Errata

One-time Ring Signature

One-Time ECC Ring Sign.

- Given:
  - $L_i = c_i P_i + d_i G$ $\qquad R_i = c_i I + d_i \mathscr{H}(P_i)$
  - $L_{\text{own}} = rG$ $\qquad R_{\text{own}} = rI$
- $c = \mathscr{H}\left(\text{document} \,|\, G \,|\, I \,|\, L_1 \,|\, \ldots \,|\, L_n \,|\, R_1 \,|\, \ldots \,|\, R_n\right)$
- $c_{\text{own}} = c - \sum_i c_i$ $\qquad d_{\text{own}} = r - c_{\text{own}} p$
- $L_{\text{own}} = c_{\text{own}} P + d_{\text{own}} G$

One-Time ECC Ring Sign.

- Given:
  - $L_i = c_i P_i + d_i G$ $\qquad R_i = c_i I + d_i \mathscr{H}(P_i)$
  - $L_{\text{own}} = rG$ $\qquad R_{\text{own}} = r\mathscr{H}(P)$
- $c = \mathscr{H}\left(\text{document} \,|\, G \,|\, I \,|\, L_1 \,|\, \ldots \,|\, L_n \,|\, R_1 \,|\, \ldots \,|\, R_n\right)$
- $c_{\text{own}} = c - \sum_i c_i$ $\qquad d_{\text{own}} = r - c_{\text{own}} p$
- $L_{\text{own}} = c_{\text{own}} P + d_{\text{own}} G$

Lelantus error 1

1-in-N Σ−Protocol

- New Problem:
  - $\{Y_1, Y_2, \ldots, Y_n\}$, $Y_i = m_i G + s_i H$, $Y_t = 0G + s_t H$
- but now we have

$$f_1 Y_1 + f_2 Y_2 + \ldots + f_n Y_n$$

$$= (m_1 x + a_1) Y_1 + (m_2 x + a_2) Y_2 + \ldots + (m_n x + a_n) Y_n$$

$$= m_k x Y_k + \sum a_k Y_k$$

Opens to 0

independent of x,
can be send beforehand
in a Pedersen Commitment

1-in-N $\Sigma-$Protocol

- New Problem:
  - $\{Y_1, Y_2, \ldots, Y_n\}, Y_i = m_i G + s_i H, Y_t = 0G + s_t H$
- but now we have

$$f_1 Y_1 + f_2 Y_2 + \ldots + f_n Y_n$$

$$= (m_1 x + a_1) Y_1 + (m_2 x + a_2) Y_2 + \ldots + (m_n x + a_n) Y_n$$

$$= m_1 x Y_k + \sum a_k Y_k$$

Wrong

Opens to 0

independent of x,

forehand

in a Pedersen Commitment

- but now we have

$$f_1 Y_1 + f_2 Y_2 + \ldots + f_n Y_n$$

$$= (m_1 x + a_1) Y_1 + (m_2 x + a_2) Y_2 + \ldots + (m_n x + a_n) Y_n$$

$$= \sum_k m_k x Y_k + \sum_{k=0}^{n-1} b_k x^k Y_k' = \left(\sum m_k Y_k \right) x^k + \text{lower order terms}$$

for some terms b_k

$$= (m_1 x + a_1)Y_1 + (m_2 x + a_2)Y_2 + \ldots + (m_n x + a_n)Y_n$$

$$= \sum_k m_k x Y_k + \sum_{k=0}^{n-1} b_k x^k Y'_k = \left(\sum m_k Y_k \right) x^k + \text{lower order terms}$$

We send these b_k terms to the verifier to subtract:

$$R = f_1 Y_1 + f_2 Y_2 + \ldots + f_n Y_n - \sum_{k=0}^{n-1} b_k x^k Y'_k$$

And proof that R opens to 0. Without the terms, R is simply

$$R = \left(\sum m_k Y_k \right) x^k = Y_i x^k$$

All $m_k \in 0,1 \Rightarrow$ the verify does not know which $m_i Y_i$ term is $\neq 0$

