

Example:

Find all positive real solutions to

$$4x^3 = 7$$



Way one:

$$x^3 = \frac{7}{4}$$

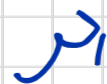
$$x = \left(\frac{7}{4}\right)^{1/3}$$



$$\log(4x^3) = \log(7)$$

$$\log(4) + 3 \log(x) = \log(7)$$

$$\log(x) = \frac{\log(7) - \log(4)}{3}$$



$$\begin{aligned} x &= e^{\frac{\log 7 - \log 4}{3}} \\ &= \left(e^{\log 7} e^{-\log 4}\right)^{1/3} \\ &= \left(\frac{7}{4}\right)^{1/3} \end{aligned}$$

base e

$$4x^3 = 7 \pmod{11}$$

$$x^3 = \frac{7}{4} \pmod{11}$$

$$x = \left(\frac{7}{4}\right)^{1/3} \pmod{11}$$

where d is
the mult. inverse
of 3
mod 10 .

$$\left(\frac{7}{4}\right)^d$$

(In \mathbb{F}_p , a^k only depends on $k \pmod{p-1}$
by Lagrange's theorem $|\mathbb{F}_p^\times|$)

$I =$ discrete logarithm for \mathbb{F}_{11} with base 2

$2^y = x$	1	2	3	4	5	6	7	8	9	10
$y = I(x)$	0	1	8	2	4	9	7	3	6	5

$$4x^3 = 7 \pmod{11}$$

← exponent is in $\mathbb{Z}/10\mathbb{Z}$

$$I(4x^3) = I(7) \pmod{10}$$

$$I(4) + 3I(x) \equiv I(7) \pmod{10}$$

← use the table

$$2 + 3I(x) \equiv 7 \pmod{10}$$

$$3I(x) \equiv 5 \pmod{10}$$

$$I(x) \equiv \frac{5}{3} \pmod{10}$$

$$\frac{1}{3} = 7$$

$$I(x) \equiv 7 \cdot 5 \pmod{10}$$

$$I(x) \equiv 5$$

$$x \equiv 2^5 \equiv 10 \pmod{11}$$

$$x \equiv 10 \pmod{11}$$

↙
Plug in to check this is a solution

$$4(10)^3 \equiv 4(-1)^3 \equiv -4 \equiv 7 \pmod{11} \quad \checkmark$$

2-(2)-(c)

$$\text{Solve } 4x^2 \equiv 9 \pmod{11}$$

$$I(4x^2) = I(9) \pmod{10}$$

$$I(4) + 2I(x) = I(9) \pmod{10}$$

$$2I(x) \equiv 4 \pmod{10}$$

~~$$I(x) \equiv 2 \pmod{10}$$~~

Cannot divide by 2 mod 10, so this is one solution, but there can be more.

One way: Try every possibility for $I(x)$
 $\leadsto I(x) = 2 \quad I(x) = 7.$

Systematic way: use CRT \sim $2 \cdot 5 = 10$.

$$y = T(x)$$

Solve $2y \equiv 4 \pmod{2}$

$$2y \equiv 4 \pmod{5}$$

$$0y \equiv 0 \pmod{2}$$

$$y \equiv 0 \text{ or } 1 \pmod{2}$$

$$(2^{-1} = 3 \pmod{5})$$
$$y \equiv 2 \pmod{5}$$

$$y \equiv 0 \pmod{2} \quad y \equiv 2 \pmod{5} \Rightarrow y \equiv \underline{2} \pmod{10}$$

$$y \equiv 1 \pmod{2} \quad y \equiv 2 \pmod{5} \Rightarrow y \equiv \underline{7} \pmod{10}$$

$$x = 2^2 \text{ or } 2^7$$

$$4 \text{ or } 7 \pmod{11}, \quad (7 = -4)$$
$$x^2 = (-x)^2$$

$M_l = 2^l - 1$ \leftarrow when this is prime,
it's called a Mersenne
prime.

(To be prime, it is necessary, but not
sufficient that l be prime)

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$$

Lucas-Lehmer Test.

$$S_1 = 4$$

$$S_{n+1} = S_n^2 - 2$$

Fact: M_l is prime $\Leftrightarrow S_{l-1} \equiv 0 \pmod{M_l}$
i.e. $M_l \mid S_{l-1}$.

Exercise³: Use HB to find all Mersenne primes M_l with $l \leq 31$.

To check for M_l ,
compute S_{l-1} by following recursion
mod M_l .

$$l = 5$$

$$M_l = 2^5 - 1 = 31$$

i	1	2	3	4
$S_i \pmod{31}$	4	14	8	0

$$S_{n+1} = S_n^2 - 2$$

$$14^2 - 2 = 194$$

$$= 8 \pmod{31}$$

$$8^2 - 2 = 62 \equiv 0 \pmod{31}$$

$$l = 2 \quad M_l = 3$$

$$S_{l-1} = 4 \quad 3 \times 4 \text{ but } 3 \text{ is prime.}$$

doesn't work for $l=2$,
OK for $l > 2$.

$$S_1 = 4$$

$$S_{n+1} = S_n^2 - 2$$

l odd prime
($l \neq 2$)