Tajemnice liczb pierwszych i tych drugich

Barbara Roszkowska-Lech

MATEMATYKA DLA CIEKAWYCH ŚWIATA

"Liczby całkowite stworzył dobry Bóg, wszystko inne wymyślili ludzie"

Leopold Kronecker (1823-1891)

Liczby rzadzą światem

Kongruencje czyli arytmetyka zegara

Definicja

$$a \equiv b(mod n) \Leftrightarrow n|a - b$$

Kongruencje czyli arytmetyka zegara

Definicja

$$a \equiv b(mod n) \Leftrightarrow n|a - b$$

Warunek $a \equiv b(mod n)$ jest spełniony wtedy i tylko wtedy, gdy liczby a i b dają równe reszty z dzielenia przez n.

Kongruencje czyli arytmetyka zegara

Definicja

$$a \equiv b(mod n) \Leftrightarrow n|a - b$$

Warunek $a \equiv b(mod n)$ jest spełniony wtedy i tylko wtedy, gdy liczby a i b dają równe reszty z dzielenia przez n.

$$a \equiv_n b$$

Kongruencje czyli arytmetyka zegara

Definicja

$$a \equiv b(modn) \Leftrightarrow n|a - b$$

Warunek $a \equiv b(modn)$ jest spełniony wtedy i tylko wtedy, gdy liczby a i b dają równe reszty z dzielenia przez n.

$$a \equiv_n b$$

Każda liczba przystaje mod n do dokładnie jednej liczby ze zbioru

$$Z_n = \{0, 1, \ldots, n-1\}.$$

Twierdzenie

Niech $a \equiv_n b$ oraz $c \equiv_n d$. Wtedy

- $a + c \equiv_n b + d$
- $ac \equiv_n bd$.
- $a^k \equiv_n b^k$

Przykład

$$8 \equiv_{11} 30, \quad 47 \equiv_{11} 3$$

Przykład

$$8 \equiv_{11} 30, \quad 47 \equiv_{11} 3$$

$$8 + 47 \equiv_{11} 30 + 3$$

Przykład

$$8 \equiv_{11} 30, \quad 47 \equiv_{11} 3$$

$$8 + 47 \equiv_{11} 30 + 3$$

$$8 \cdot 47 = 337 \equiv_{11} 30 \cdot 3 = 90$$

Przykład

$$8 \equiv_{11} 30, \quad 47 \equiv_{11} 3$$

$$8 + 47 \equiv_{11} 30 + 3$$

$$8 \cdot 47 = 337 \equiv_{11} 30 \cdot 3 = 90$$

$$6 \equiv_3 3$$

Przykład

$$8 \equiv_{11} 30, \quad 47 \equiv_{11} 3$$

$$8 + 47 \equiv_{11} 30 + 3$$

$$8 \cdot 47 = 337 \equiv_{11} 30 \cdot 3 = 90$$

$$6 \equiv_3 3 \qquad 2 \equiv_3 1?$$

Przykład

$$8 \equiv_{11} 30, \quad 47 \equiv_{11} 3$$

$$8 + 47 \equiv_{11} 30 + 3$$

$$8 \cdot 47 = 337 \equiv_{11} 30 \cdot 3 = 90$$

$$6 \equiv_3 3 \qquad 2 \equiv_3 1?$$

NIE!

$$55 \equiv_7 20$$

$$55 \equiv_7 20 \qquad 11 \equiv_7 4$$

$$55 \equiv_7 20 \qquad 11 \equiv_7 4$$

$$5 \cdot 3 \equiv_7 1$$

$$55 \equiv_7 20 \qquad 11 \equiv_7 4$$

$$5 \cdot 3 \equiv_7 1$$

$$3 \cdot 55 \equiv_7 3 \cdot 20$$

$$55 \equiv_7 20 \qquad 11 \equiv_7 4$$

$$5 \cdot 3 \equiv_7 1$$

$$3 \cdot 55 \equiv_7 3 \cdot 20$$

$$3 \cdot 55 = 3 \cdot 5 \cdot 11 \equiv_7 11,$$

$$55 \equiv_7 20 \qquad 11 \equiv_7 4$$

$$5 \cdot 3 \equiv_7 1$$

$$3 \cdot 55 \equiv_7 3 \cdot 20$$

$$3 \cdot 55 = 3 \cdot 5 \cdot 11 \equiv_7 11, \quad 3 \cdot 20 = 3 \cdot 5 \cdot 4 \equiv_7 4.$$

$$55 \equiv_7 20 \qquad 11 \equiv_7 4$$

$$5 \cdot 3 \equiv_7 1$$

$$3 \cdot 55 \equiv_7 3 \cdot 20$$

$$3 \cdot 55 = 3 \cdot 5 \cdot 11 \equiv_7 11, \quad 3 \cdot 20 = 3 \cdot 5 \cdot 4 \equiv_7 4.$$

$$11 \equiv_7 4$$

Definicja

Element $k \in Z_n$ nazywamy odwracalnym modulo n, jeśli istnieje element $m \in Z_n$ taki, że

$$mk \equiv_n 1.$$

Definicja

Element $k \in Z_n$ nazywamy odwracalnym modulo n, jeśli istnieje element $m \in Z_n$ taki, że

$$mk \equiv_n 1.$$

Przykład

5 jest odwracalne mod 7,

Definicja

Element $k \in Z_n$ nazywamy odwracalnym modulo n, jeśli istnieje element $m \in Z_n$ taki, że

$$mk \equiv_n 1.$$

Przykład

5 jest odwracalne mod 7,

3 nie jest odwracalne mod 6.

Definicja

Element $k \in Z_n$ nazywamy odwracalnym modulo n, jeśli istnieje element $m \in Z_n$ taki, że

$$mk \equiv_n 1.$$

Przykład

5 jest odwracalne mod 7,
3 nie jest odwracalne mod 6.

Twierdzenie

Element $k \in Z_n$ jest odwracalny modulo n wtedy i tylko wtedy gdy $NWD(n, k) = 1$.

Nikogo nie obchodzi los podzielnych

Zadanie

Jaka jest cyfra jedności liczby 23^{200}?

