Toán rời rạc

SỐ NGUYÊN

Tạ Thị Nguyệt Nga 2020

4. Số nguyên

1. SỐ NGUYÊN
2. THUẬT TOÁN EUCLIDE
3. SỐ NGUYÊN TỐ
4. ĐỒNG DƯ

ƯỚC

Định nghĩa 1.1 Cho số nguyên n. Ta định nghĩa số nguyên *d là ước của n* hay *d chia hết n* nếu tồn tại một số nguyên m sao cho $n = dm$.

Kí hiệu $d \mid n$ khi d là ước của n. Và $d \nmid n$ khi d không là ước của n.

Ví dụ. 1. Số 3 là ước của 12 vì $12 = 3.4$.

2. Số 3 không là ước của 8, vì không tồn tại số nguyên nào để nhân 3 bằng 8.

3. Một số nguyên luôn có sẵn hai ước là 1 và chính nó.

4. Cho N= 11. 17. 19. Chứng minh rằng 17 là ước của N.

5. Tìm số tự nhiên có đúng 3 ước dương.

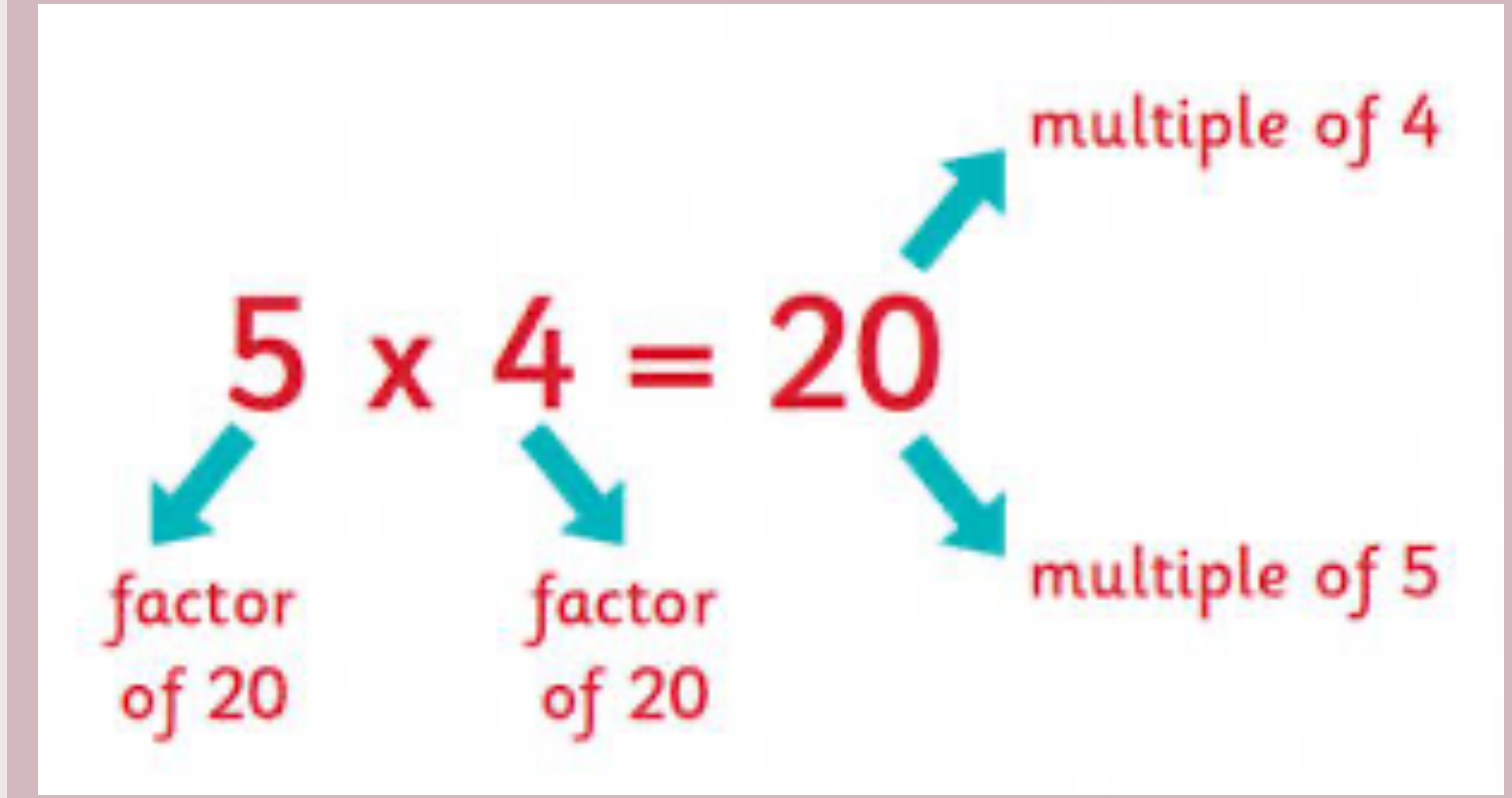
ƯỚC

Tính chất: $a \neq 0$ và b, c là các số nguyên. Ta có

- $a \mid b$ và $a \mid c$ thì $a \mid (b + c)$
- $a \mid b$ thì $a \mid bc$
- $a \mid b$ và $b \mid c$ thì $a \mid c$
