 9 \quad\ 7$

$2^7 \equiv 7 \bmod 11$

- That works precisely when $a^{mk} \equiv a \pmod{p}$

$2^{7\cdot 3} \equiv 2^{21} \equiv 2 \pmod{11}$ because $2^{10} \equiv 1$.

$2 \equiv 2^{11} \equiv 2^{21}$

When does that strategy work?

- We need $a^{km} \equiv a \pmod{p}$.
- Or in other words, we need an exponent that is a multiple of k such that the two are equivalent.
- Fermat's Little Theorem says that

$$1 \equiv a^{(p-1)l}$$
$$a \equiv a^{(p-1)l+1}$$

- Equivalently, need to find integers m and l such that

$$mk = l(p-1) + 1$$

- We can rewrite this as:

$$1 = m\underline{k} - l(\underline{p-1})$$

- Or, in other words, the strategy works if 1 is a combination of k and $p-1$, which is true precisely when $\gcd(k, p-1) = 1$ (relatively prime)

One algorithm for $b \equiv \sqrt[k]{a} \bmod p$

- This algorithm works *if*
  - p is prime
  - $a \not\equiv 0 \bmod p$
  - k is relatively prime to $p-1$

} required for Fermat's Little thm

← needed to find a linear combo for 1

- Find $1 = mk - l(p-1)$ using reverse Euclidean alg

Ex. $\sqrt[3]{3} \bmod 11$

$\gcd(\underset{k}{3}, \underset{p-1}{10})$

$10 = 3 \cdot 3 + 1$

$1 = 10 - 3 \cdot 3$

$1 = \underbrace{(-3)}_{m} \cdot \underset{k}{3} - \underbrace{(-1)}_{l} \cdot \underset{p-1}{10}$

- Then $\sqrt[k]{a} \equiv a^m \bmod p$. Solve for $b \equiv a^m \bmod p$.

$b \equiv 3^{-3} \equiv 3^{-3+10} \equiv 3^7 \bmod 11 \equiv 3 \cdot 3^2 \cdot 3^4$

$3 \equiv 3$

$3^2 \equiv 9$

$3^4 \equiv 81 \equiv 4$

$\equiv 3 \cdot 9 \cdot 4 \bmod 11$

$\equiv 9 \bmod 11$

- Check that $b^k \equiv a \pmod p$

$9^3 \equiv 3 \bmod 11$

Worked example

- $\sqrt[5]{10} \bmod 13$

Find 1 as combo of 5 & 12

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

$$1 = 5 - 2\cdot 2$$
$$1 = 5 - 2\cdot(12 - 5\cdot 2)$$
$$1 = \underset{k}{5}\cdot\underset{m}{5} - \underset{p-1}{12}\cdot\underset{2}{2}$$

$$\sqrt[5]{10} \equiv 10^5 \bmod 13$$

$$10^{25} \equiv 10^{12\cdot 2+1} \equiv 10^1 \bmod 13$$

$$10^1 \equiv 10$$
$$10^2 \equiv 100 \equiv 9 \bmod 13$$
$$10^4 \equiv 81 \equiv 3$$

$$10^5 \equiv 10^4\cdot 10 \equiv 3\cdot 10$$
$$\equiv 30 \equiv \boxed{4 \bmod 13}$$

Check: $4^5 \stackrel{?}{\equiv} 10 \bmod 13$

$$4^1 \equiv 4$$
$$4^2 \equiv 16 \equiv 3$$
$$4^4 \equiv 9$$

$$4^5 \equiv 9\cdot 4 \equiv 36 \equiv 10 \bmod 13$$

✓

Try it out

- Let p be prime, and $\gcd(k, p-1) = 1$.
- Given $b = \sqrt[k]{a} \pmod p$, find $1 = mk - l(p-1)$.
- Solution $b = a^m$
- Solve: $\sqrt[3]{6}$ mod 17

Find 1 as a combo of 3 & 16

$16 = 3 \cdot 5 + 1$

$1 = 16 - 3 \cdot 5$

$1 = 3 \cdot (-5) - 16 \cdot (-1)$

m l

Sol: 6^{-5} mod 17

$\equiv 6^{11}$ mod 17

$6^1 \equiv 6$

$6^2 \equiv 36 \equiv 2$

$6^4 \equiv 4$

$6^8 \equiv 16 \equiv -1$

$6^{11} \equiv 6^8 \cdot 6^2 \cdot 6 \equiv -1 \cdot 2 \cdot 6$

$\equiv -12 \equiv 5$ mod 17

A: 2
B: 3
C: 4
D: 5
E: None of the above

Try it out

- Let p be prime, and $\gcd(k, p-1) = 1$.
- Given $b = \sqrt[k]{a} \pmod{p}$, find $1 = mk - l(p-1)$.
- Solution $b = a^m$
- Solve: $\sqrt[4]{6}$ mod 17

Doesn't work since $\gcd(4, 16) = 4$.

A: 2
B: 3
C: 4
D: 5
E: None of the above