Nikogo nie obchodzi los podzielnych

Zadanie

Jaka jest cyfra jedności liczby 23^{200}?

$$23 \equiv_{10} 3$$

Nikogo nie obchodzi los podzielnych

Zadanie

Jaka jest cyfra jedności liczby 23^{200}?

$$23 \equiv_{10} 3$$

$$23^2 \equiv_{10} 3^2 = 9,$$

Nikogo nie obchodzi los podzielnych

Zadanie

Jaka jest cyfra jedności liczby 23^{200}?

$$23 \equiv_{10} 3$$

$$23^2 \equiv_{10} 3^2 = 9, \quad 9 \equiv_{10} -1$$

Nikogo nie obchodzi los podzielnych

Zadanie

Jaka jest cyfra jedności liczby 23^{200}?

$$23 \equiv_{10} 3$$

$$23^2 \equiv_{10} 3^2 = 9, \quad 9 \equiv_{10} -1$$

$$23^{200} \equiv_{10} (-1)^{100} = 1.$$

Zadanie

Jaka jest reszta z dzielenia liczby 3^{1000} przez 7?

$$3^1 \equiv_7 3,$$

Zadanie

Jaka jest reszta z dzielenia liczby 3^{1000} przez 7?

$$3^1 \equiv_7 3, \quad 3^2 \equiv_7 2,$$

Zadanie

Jaka jest reszta z dzielenia liczby 3^{1000} przez 7?

$$3^1 \equiv_7 3, \quad 3^2 \equiv_7 2, \quad 3^3 \equiv_7 6 \equiv_7 -1,$$

Zadanie

Jaka jest reszta z dzielenia liczby 3^{1000} przez 7?

$$3^1 \equiv_7 3, \quad 3^2 \equiv_7 2, \quad 3^3 \equiv_7 6 \equiv_7 -1, \quad 3^6 \equiv_7 1,$$

Zadanie

Jaka jest reszta z dzielenia liczby 3^{1000} przez 7?

$$3^1 \equiv_7 3, \quad 3^2 \equiv_7 2, \quad 3^3 \equiv_7 6 \equiv_7 -1, \quad 3^6 \equiv_7 1,$$

$$3^{1000} = 3^{166 \cdot 6 + 4} = (3^6)^{166} \cdot 3^4$$

Zadanie

Jaka jest reszta z dzielenia liczby 3^{1000} przez 7?

$$3^1 \equiv_7 3, \quad 3^2 \equiv_7 2, \quad 3^3 \equiv_7 6 \equiv_7 -1, \quad 3^6 \equiv_7 1,$$

$$3^{1000} = 3^{166\cdot 6+4} = (3^6)^{166}\cdot 3^4 \equiv_7 1^{166}\cdot 3^4 \equiv_7 -1\cdot 3 \equiv_7 4$$

Małe jest piękne: Małe Twierdzenie Fermata

Pierre Fermat
(1601-1665)

Twierdzenie

Niech p bedzie liczba pierwszą. Wtedy dla dowolnej liczby całkowitej a, $a^p \equiv_p a$.

Małe jest piękne: Małe Twierdzenie Fermata

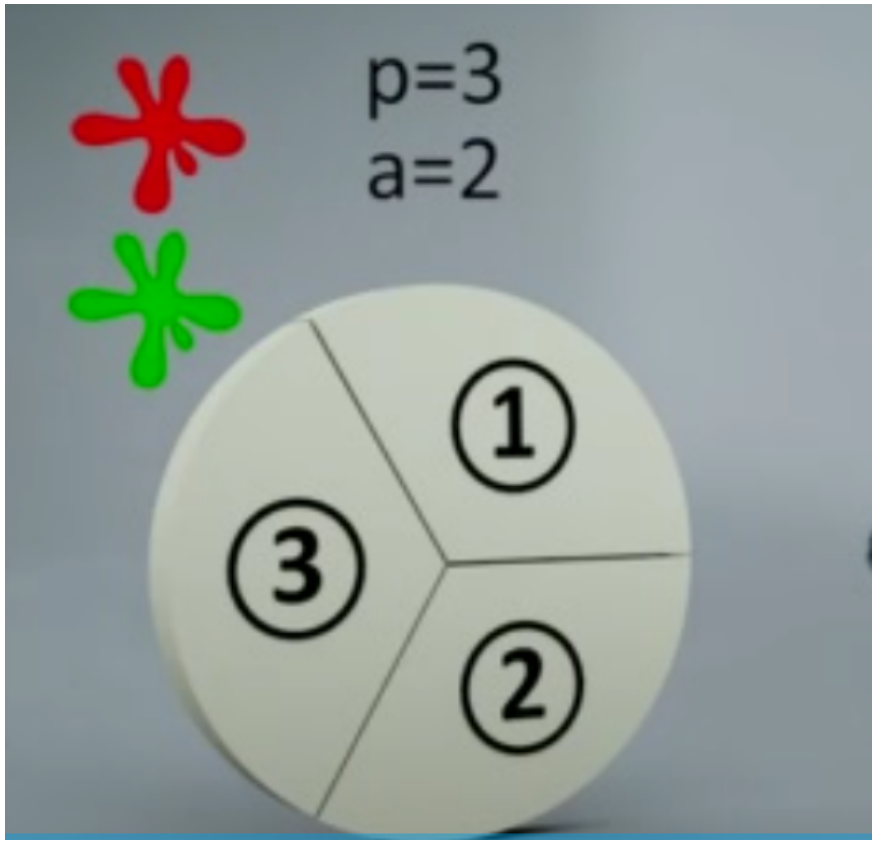
Pierre Fermat
(1601-1665)