Lelantus error 2

Leleantus error 2

- A jointSplit transaction produces coins with secret serial numbers

  - The transaction kernel is

$$\mathsf{In}_1 + \ldots + \mathsf{In}_n - \mathsf{Out}_1 - \ldots - \mathsf{Out}_m - \underbrace{eG}_{\text{extra output}} = \underbrace{0G + \delta H + \varepsilon F}_{\text{transaction kernel}}$$

instead of

$$\mathsf{In}_1 + \ldots + \mathsf{In}_n - \mathsf{Out}_1 - \ldots - \mathsf{Out}_m - \underbrace{eG}_{\text{extra output}} = \underbrace{0G + 0H + \varepsilon F}_{\text{transaction kernel}}$$

Leleantus JoinSplit

- Similarly to MimbleWimble transactions:

wrong

$$\text{In}_1 + \ldots + \text{In}_n - \text{Out}_1 - \ldots - \text{Out}_m - \underbrace{eG}_{\text{extra output}} = \underbrace{0G + 0H + \varepsilon F}_{\text{transaction kernel}}$$

1. For every input, present a 1-in-N Σ-protocol

   - publish Serial #, 1-in-N proof provides transaction input

$$\underbrace{c_1}_{=0} Y_1 + \underbrace{c_2}_{=0} Y_2 + \ldots + \underbrace{c_t}_{=1} Y_t + \ldots + \underbrace{c_n}_{=0} Y_n = \underbrace{Z}_{vG+0F+\gamma' F}$$

Leleantus JoinSplit

- Similarly to MimbleWimble transactions:

wrong

$$T = \mathrm{In}_1 + \ldots + \mathrm{In}_n - \mathrm{Out}_1 - \ldots - \mathrm{Out}_m - eG = \underbrace{0G + 0H + \varepsilon F}$$

transaction kernel

2. Proof that transaction kernel *only consists of Fs* with Schnorr Signature

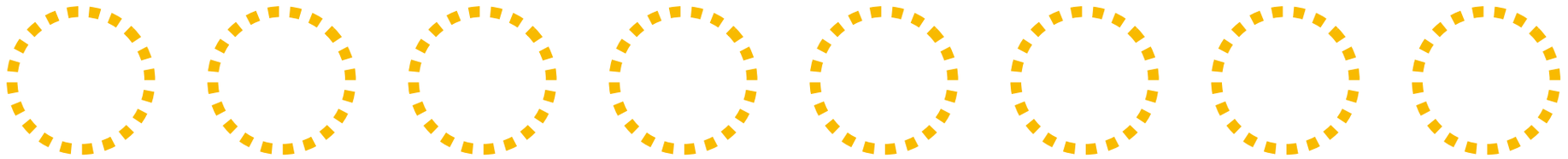
$$(s, R), \text{ so that } \underbrace{sF}_{\text{only F}} = \underbrace{R}_{\text{only F}} + \mathscr{H}(R \mid T) \underbrace{T}_{\text{only F}}$$

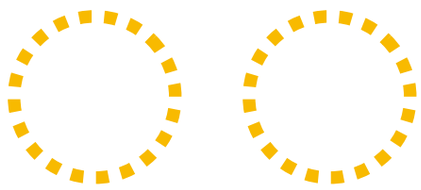
Lelantus JoinSplit

Used serial#

e8fb04ab61cfdd9ab54d9b1
ea6a1728b274a7e3c667523
cdcb04f2b45a6dd3c13e90c
050cf72a2c4ff1f4df4084a
5a35670340e4107632e4629
f59cc4cef45a8063e4afb65
2d28e9bb87f78a5c0b6b008
1c4433bd43daafa3806759b
4f587540daa9bcb002b3699
a6e434bb929b8c4d9adf1fb
73f143adf73708de491ff9d
95b96411c8dc99f6be2b443
…

hidden coins (Pedersen Commitments)





Proof of valid transaction: (c, d, α)