- $a \mid b$ và $b \mid a$ thì $a = b$ hoặc $a = -b$
- $ab \mid c$ thì $a \mid c$ và $b \mid c$

Bài tập: Cho n và m là nguyên dương sao cho $n \leq m$ và $n \nmid m$. Nếu d là ước của n thì d là ước của m khi và chỉ khi d là ước của $(m \bmod n)$.

Từ đó suy ra $gcd(m, n) = gcd(n, m \bmod n)$



Dạng biểu diễn số nguyên

Định lý. Cho b là số nguyên lớn hơn 1. Khi đó mọi số nguyên dương n đều được biểu diễn duy nhất dưới dạng

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots a_1 b^1 + a_0$$

trong đó k là số nguyên không âm và a_i là số nguyên thỏa $0 \leq a_i < b$.

Dạng biểu diễn này được gọi là dạng biểu diễn theo cơ số b của n. và được ký hiệu $n = (a_k, a_{k-1}, \ldots a_0)_b$.

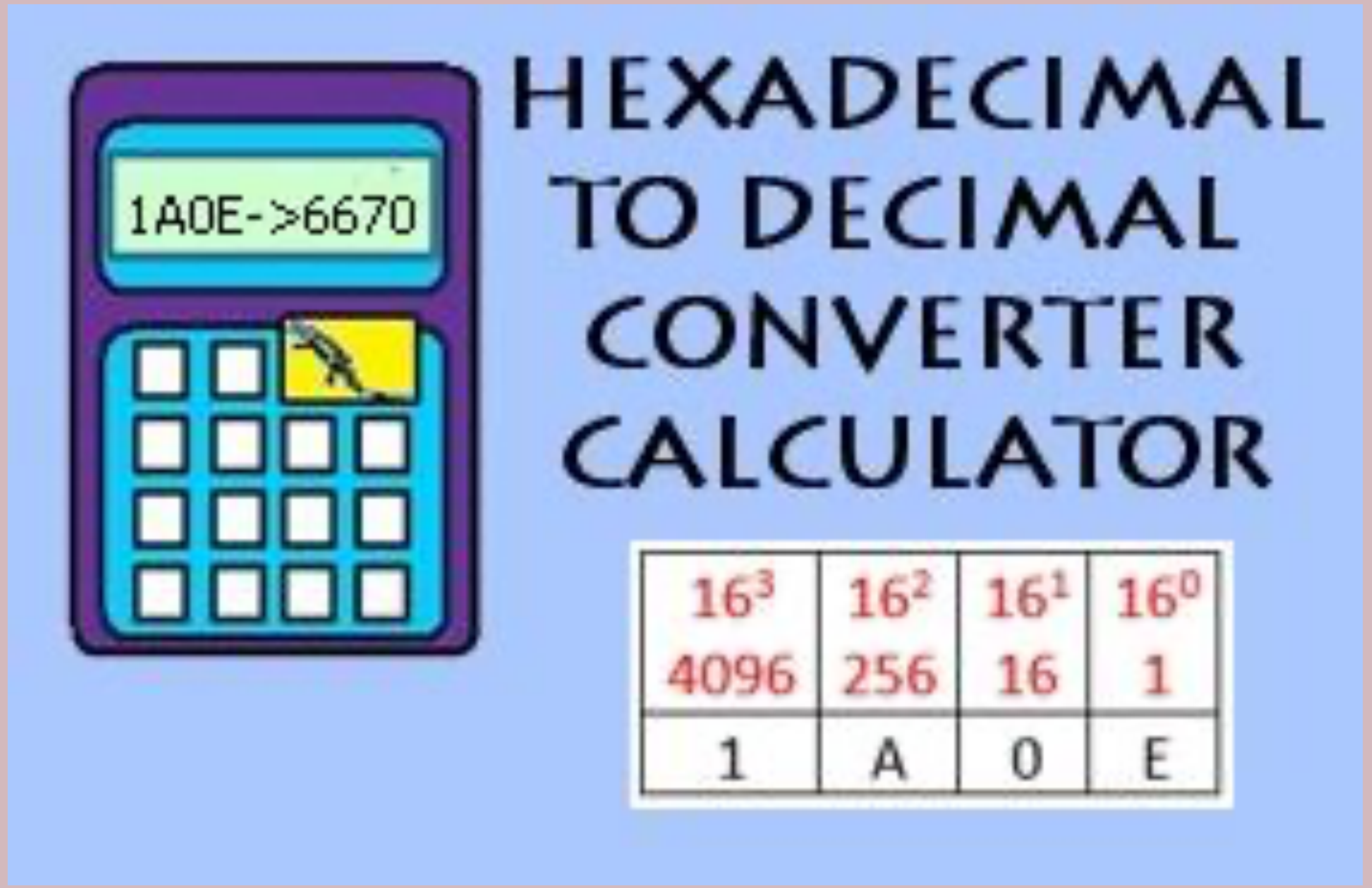
Ta có dạng nhị phân b = 2, bát phân b = 8, thập phân b = 10, thập lục phân b = 16.