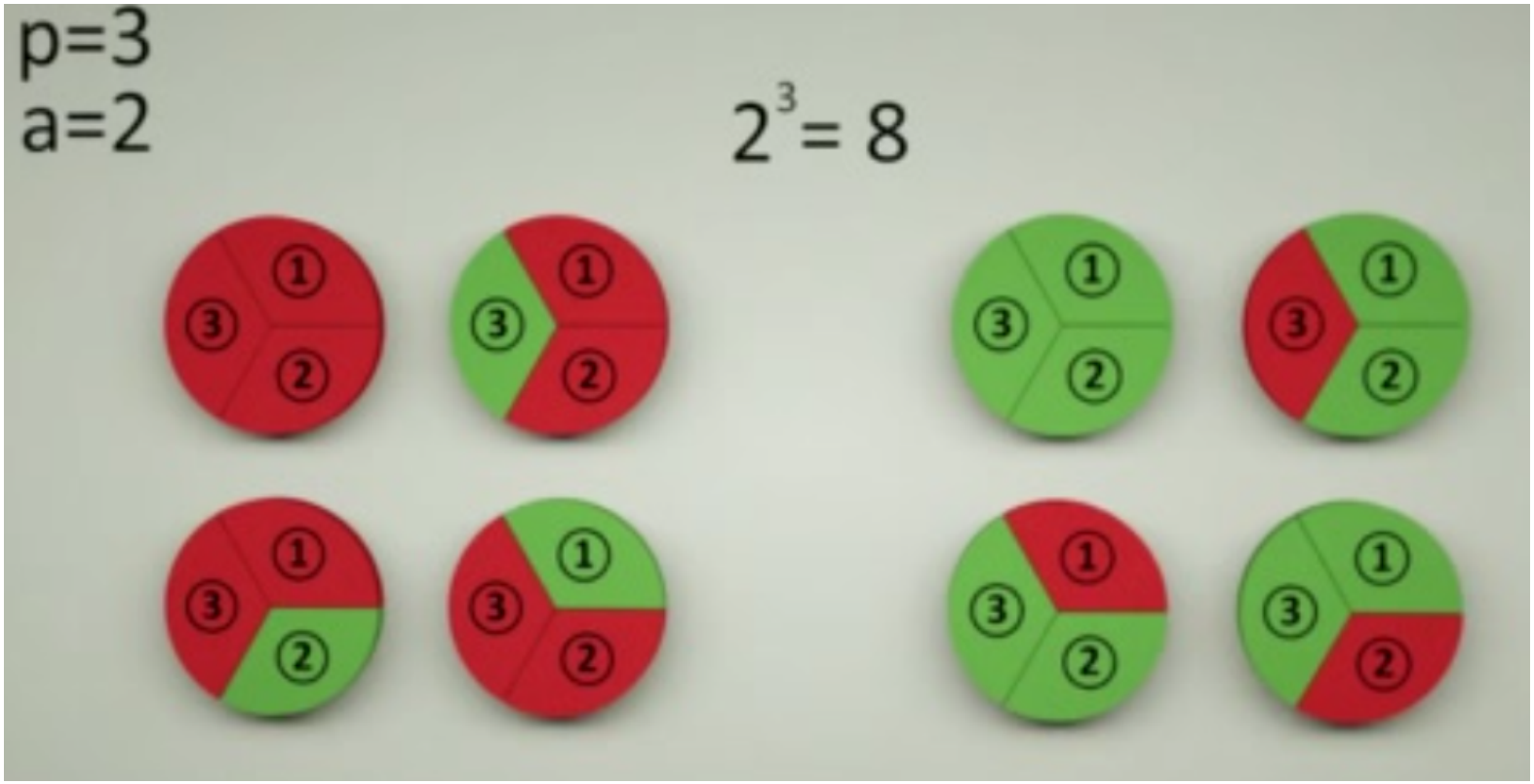
Twierdzenie

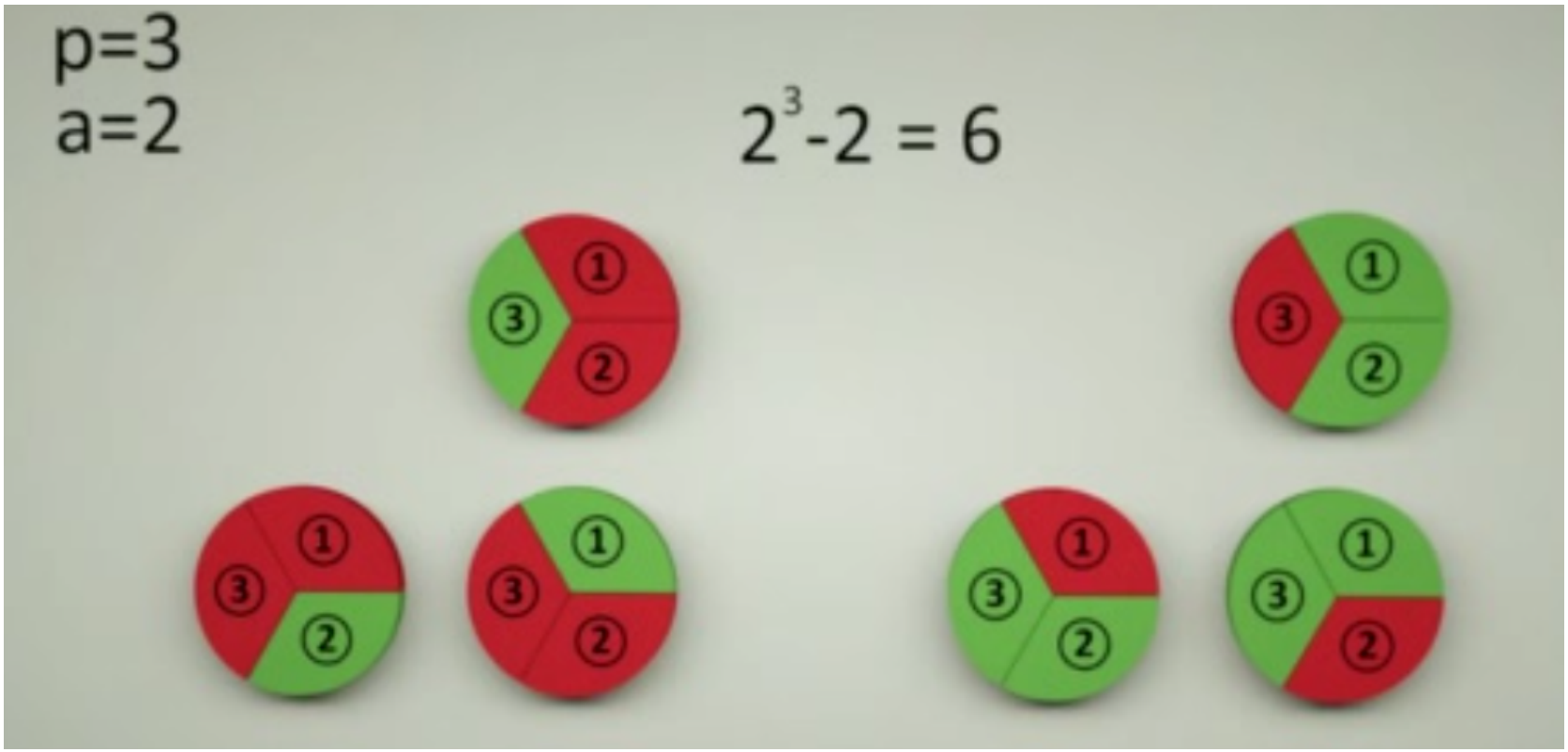
Niech p bedzie liczba pierwszą. Wtedy dla dowolnej liczby całkowitej a, $a^p \equiv_p a$.

