WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com

Foundational Mathematics for Web3 Builders

Lecture 18

May 30, 2024

Euler's Theorem

1.1 Euler phi function, $\phi(n)$

Definition 1

Euler phi function, denoted $\phi(n)$, is the number of positive integers less than n which are relatively prime to n.

Some texts use the symbol $\varphi(n)$.

The following table gives $\phi(n)$ for $n = 1, 2, 3, \cdots, 14$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6

In general, if p is a prime number, $\phi(p) = p - 1$.

If n is a positive integer with prime factors $p_1,\ p_2,\ p_3,\ \cdots,\ p_k$ then

$$\phi(n) = (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \cdots (1 - \frac{1}{p_k})n.$$

Example 1

Denote the Euler phi function by $\phi(n)$. Find:

a) $\phi(19)$ b) $\phi(840)$ c) $\phi(930)$

Solution

Since 19 is prime, $\phi(19) = 19 - 1 = 18$

$$\begin{aligned}\phi(840) &= \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} \times 840 \\ &= 192\end{aligned}$$

$$\begin{aligned}\phi(930) &= \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{30}{31} \times 930 \\ &= 240\end{aligned}$$

Example 2

Find:

a) $\phi(4900)$ b) $\phi(765)$.

Solution

a) Since $4900 = 2^2 \times 5^2 \times 7^2$, we have

$$\phi(4900) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) 4900$$

$$= \frac{1}{2} \times \frac{4}{5} \times \frac{6}{7} \times 4900 = 1680$$

b) Since $765 = 3^2 \times 5 \times 17$, we have

$$\phi(765) = \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{17}\right) \times 765$$

$$= \frac{2}{3} \times \frac{4}{5} \times \frac{16}{17} \times 765 = 384$$

Revision Questions 1

Show that

a) $\phi(15) = 8$

b) $\phi(29) = 28$

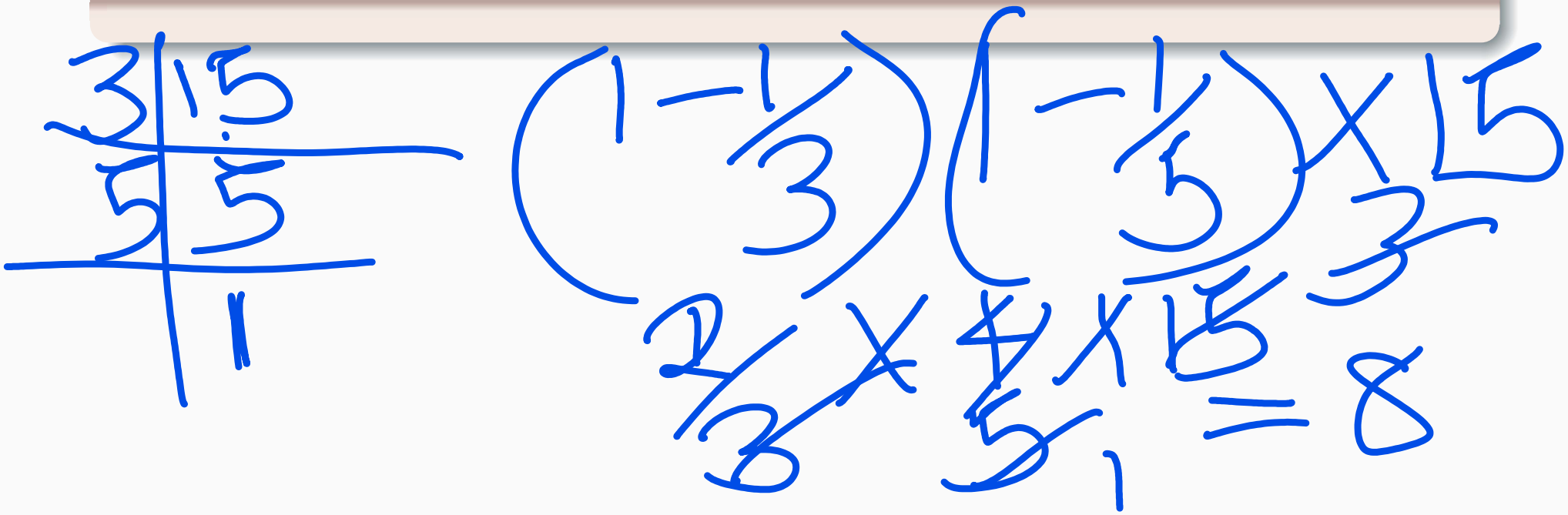
c) $\phi(20) = 8$

d) $\phi(715) = 480$

e) $\phi(716) = 356$

f) $\phi(718) = 358$

Solution



Solution (conti...)