Ví dụ.

- Tìm số nguyên có dạng biểu diễn nhị phân là $(1011111)_2$
- $(456)_8$
- $(123AF)_{16}$

Trong hệ thập lục thì A=10, B=11, C=12, D=13, E=14, F=15.

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots a_1 b^1 + a_0$$



TÌM DẠNG BIỂU DIỄN CƠ SỞ *B* CỦA *N*

$n = q_0 b + a_0$ Chia n cho b dư a_0

$n = (q_1 b + a_1)b + a_0$ Chia q_0 cho b dư a_1

....

Chia đến khi thương bằng 0 thì thôi
$q_k = 0.b + a_k$.

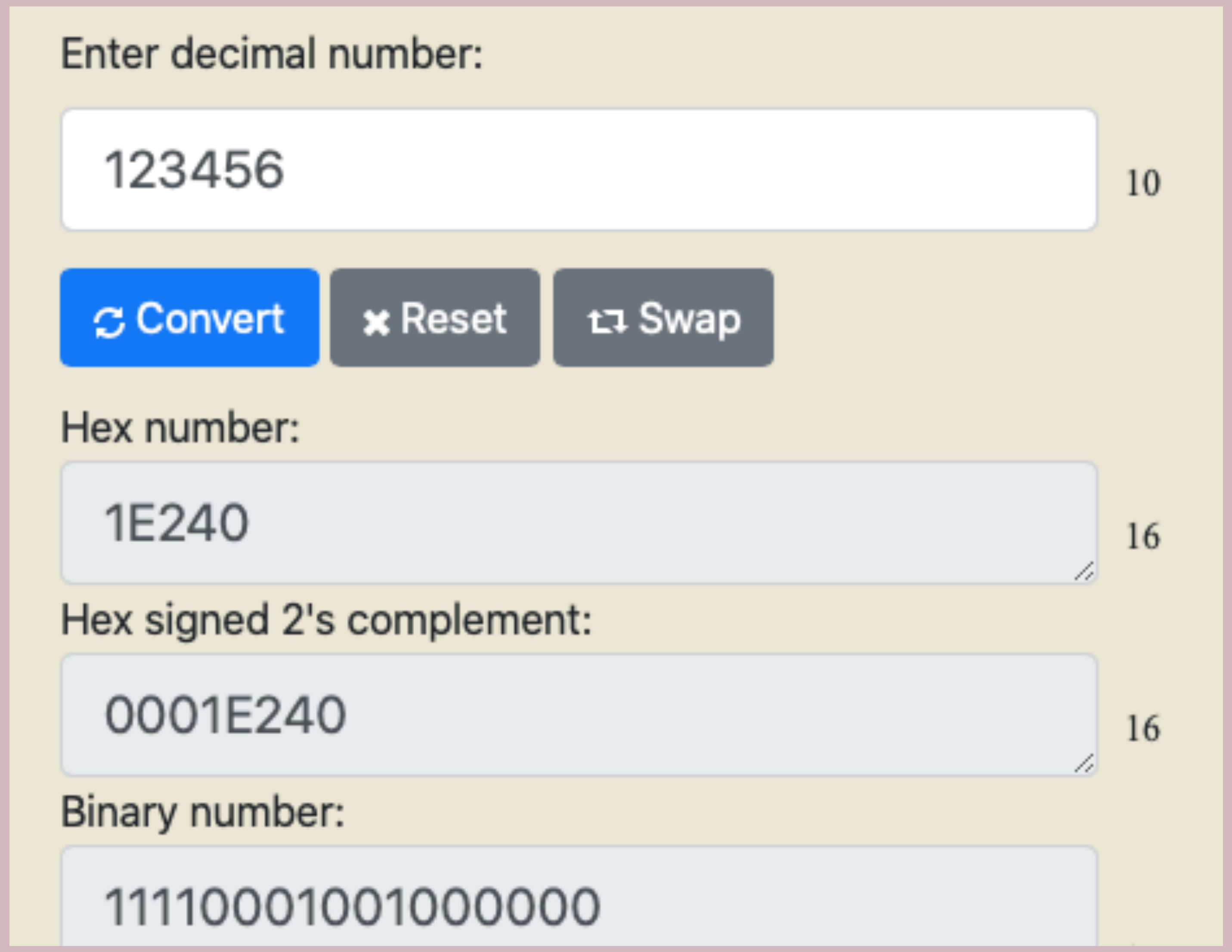
Khi đó $n = (a_k, a_{k-1} \ldots a_0)_b$