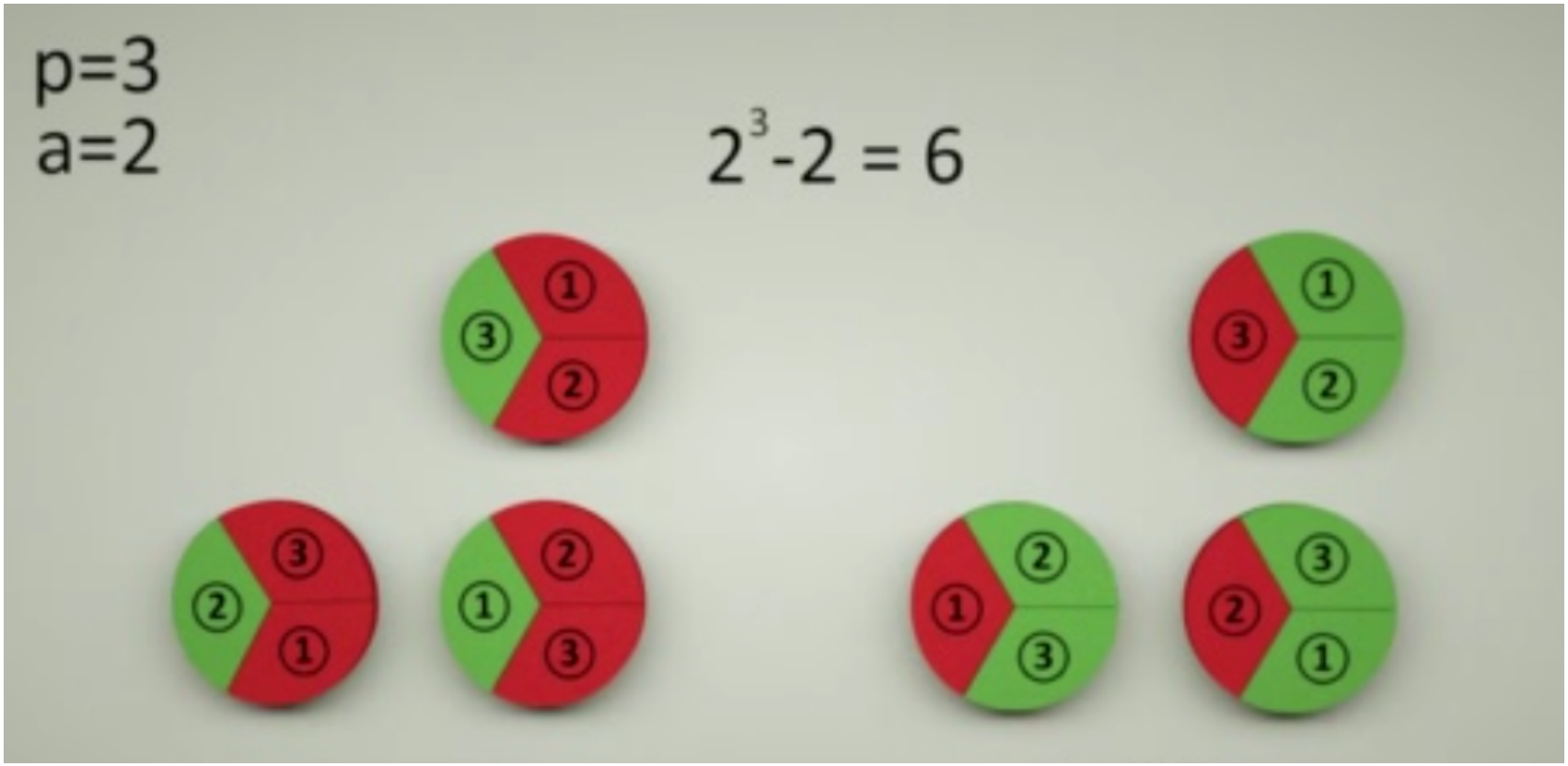
Jeśli $p \nmid a$, to

$$a^{p-1} \equiv 1(mod p).$$

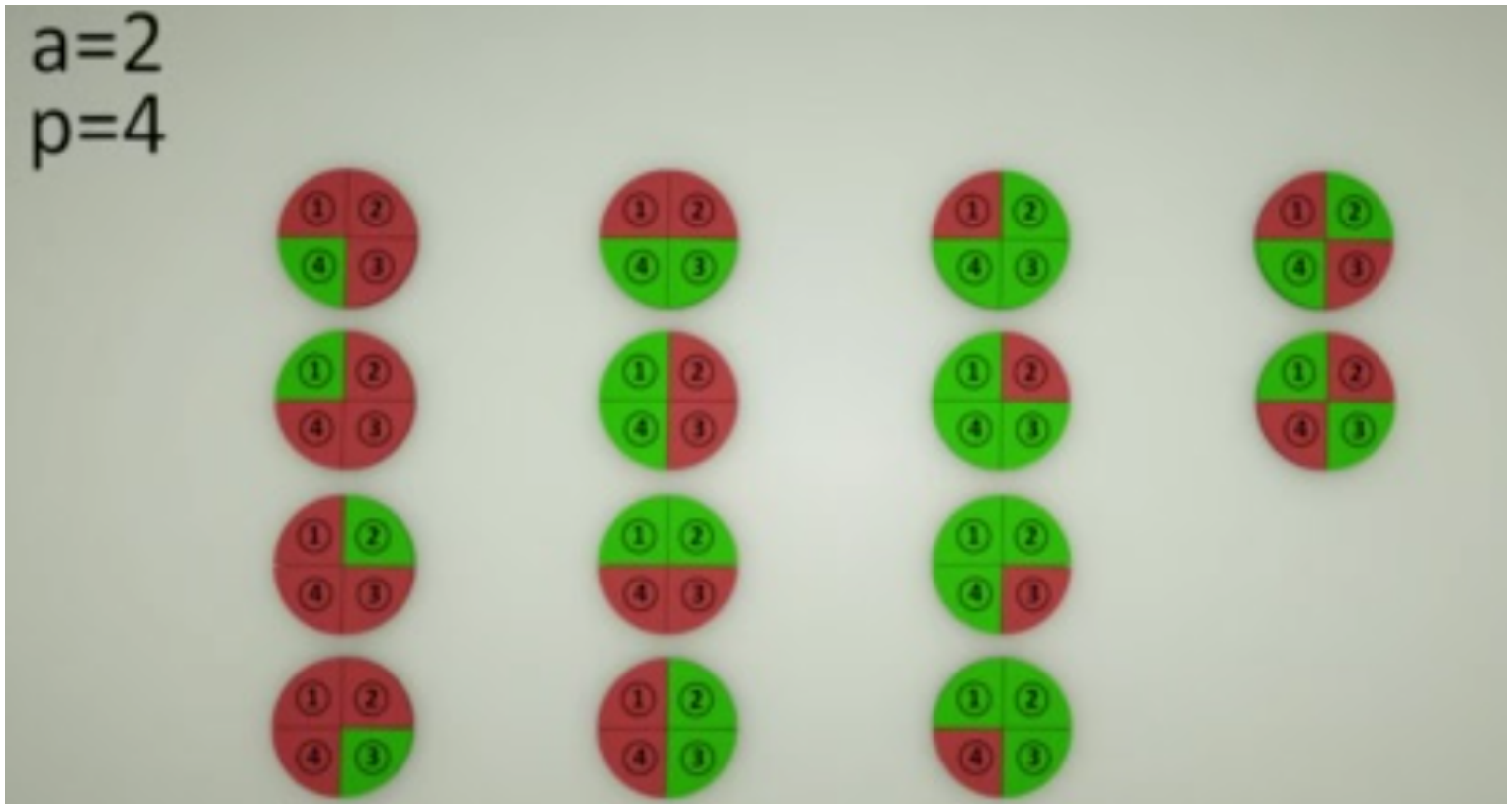

p=3
a=2
1
3
2

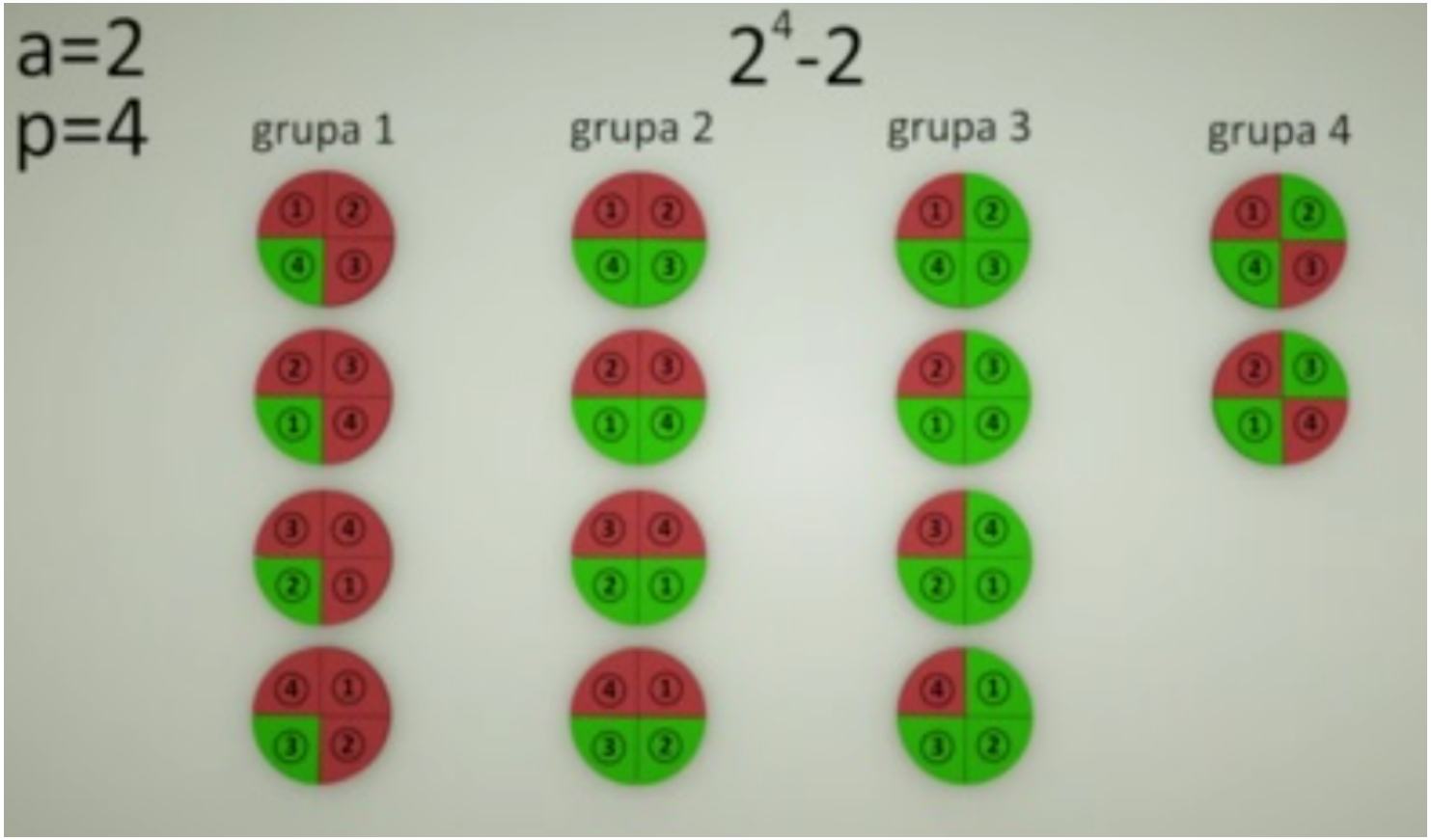

p=3
a=2
$2^3 = 8$
1
3
2


p=3
a=2
$2^3-2=6$

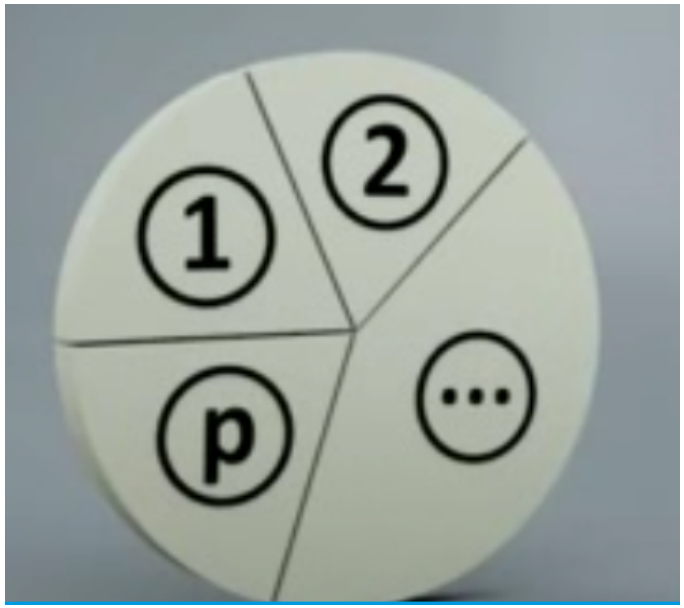


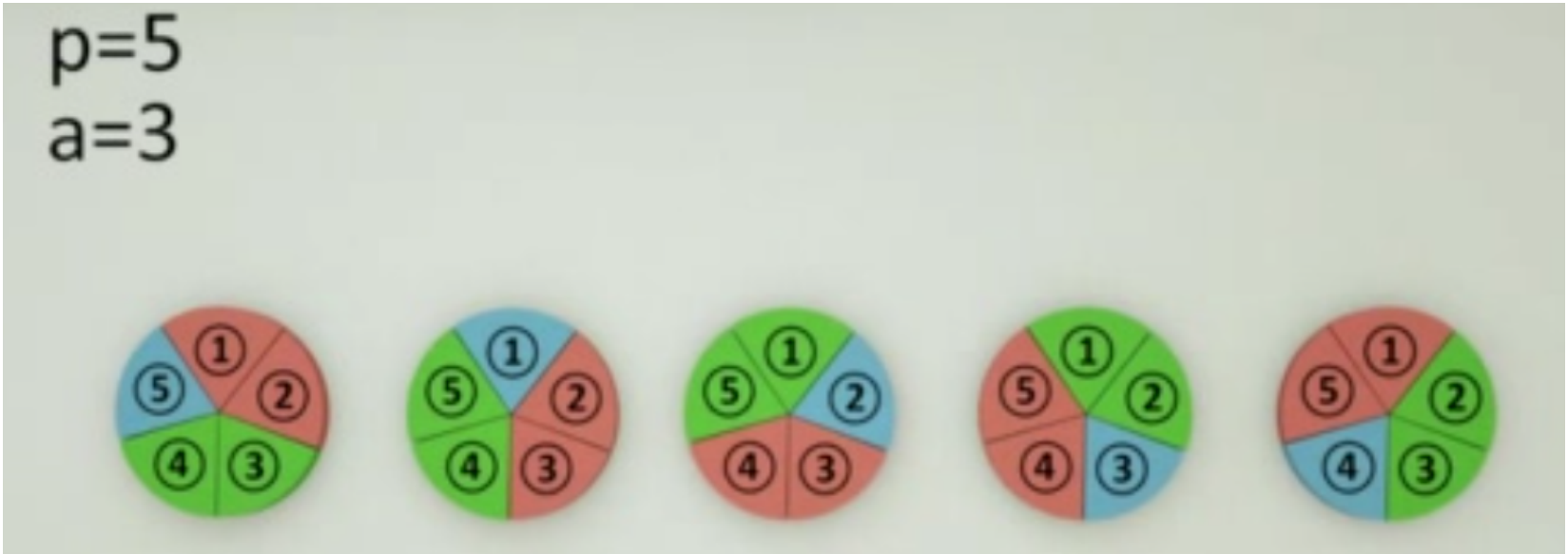
$$3|2^3-2$$


a=2
p=4



$$4 \nmid 2^4 - 2$$


1
2
p
...



$$p \mid a^p - a$$

Czy można twierdzenie Fermata odwrócić?

Czy można twierdzenie Fermata odwrócić?
Czy z faktu, że

$$p \mid a^p - a$$

wynika, że p jest liczbą pierwszą?

Czy można twierdzenie Fermata odwrócić?
Czy z faktu, że

$$p | a^p - a$$

wynika, że p jest liczbą pierwszą?

$$3^{90} = (3^4)^{22} \cdot 3^2 \equiv_{91} ((-10)^2)^{11} \cdot 9 \equiv_{91}$$

Czy można twierdzenie Fermata odwrócić?
Czy z faktu, że

$$p | a^p - a$$

wynika, że p jest liczbą pierwszą?

$$3^{90} = (3^4)^{22} \cdot 3^2 \equiv_{91} ((-10)^2)^{11} \cdot 9 \equiv_{91}$$

$$\equiv_{91} 9^{12} \equiv_{91} (-10)^6 \equiv_{91} 9^3 \equiv_{91} (-10) \cdot 9 \equiv_{91} 1$$

Czy można twierdzenie Fermata odwrócić?
Czy z faktu, że