$\phi(29) =$

$\phi(p) = p - 1$

$= 29 - 1$

$= \underline{28}$

Solution (conti...)

$\phi(20)$

2	20
2	10
5	5
	1

$2 \times 2 \times 5 = 2^2 \times 5$

$= (2, 5)$

$\phi(n) = (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$

$\phi(20) = (1 - 1/2)(1 - 1/5)20$

$= 1/2 \times 4/5 \times 20 = 8$

Solution (conti...)

$\phi(715)$

5	715
11	143
13	13
	1

$5 \times 11 \times 13$

$\phi 715 = \left(1-\frac{1}{5}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)715$

$\frac{4}{5} \times \frac{10}{11} \times \frac{12}{13} \times 715$

$= 480$

Solution (conti...)

$\phi(716)$

2	716
2	358
179	179
	1

$\phi(716) = (1-\frac{1}{2})(1-\frac{1}{179})716$

$= \frac{1}{2} \times \frac{178}{179} \times 716$

$= 4 \times 89 = 356$

Solution (conti...)

$718 = 2 \times 359$

$1 \times 358 = 358$

$\phi(718)$

2	718
359	359
	1

$(p-1)(q-1) = \phi(n)$

$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{359}\right) = 714$

179

$1 \times 358 \times 718^2 = 358$

2 359

1 1

Solution (conti...)

1.2 Euler's Theorem

Theorem 2 (Euler's Theorem)

Let $m \in \mathbb{Z}$ and a be an integer relatively prime to m. Then

$$a^{\phi(m)} \equiv 1 \bmod m$$

Example 3

Find the last digit of 3^6.

Solution

To find the last digit of 3^6 we reduce $3^6 \bmod 10$.

Since $\gcd(3, 10) = 1$, we use Euler's Theorem.

Thus, $3^{\phi(10)} \equiv 1 \bmod 10$ or $3^4 \equiv 1 \bmod 10$.

By division algorithm, $6 = 4 \cdot 1 + 2$.

Thus $3^6 \bmod 10 = 3^2 \bmod 10 = 9 \bmod 10$

Therefore, last digit of 3^6 is 9.

Example 4

Find the last digit of 27^{71}.

Solution

To find the last digit of 27^{71} we reduce $27^{71} \bmod 10 = 7^{71} \bmod 10$.

Since $\gcd(7, 10) = 1$, we use Euler's Theorem.

Thus, $7^{\phi(10)} \equiv 1 \bmod 10$ or $7^4 \equiv 1 \bmod 10$.

By division algorithm, $71 = 4 \cdot 17 + 3$.

Thus $7^{71} \bmod 10 = 7^3 \bmod 10$

$$= 343 \bmod 10 = 3$$

Therefore, last digit of 27^{71} is 3.

Example 5

Find the last digit of 55^{29}

Solution

To find the last digit of 55^{29} we reduce $55^{29} \bmod 10$

We want to use Euler's Theorem but $\gcd(55, 10) = 5$ so we can't use it directly. So first, $55 = 5 \cdot 11$.

Thus, $55^{29} = 5^{29} \times 11^{29}$.

Since $\gcd(11, 10) = 1$, we have that $11^{\phi(10)} = 1 \bmod 10$ or $11^4 = 1 \bmod 10$. Since $29 = 4 \cdot 7 + 1$, we have that $11^{29} = 11^1 = 11$.

Thus, $5^{29} \times 11^{29} = 5^{29} \times 11 \bmod 10$

Let us use the fast powering algorithm to solve $5^{29} \bmod 10$.

$5^1 = 5$ $\quad$ $5^4 = 5$ $\quad$ $5^{16} = 5$

$5^2 = 5$ $\quad$ $5^8 = 5$ $\quad$ $5^{29} = 5^{16} \times 5^8 \times 5^4 \times 5^1 = 5$

Thus $5^{29} \times 11 \bmod 10 = 5 \times 11 = 55 \bmod 10$.