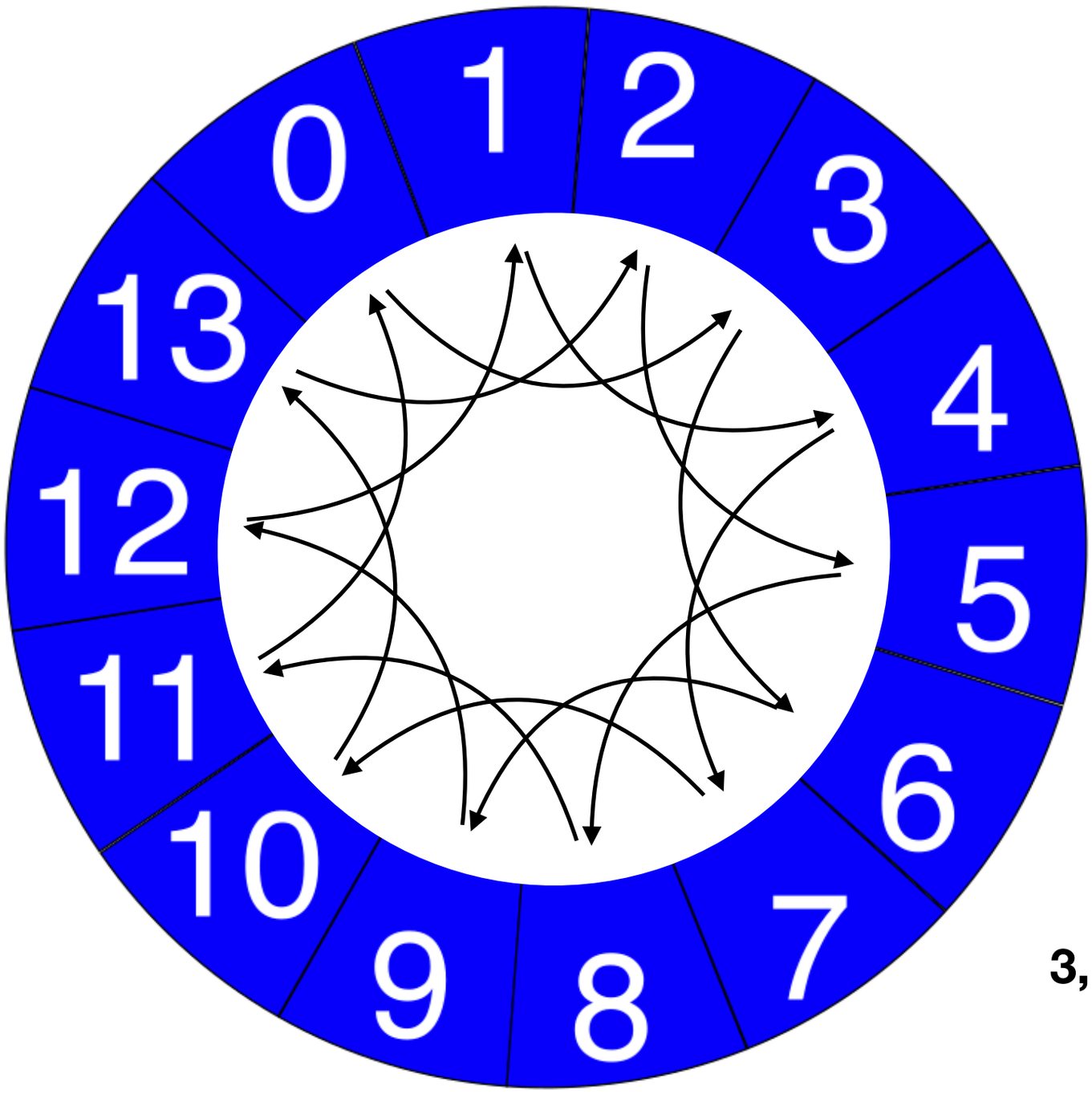
Input1 + Input2 + Input3 + Output1 + Output2 + ExtraCashOut=T

If $c = \mathscr{H}(T \,|\, cT + dH + \alpha F)$, then T can be described as a factor of only H and F:

- does not have any G components = no money was created or destroyed

Module Math

Module Math



N not prime (14)

Group order:

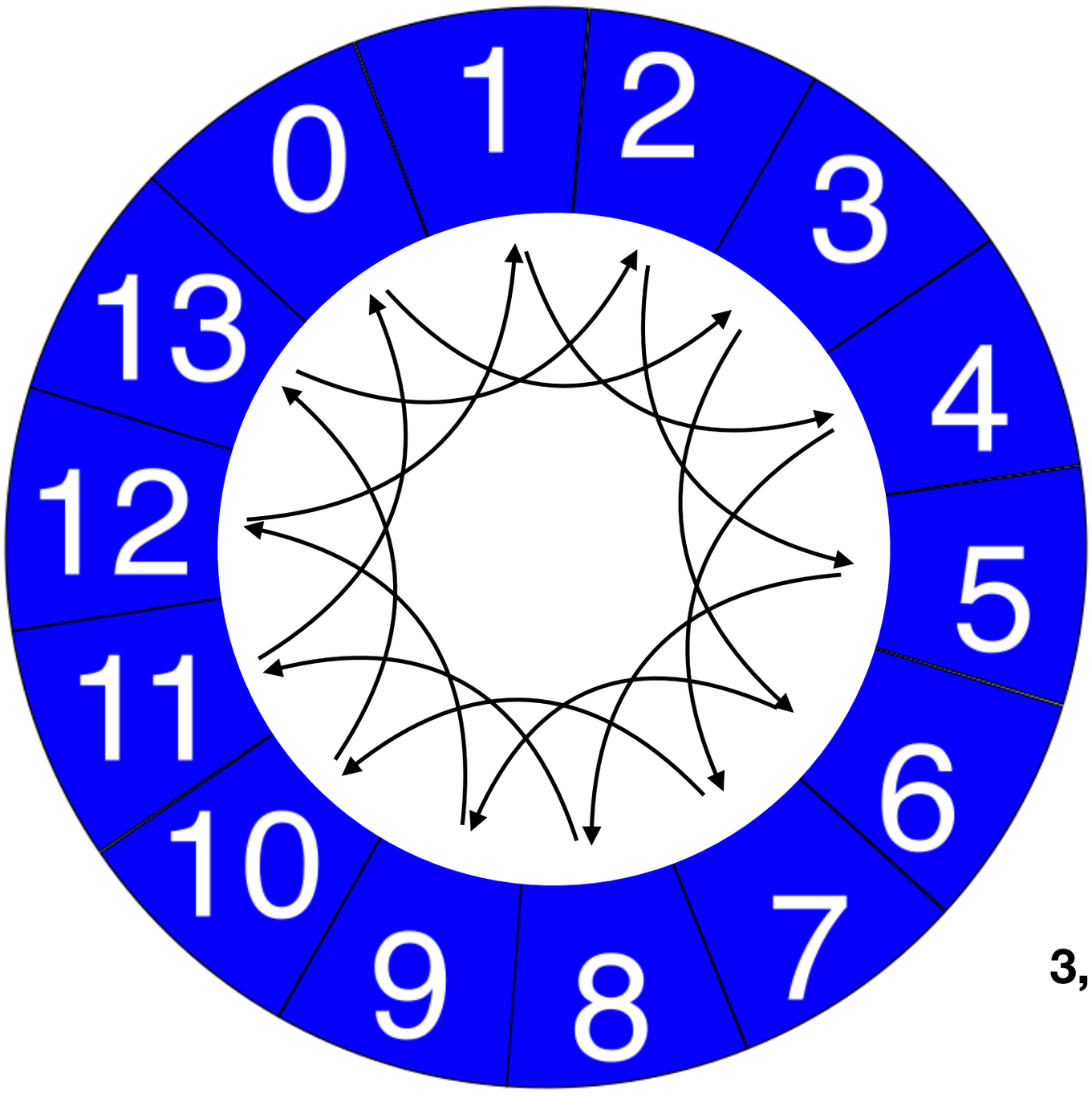
How often can I multiply an element before I get back to the beginning

Example: base element 3

3, 6, 9, 12, 1, 4, 7, 10, 13, 2, 5, 8, 11, 0

order 14

Module Math



N not prime (14)