$$p | a^p - a$$

wynika, że p jest liczbą pierwszą?

$$3^{90} = (3^4)^{22} \cdot 3^2 \equiv_{91} ((-10)^2)^{11} \cdot 9 \equiv_{91}$$

$$\equiv_{91} 9^{12} \equiv_{91} (-10)^6 \equiv_{91} 9^3 \equiv_{91} (-10) \cdot 9 \equiv_{91} 1$$

ale

$$91 = 7 \cdot 13$$

Czy można twierdzenie Fermata odwrócić?
Czy z faktu, że

$$p | a^p - a$$

wynika, że p jest liczbą pierwszą?

$$3^{90} = (3^4)^{22} \cdot 3^2 \equiv_{91} ((-10)^2)^{11} \cdot 9 \equiv_{91}$$

$$\equiv_{91} 9^{12} \equiv_{91} (-10)^6 \equiv_{91} 9^3 \equiv_{91} (-10) \cdot 9 \equiv_{91} 1$$

ale

$$91 = 7 \cdot 13$$

Liczba 91 jest **liczbą pseudopierwszą** przy podstawie 3.

Liczbowi oszuści

$$2^{90} \equiv_{91} 64 \neq 1$$

Liczbowi oszuści

$$2^{90} \equiv_{91} 64 \neq 1$$

Liczba 2 jest świadkiem złożoności liczby 91.

Liczbowi oszuści

$$2^{90} \equiv_{91} 64 \neq 1$$

Liczba 2 jest świadkiem złożoności liczby 91.
Najmniejszą liczbą pseudopierwszą przy podstawie 2 jest 341.

$$2^{340} \equiv_{341} 1,$$

Liczbowi oszuści

$$2^{90} \equiv_{91} 64 \neq 1$$

Liczba 2 jest świadkiem złożoności liczby 91.