The last digit is 5.

Example (conti...)

Note that we can still do these questions using fast powering algorithm. Take example 4 for instance, and compute $27^{71} \bmod 10 = 7^{71} \bmod 10$ by fast powering algorithm.

$$7^1 = 7$$
$$7^2 = 9$$
$$7^4 = 1$$

Since $7^4 = 1$, our work has been simplified.

By division algorithm, $71 = 4 \cdot 17 + 3$

Thus,

$$\begin{aligned} 7^{71} &= 7^3 \\ &= 7^{2+1} \\ &= 7 \times 9 = 3 \bmod 10 \end{aligned}$$

Example 6

Find the last two digits of 1111^{71023}

Solution

To find the last two digits of 1111^{71023} we reduce $1111^{71023} \bmod 100 = 11^{71023} \bmod 100$. Since $\gcd(11, 100) = 1$, we use Euler's Theorem. Here, $\phi(100) = \frac{1}{2} \times \frac{4}{5} \times 100 = 40$

Thus, $11^{\phi(100)} \equiv 1 \bmod 100$ or $11^{40} \equiv 1 \bmod 100$.

By division algorithm, $71023 = 40 \cdot 1775 + 23$.

Thus $11^{71023} \bmod 100 = 11^{23} \bmod 100$.Thus;

$11^1 = 11$

$11^2 = 21$

$11^4 = 41$

$11^8 = 81$

$11^{16} = 61$

$11^{23} = 11^{16} \times 11^4 \times 11^2 \times 11^1$

$= 61 \times 41 \times 21 \times 11$

$= 577731$

Therefore, last two digits of 1111^{71023} is 31.

Example 7

Find the last three digits of 17^{20001}.

Solution

To find the last three digits of 17^{20001} we reduce $17^{20001} \bmod 1000$.

Since $\gcd(17, 1000) = 1$, we use Euler's Theorem. Here, $\phi(1000) = \frac{1}{2} \times \frac{4}{5} \times 1000 = 400$

Thus, $17^{\phi(1000)} \equiv 1 \bmod 1000$ or $17^{400} \equiv 1 \bmod 1000$.

By division algorithm, $20001 = 400 \cdot 50 + 1$.

Thus $17^{20001} \bmod 1000 = 17^1 \bmod 1000 = 17$.

Therefore, last three digits of 17^{20001} is 017.