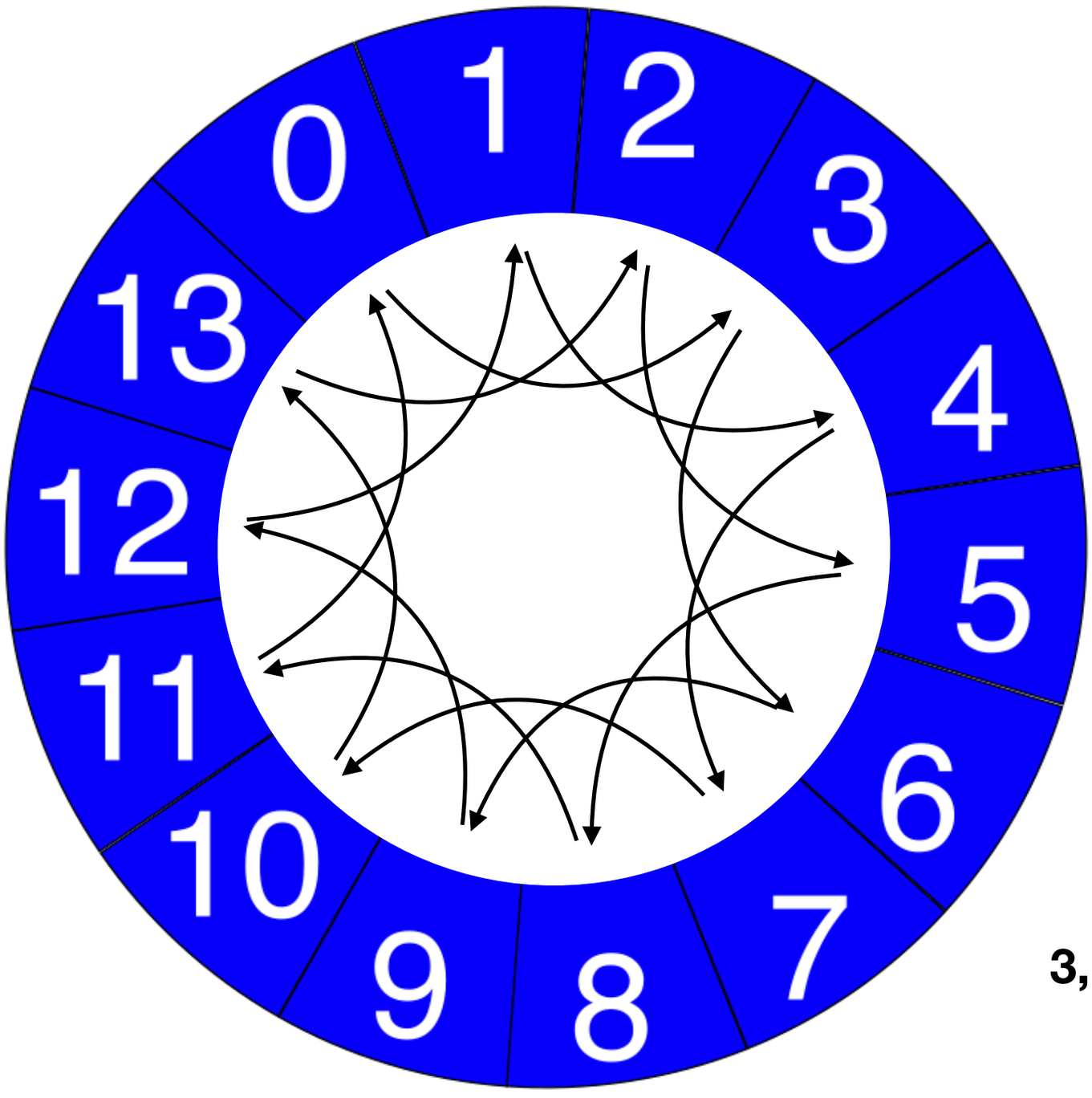
Order of the induced sub-group

How often can I multiply an element before I get back to the beginning

Example: base element 3

3, 6, 9, 12, 1, 4, 7, 10, 13, 2, 5, 8, 11, 0

Module Math



N not prime (14)

Group order:

Number of generators,
i.e. how many elements x exist that can generate the entire group via $x, 2x, 3x, \ldots$

Example: base element 3

3, 6, 9, 12, 1, 4, 7, 10, 13, 2, 5, 8, 11, 0