Najmniejszą liczbą pseudopierwszą przy podstawie 2 jest 341.

$$2^{340} \equiv_{341} 1,$$

$$341 = 11 \cdot 31.$$

Czy dla każdej liczby złożonej istnieje "świadek złożoności"?

Czy dla każdej liczby złożonej istnieje "świadek złożoności"?
Liczba

$$561 = 3 \cdot 11 \cdot 17$$

jest liczbą pseudopierwszą przy dowolnej podstawie,

Czy dla każdej liczby złożonej istnieje "świadek złożoności"?
Liczba

$$561 = 3 \cdot 11 \cdot 17$$

jest liczbą pseudopierwszą przy dowolnej podstawie,

$$NWD(a, 561) = 1 \Longrightarrow a^{560} \equiv_{561} 1$$

Czy dla każdej liczby złożonej istnieje "świadek złożoności"?
Liczba

$$561 = 3 \cdot 11 \cdot 17$$

jest liczbą pseudopierwszą przy dowolnej podstawie,

$$NWD(a, 561) = 1 \Longrightarrow a^{560} \equiv_{561} 1$$

Liczby złożone spełniające ten warunek nazywamy liczbami Carmichaela.

Czy dla każdej liczby złożonej istnieje "świadek złożoności"?
Liczba

$$561 = 3 \cdot 11 \cdot 17$$

jest liczbą pseudopierwszą przy dowolnej podstawie,

$$NWD(a, 561) = 1 \Longrightarrow a^{560} \equiv_{561} 1$$

Liczby złożone spełniające ten warunek nazywamy liczbami Carmichaela.