Ví dụ.

Tìm dạng biểu diễn nhị phân của 123

Tìm dạng biểu diễn bát phân của 123456

Tìm dạng biểu diễn thập lục phân của 123456



Chia lấy dư

Định nghĩa

Định lý. Cho $d \geq 1$ và n là hai số nguyên. Khi đó tồn tại duy nhất cặp số nguyên (r, q) sao cho $n = qd + r$ với $0 \leq r < d$.

q: thương. r: số dư

- **Ví dụ.**

n=89 d=14 thì

89=14.6+5, q=6 r=5?

n	d	q	r	Chia
89	14	6	5	89=14.6+5
507	202	2	103	507=202.2+103
-507	202	-3	99	-507=202.(-3)+99

Chia lấy dư

Tồn tại. (quy nạp mạnh) Cố định d, chứng minh quy nạp theo n

- P(n): Tồn tại q và r sao cho $n = dq + r$, với $0 \leq r < d$.
- Case 1: $n \geq 0$.
  - $0 \leq n < d$. Ta có q=0 và r=n.
  - Giả sử P(n′) đúng với mọi $0 \leq n' < n$, đặc biệt với $n' = n - d$, tồn tại q' và $0 \leq r' < d$ sao cho $n' = n - d = q'd + r'$. Hay $n = (q' + 1)d + r'$. bộ (q, r) chính là $(q' + 1, r')$. P(n) đúng với n.
- Case 2. $n \leq 0$. Theo case 1 thì $-n = q'd + r'$ với $0 \leq r' < d$
  - TH1. $r' = 0$. $n = -q'd + 0$. Bộ (q, r) là $(-q', 0)$
  - TH2, $r' \neq 0$ $n = -q'd - r' = -q'd - d + d - r' = (-q' - 1)d + (d - r')$