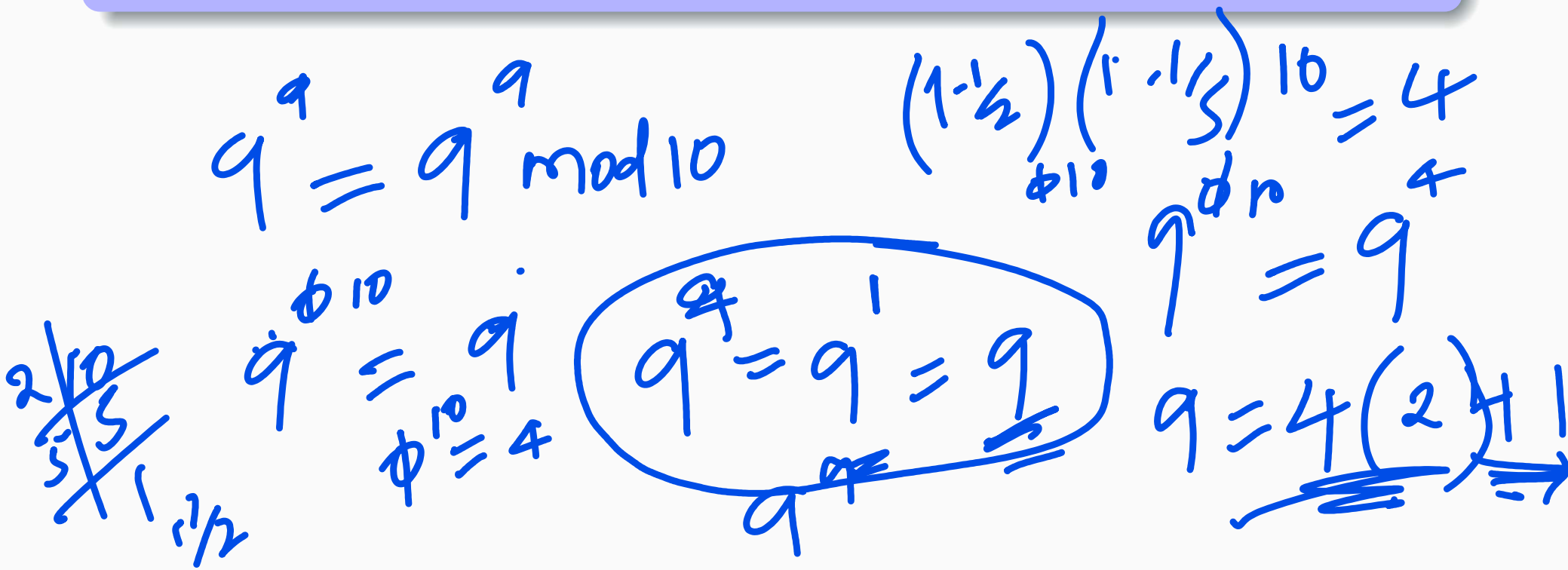
Revision Questions 2

1. Find the last digit of:

   a) 9^9 b) 3^{20} c) 4^{10} d) 15^{33}

2. Find the last two digits of:

   a) 9^9 b) 3^{230} c) 4^{53} d) 115^{72}



Solution (conti...)

3^{20}

$a^{\phi(n)} \equiv 1 \bmod n$

$3^{\phi(10)} \equiv 1 \bmod 10$

$3^4 \equiv 1 \bmod 10$

$3^{4 \times 5} \equiv 1 \bmod 10$

$3^{20} \equiv 1 \bmod 10$

$20 = 5(4) + 0$

$(3^{4})^{5} \times 3^{0}$

$1^{5} \times 1 = 1$

Solution (conti...)

$4^{10} \bmod 10$

$4^1 = 4$

$4^2 = 6$

$4^3 = 6$

$4^4 = 6$

4

$4^{10} = 4^{(8+2)}$

$= 4^8 \times 4^2$

$= 6 \times 6$

$= 36 \bmod 10$

$= 6$

Solution (conti...)

$15^{33} \bmod 10$

$(15, 10)$

$5^{33} \bmod 10$

$5^1 = 5$

$5^2 = 5$

$5^4 = 5$

$5^8 = 5$

$5^{16} = 5$

$5^{32} = 5$

$5^{33} \bmod 10 = 15^{33} \bmod 10$

$5^{33} = 5^{32+1}$

$= 5^{32} \times 5^1$

$= 5 \times 5$

$= 25 \bmod 10$

$= 5$

Solution (conti...)

$9^9 \bmod 100$

$9^1 = 9$

$9^2 = 81$

$9^4 = 61$

$9^8 = 21$

$9^9 = 9^{8+1} = 9^8 \cdot 9^1$

$= 21 \times 9 = 189$

$189 \bmod 100 = 89$

Solution (conti...)

$3^{230} \bmod 100$

$a^{\phi(n)} \equiv 1 \bmod n$

$\phi(100) = 40$

$3^{40} \equiv 1 \bmod 100$

$230 = 5(40) + 30$

$(3^{40})^5 \times 3^{30}$

$1^5 \times 3^{30}$

$3^{30} \bmod 100$

$3^1 = 3$

$3^2 = 9$

$3^4 = 81$

$3^8 = 61$

$3^{16} = 21$

$3^{30} = 3^{16+8+4+2}$

Solution (conti...)

$3^{16} \times 3^{8} \times 3^{4} \times 3^{2}$

$= 21 \times 61 \times 81 \times 9$

$= 933849 \bmod 10$

$= 9$

Solution (conti...)