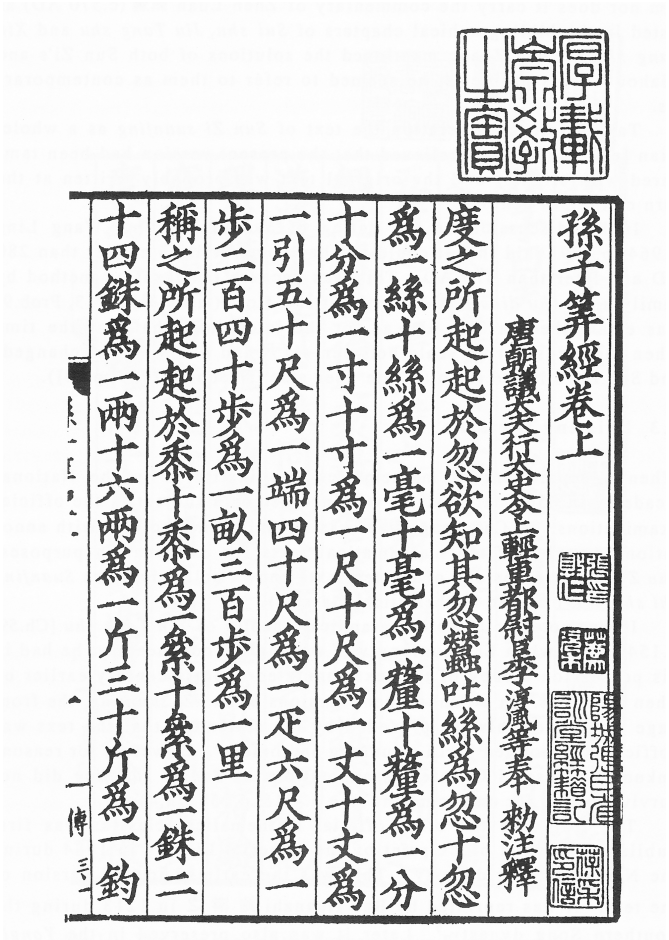
Daniel Carmichael (1879-1967)

Daniel Carmichael (1879-1967)

Liczb Carmichaela jest nieskończenie wiele.

Chińskie początki

Około 100 roku naszej ery chiński matematyk Sun Zi rozwiązał problem znajdowania liczb całkowitych, które przy dzieleniu przez $3, 5, 7$ dają reszty odpowiednio $2, 3, 2$.


孫子算經卷上

唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋

度之所起起於忽欲知其忽蠛蠓吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一氂十氂爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里

稱之所起起於黍十黍爲一絫十絫爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

$$x \equiv_3 2, \quad x \equiv_5 3, \quad x \equiv_7 2$$

$$x \equiv_3 2, \quad x \equiv_5 3, \quad x \equiv_7 2$$

$3k+2$:

$$x \equiv_3 2, \quad x \equiv_5 3, \quad x \equiv_7 2$$

$$3k+2: \quad 5, \quad 8, \quad 11, \quad 14, \quad 17, \quad 20, \quad 23, \quad 26, \quad 29, \quad \ldots$$

$$x \equiv_3 2, \quad x \equiv_5 3, \quad x \equiv_7 2$$

$3k+2:$ $5,$ $8,$ $11,$ $14,$ $17,$ $20,$ $23,$ $26,$ $29,$ $\ldots$

$5k+3:$

$$x \equiv_3 2, \quad x \equiv_5 3, \quad x \equiv_7 2$$

$3k+2:$ 5, 8, 11, 14, 17, 20, 23, 26, 29, ...

$5k+3:$ 8, 13, 18, 23, 28, 33, 38, 43, 48 ...

$$x \equiv_3 2, \quad x \equiv_5 3, \quad x \equiv_7 2$$

$3k+2:$ 5, 8, 11, 14, 17, 20, 23, 26, 29, ...

$5k+3:$ 8, 13, 18, 23, 28, 33, 38, 43, 48 ...

$3k+2:$ 5, 8, 11, 14, 17, 20, 23, 26, 29, ...

$5k+3:$ 8, 13 18, 23, 28, 33, 38, 43, 48, ...

$3k+2:\quad 5,\quad 8,\quad 11,\quad 14,\quad 17,\quad 20,\quad 23,\quad 26,\quad 29,\ldots$

$5k+3:\quad 8,\quad 13\quad 18,\quad 23,\quad 28,\quad 33,\quad 38,\quad 43,\quad 48,\quad \ldots$

$7k+2:\quad 9,\quad 16,\quad 23,\quad 30,\quad 37,\quad 44,\quad 51,\quad 58\quad \ldots$

$3k+2:\quad 5,\quad 8,\quad 11,\quad 14,\quad 17,\quad 20,\quad 23,\quad 26,\quad 29,\ldots$

$5k+3:\quad 8,\quad 13,\quad 18,\quad 23,\quad 28,\quad 33,\quad 38,\quad 43,\quad 48,\quad \ldots$

$7k+2:\quad 9,\quad 16,\quad 23,\quad 30,\quad 37,\quad 44,\quad 51\quad 58\quad \ldots$

$3k+2:\quad 5,\quad 8,\quad 11,\quad 14,\quad 17,\quad 20,\quad 23,\quad 26,\quad 29,\ldots$

$5k+3:\quad 8,\quad 13,\quad 18,\quad 23,\quad 28,\quad 33,\quad 38,\quad 43,\quad 48,\quad \ldots$

$7k+2:\quad 9,\quad 16,\quad 23,\quad 30,\quad 37,\quad 44,\quad 51\quad 58\quad \ldots$