  Bộ số $(-q' - 1, d - r')$ chính là bộ số cần tìm

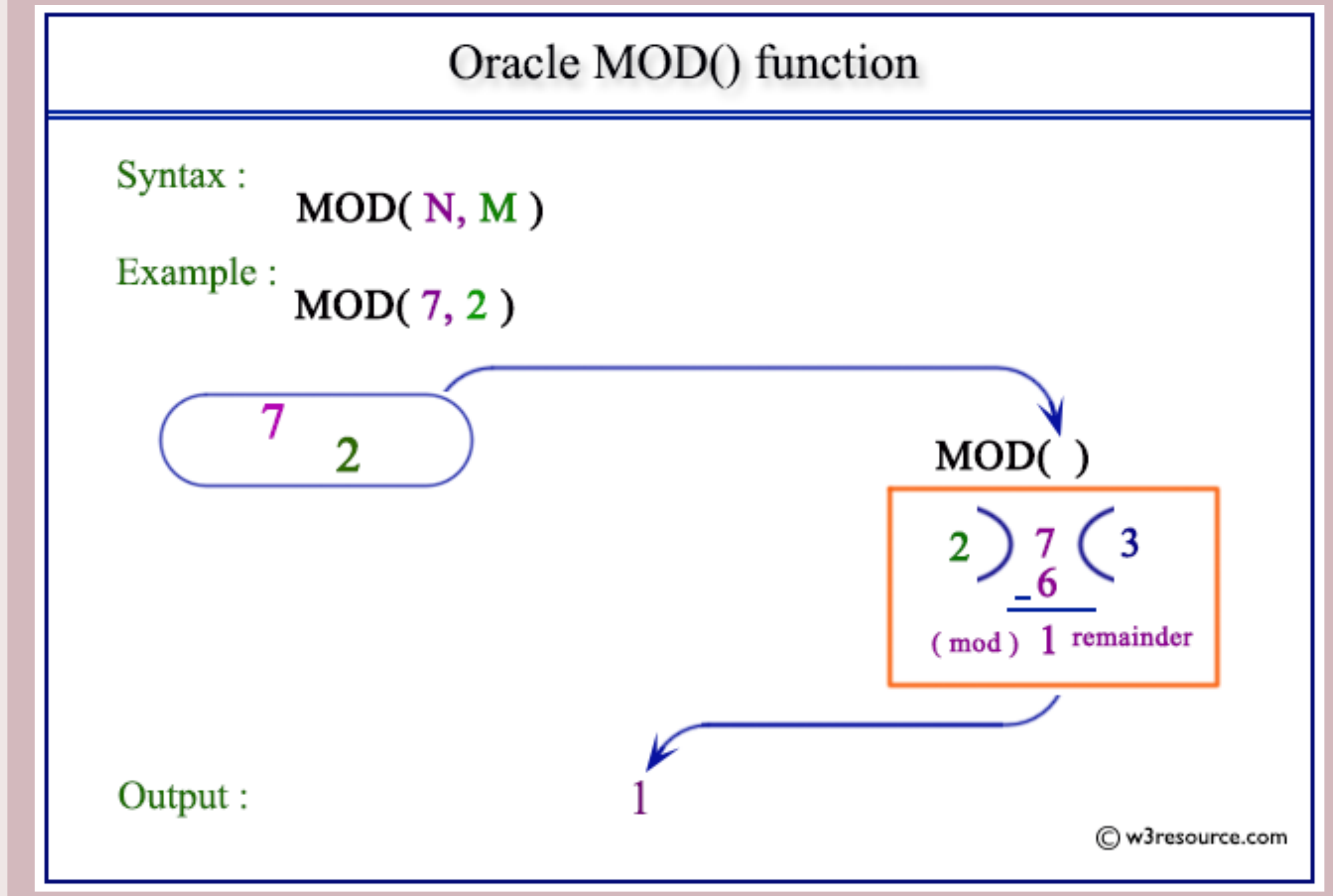
Duy nhất. Giả sử có hai bộ số (q_1, r_1) và (q_2, r_2) với $0 \leq r_1, r_2 < d$ sao cho: $n = q_1d + r_1$ $n = q_2d + r_2$

Khi đó ta có $d(q_1 - q_2) = r_2 - r_1$

Mod và div

- Pascal: *n div d —> q, và n mod d—>r.*
- C, C++, *Java: n/d—>q và n%d—>r.*
- *Vậy 10/3= 3 hay 10/3=3.333333?*
- *Thực hiện phép chia ở đâu?*

"you do not pay for what you do not use"



Ước chung lớn nhất và bội chung nhỏ nhất

Định nghĩa: d>0 gọi là ước chung lớn nhất của hai số a, b nếu d là số nguyên lớn nhất sao cho d | a và d | b. Kí hiệu *UCLN(a,b)* hoặc *GCD(a,b)* greatest common divisor hoặc ().

Định nghĩa: m>0 gọi là bội chung nhỏ nhất của hai số a, b nếu m là số nguyên nhỏ nhất sao cho a | m và b | m. Kí hiệu *BCNN(a,b)* hoặc *LCM (a,b)* least common multiple hoặc [].

Ví dụ gcd(15,25)=5. (6,27) ? (1638, 16457)?

lcm(15,25)=75 (202,505)?