4^{53}

$4^{53} \bmod 100$

$4^1 = 4$

$4^2 = 16$

$4^4 = 56$

$4^8 = 36$

$4^{16} = 96$

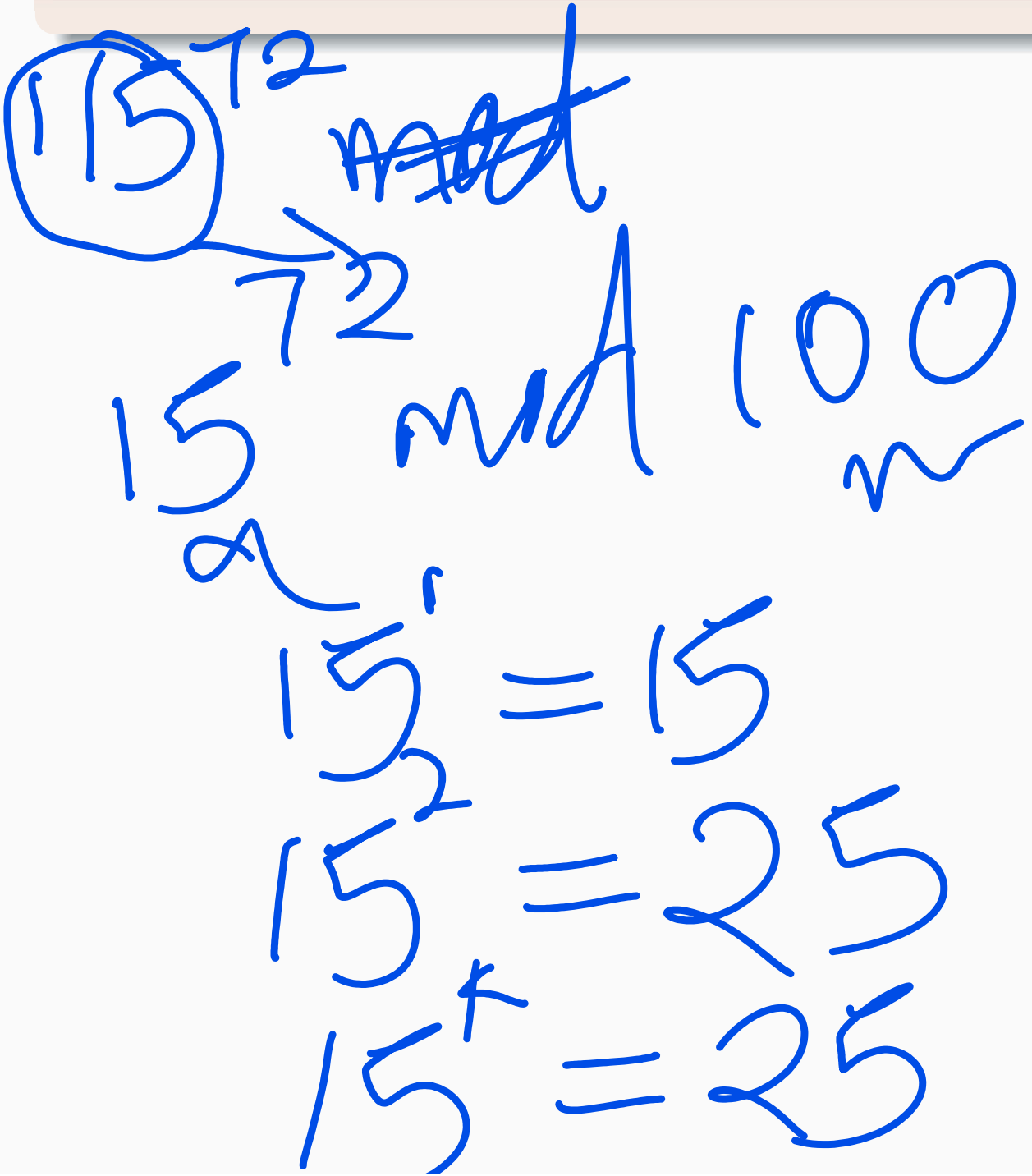
$4^{32} = 16$

$4^{53} = 4^{32+16+4+1}$

$= 16 \times 96 \times 56 \times 4$

$= 344064 \bmod 100$

Solution (conti...)



Solution (conti...)

$$15^{8} = 25$$

$$15^{16} = 25$$

$$15^{32} = 25$$

$$15^{64} = 25$$

$$72 = 64 + 8$$

Solution (conti...)

$15^{64} \times 15^{8}$

25×25

$625 \bmod 100$

25