$$x = 23 + 7 \cdot 5 \cdot 3 \cdot k,$$

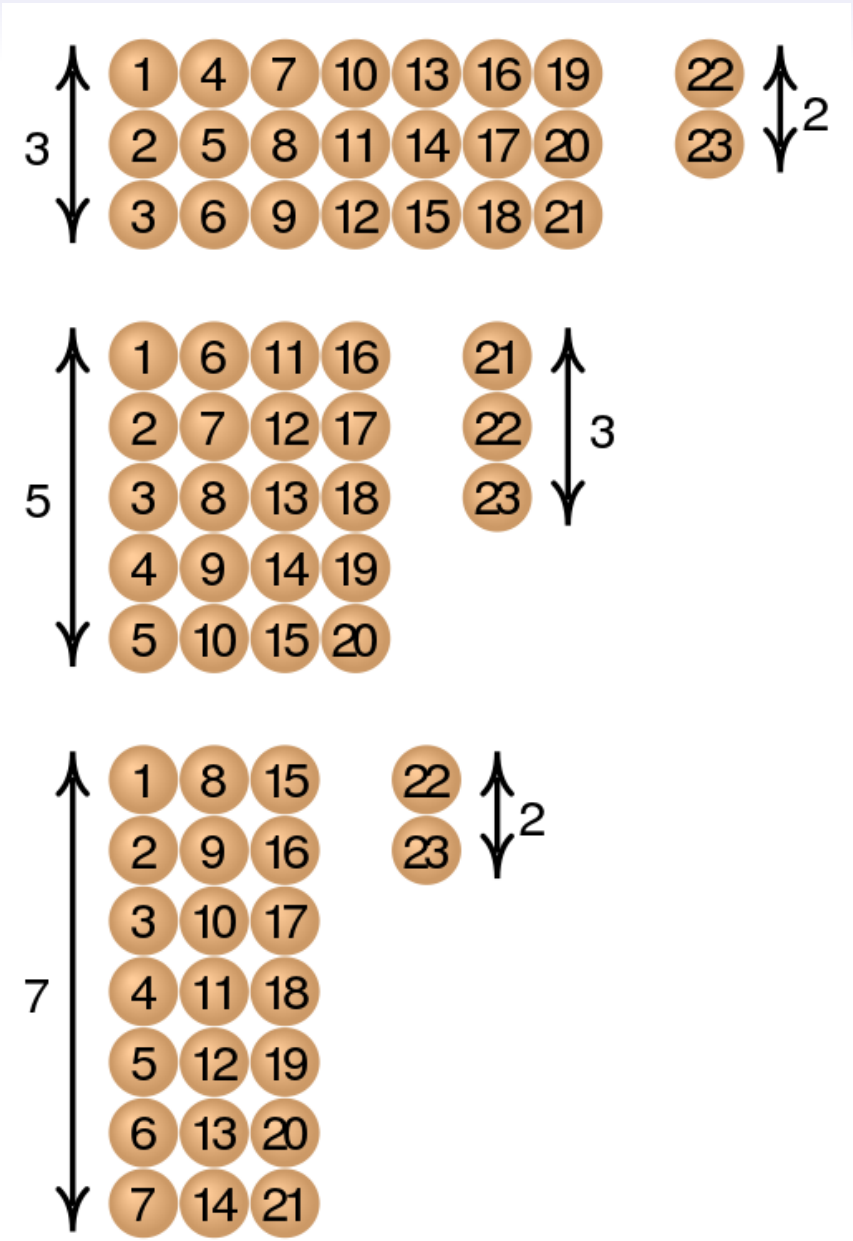
$3k+2:\quad 5,\quad 8,\quad 11,\quad 14,\quad 17,\quad 20,\quad 23,\quad 26,\quad 29,\ldots$

$5k+3:\quad 8,\quad 13,\quad 18,\quad 23,\quad 28,\quad 33,\quad 38,\quad 43,\quad 48,\quad \ldots$

$7k+2:\quad 9,\quad 16,\quad 23,\quad 30,\quad 37,\quad 44,\quad 51\quad 58\quad \ldots$

$$x = 23 + 7 \cdot 5 \cdot 3 \cdot k,$$

$$x \equiv_{105} 23.$$


1 4 7 10 13 16 19
2 5 8 11 14 17 20
3 6 9 12 15 18 21
3
22
23
2
1 6 11 16
2 7 12 17
3 8 13 18
4 9 14 19
5 10 15 20
5
21
22
23
3
1 8 15
2 9 16
3 10 17
4 11 18
5 12 19
6 13 20
7 14 21
7
22
23
2

Twierdzenie

Dla parami względnie pierwszych modułów $m_1, m_2, \ldots, m_r$, oraz liczb całkowitych $a_1, a_2, \ldots a_r$ układ kongruencji

$$x \equiv_{m_1} a_1$$

$$x \equiv_{m_2} a_2$$

$$\vdots$$

$$x \equiv_{m_r} a_r$$

ma dokładnie jedno rozwiązanie modulo $M = m_1 \cdot \ldots \cdot m_r$.

Definicja

Liczbę całkowitą a względnie pierwszą z liczbą n nazywamy resztą kwadratową modulo n, wtedy i tylko wtedy, gdy istnieje liczba całkowita x, taka że

$$x^2 \equiv_n a.$$

Przykład

Resztami kwadratowymi mod 11 są:

Przykład

Resztami kwadratowymi mod 11 są:

$$1, 4, 9, 5, 3.$$

Przykład

Resztami kwadratowymi mod 11 są:

$$1, 4, 9, 5, 3.$$

Reszty kwadratowe mod 15 to

Przykład

Resztami kwadratowymi mod 11 są:

$$1, 4, 9, 5, 3.$$

Reszty kwadratowe mod 15 to

$$1, 4.$$

Przykład

Resztami kwadratowymi mod 11 są:

$$1, 4, 9, 5, 3.$$

Reszty kwadratowe mod 15 to

$$1, 4.$$

Reszty kwadratowe mod liczby pierwsze

Twierdzenie

Jest dokładnie $\frac{p-1}{2}$ reszt kwadratowych mod liczba pierwsza $p > 2$.

Reszty kwadratowe mod liczby pierwsze

Twierdzenie

Jest dokładnie $\frac{p-1}{2}$ reszt kwadratowych mod liczba pierwsza $p > 2$.

Twierdzenie

Niech p będzie liczbą pierwszą $a \neq 0$. Kongruencja $x^2 \equiv_p a$ ma dwa rozwiązania, jeśli a jest resztą kwadratową mod p.

Przykład

$$2^2 \equiv_{15} 4,$$

Przykład

$$2^2 \equiv_{15} 4,$$

$$7^2 \equiv_{15} 4,$$

Przykład

$$2^2 \equiv_{15} 4,$$

$$7^2 \equiv_{15} 4,$$

$$8^2 \equiv_{15} 4,$$

Przykład

$$2^2 \equiv_{15} 4,$$

$$7^2 \equiv_{15} 4,$$

$$8^2 \equiv_{15} 4,$$

$$13^2 \equiv_{15} 4$$

O nieprawdopodobne liczby pierwsze,
niech łowcy formuł krążą
w oparach abstrakcji i tracą
resztki poloru:
Wy bądźcie nonkonformistyczne, uprzykrzone,
nie dajcie się złowić w sieci
układów, ciągów, wyjaśnień
i wzorów.

(Helen Spalding)

Bibliografia


Gardner Martin, Ostatnie Rozrywki, rozdział 12 Prószyński i s-ka, Warszawa


Animacje i wykresy wygenerowane za pomocą programu Wolfram mathematica 7.


Portrety matematyków, obrazki: wikipedia.

KONIEC

Dziękuję za uwagę