THUẬT TOÁN EUCLID

Euclid(n, m):

Input: positive integers n and $m \geq n$
Output: gcd(n, m)

```
if m mod n = 0 then
    return n
else
    return Euclid(m mod n, n)
```

Tìm $UCLN(120,48)$

Step 1: Chia m cho n: $m = n \,.\, d + r$

Step 2: Nếu $r = 0$ kết luận $UCLN(m, n) = n$

Step 3: Nếu $r \neq 0$ thì $m := n$;

$n := r$;

Step 4: Quay lại step 1

THUẬT TOÁN EUCLID

$$\textbf{Euclid}(17,42) = \textbf{Euclid}(\underbrace{42 \bmod 17}_{=8}, 17)$$

42= 2.17+8

$$= \textbf{Euclid}(\underbrace{17 \bmod 8}_{=1}, 8)$$

17=2.8+1

$$= 1.$$

8=8 .1+0

$$\textbf{Euclid}(48,1024) = \textbf{Euclid}(\underbrace{1024 \bmod 48}_{=16}, 48)$$

$$= 16.$$

$$\textbf{Euclid}(91,287) = \textbf{Euclid}(\underbrace{287 \bmod 91}_{=14}, 91) = \textbf{Euclid}(\underbrace{91 \bmod 14}_{=7}, 14) = 7.$$

287=3.91+14

91 = 6.14 +7

14 = 2.7 +0

Euclid(n,m)

- $n = 111$, $m = 202$
- n=333, m=2017
- n=156, m=360
- n=2322, m=654

THUẬT TOÁN EUCLID MỞ RỘNG

extended-Euclid(n, m):

Input: positive integers n and $m \geq n$.

Output: $x, y, r \in \mathbb{Z}$ where $\gcd(n, m) = r = xn + ym$

if $m \bmod n = 0$ **then**

  return $1, 0, n$ $//1 \cdot n + 0 \cdot m = n = \gcd(n, m)$

else

  $x, y, r :=$ **extended-Euclid**$(m \bmod n, n)$

  return $y - \left\lfloor \frac{m}{n} \right\rfloor \cdot x, x, r$

Tìm *EMR*(91,287)

287=3.91+14

91 = 6.14 +7

14 = 2.7 +0

Ta có 7=91-6.14

=91-6.(287-3.91)

=19.91-6.287

Vậy (x,y)=(19,-6)

THUẬT TOÁN EUCLID MỞ RỘNG

$$7854 = 1 \cdot 4746 + 3108$$
$$4746 = 1 \cdot 3108 + 1638$$
$$3108 = 1 \cdot 1638 + 1470$$
$$1638 = 1 \cdot 1470 + 168$$
$$1470 = 8 \cdot 168 + 126$$
$$168 = 1 \cdot 126 + 42$$
$$126 = 3 \cdot 42 + 0.$$

Vậy $UCLN(7854, 4746) = 42$

Tìm (x, y) sao cho $42 = 7854x + 4746y$

$$42 = 168 - 1 \cdot 126$$
$$= 168 - 1 \cdot (1470 - 8 \cdot 168) = 9 \cdot 168 - 1 \cdot 1470$$
$$= 9 \cdot (1638 - 1 \cdot 1470) - 1 \cdot 1470 = 9 \cdot 1638 - 10 \cdot 1470$$
$$= 9 \cdot 1638 - 10 \cdot (3108 - 1 \cdot 1638) = 19 \cdot 1638 - 10 \cdot 3108$$
$$= 19 \cdot (4746 - 1 \cdot 3108) - 10 \cdot 3108 = 19 \cdot 4746 - 29 \cdot 3108$$
$$= 19 \cdot 4746 - 29 \cdot (7854 - 1 \cdot 4746) = 48 \cdot 4746 - 29 \cdot 7854$$

Bội chung nhỏ nhất

Định lý: Cho $m, n \in Z^*$, $d = gcd(m, n)$ and $e = lcm[m, n]$. Khi đó

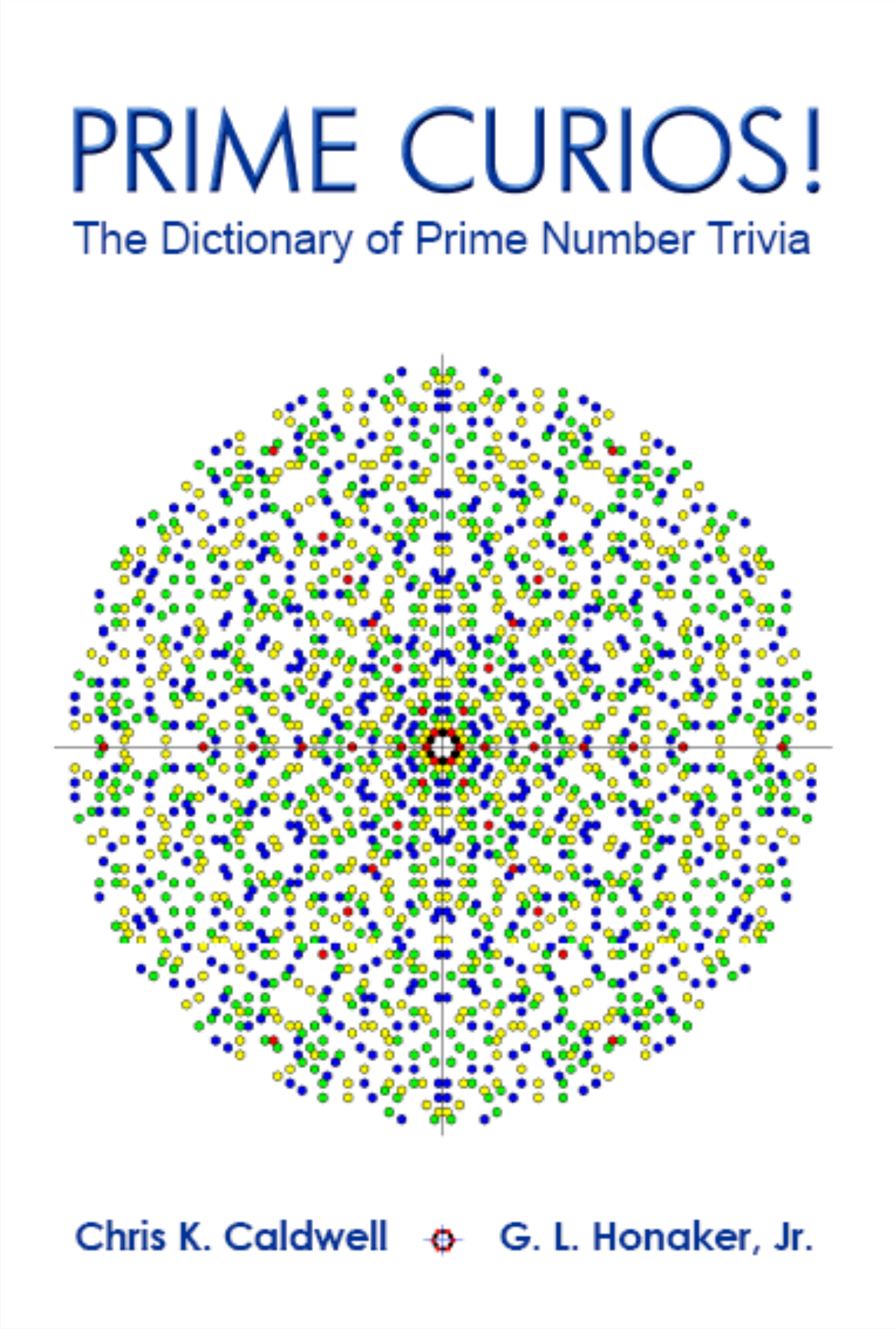
- $de = |mn|$ hay $e = \dfrac{|mn|}{d}$
- Nếu có bộ (x, y) sao cho $d = mx + ny$ thì. $\dfrac{1}{e} = \dfrac{d}{|mn|} = \dfrac{mx + ny}{|mn|} = \dfrac{u}{m} + \dfrac{v}{n}$
- $u = y$ và $v = x$ nếu $mn > 0$ và $u = -y$ và $v = -x$ nếu $mn < 0$

Ví dụ: $m = 718729, n = 397386$

Tìm d, x, y, e, u, v

4. Số nguyên

1. SỐ NGUYÊN
2. THUẬT TOÁN EUCLIDE
3. SỐ NGUYÊN TỐ
4. ĐỒNG DƯ



Số nguyên tố

Định nghĩa

Số nguyên tố là số tự nhiên lớn hơn 1 chỉ có ước dương là 1 và chính nó

	1	**2**	**3**	4	**5**	6	**7**	8	9
10	**11**	12	**13**	14	15	16	**17**	18	**19**
20	21	22	**23**	24	25	26	27	28	**29**
30	**31**	32	33	34	35	36	**37**	38	39
40	**41**	42	**43**	44	45	46	**47**	48	49
50	51	52	**53**	54	55	56	57	58	**59**
60	**61**	62	63	64	65	66	**67**	68	69
70	**71**	72	**73**	74	75	76	77	78	**79**
80	81	82	**83**	84	85	86	87	88	**89**
90	91	92	93	94	95	96	**97**	98	99

Bảng các số nguyên tố nhỏ hơn 100

Phân tích thành thừa số nguyên tố

Định lý

Định lý. [Định lý căn bản của số học] *Mọi số nguyên dương đều được phân tích thành tích hữu hạn những thừa số nguyên tố. Hơn nữa, cách phân tích này là duy nhất, sai khác một phép hoán vị các thừa số nguyên tố.*

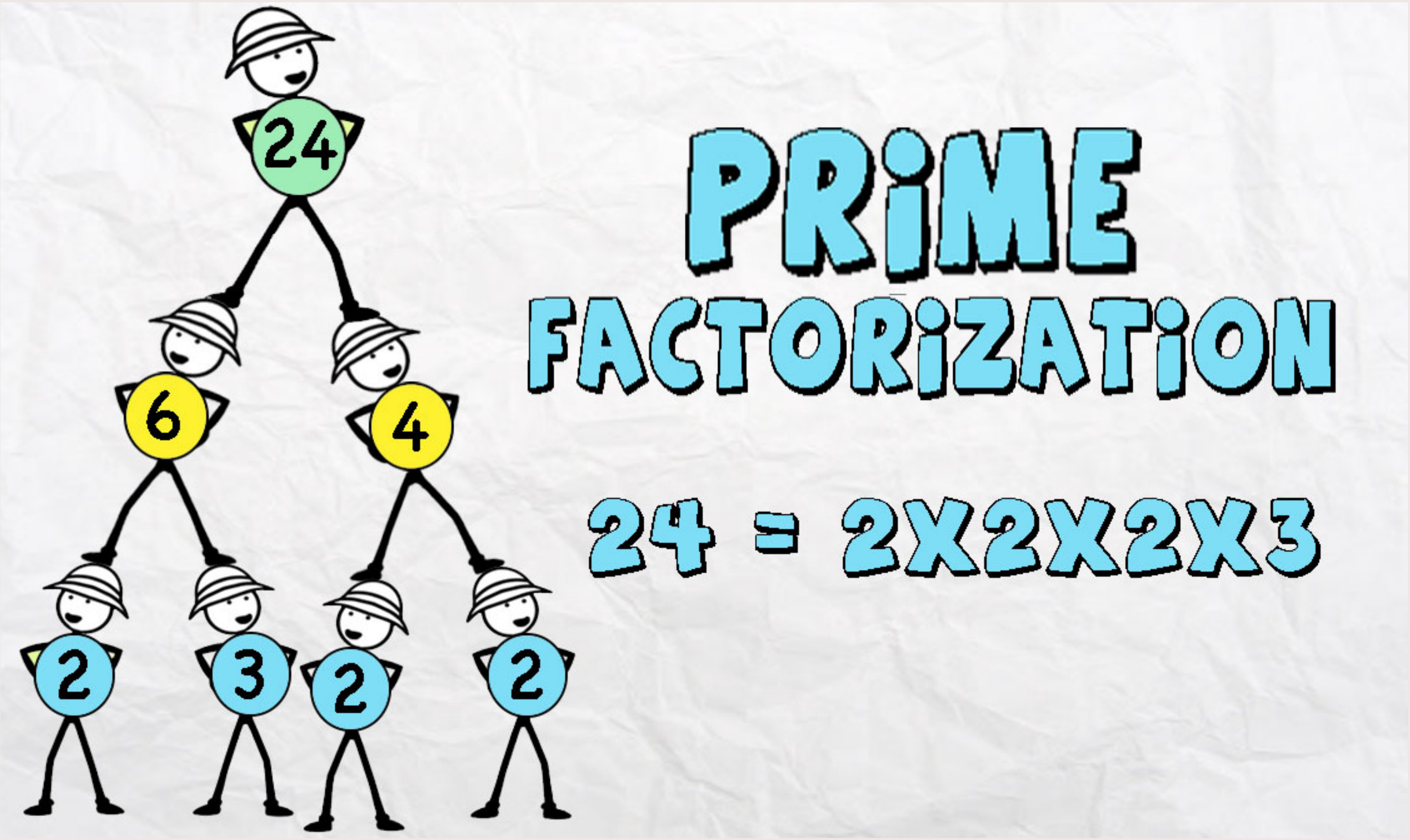
$$N = p_1^{n_1}.p_2^{n_2}\dots p_k^{n_k}$$

Ví dụ. $72600 = 2^3 \times 3 \times 5^2 \times 11^1$.

Các ước số dương của N sẽ có dạng $d = p_1^{t_1}.p_2^{t_2}\dots p_k^{t_k}$,

trong đó $0 \le t_i \le n_i$.

Số các ước dương của N sẽ là $(n_1+1)\dots(n_k+1)$.



Phân tích thành thừa số nguyên tố

Ví dụ

Phân tích các số sau ra thừa số nguyên tố.

Tìm ước chung lớn nhất, bội chung nhỏ nhất.

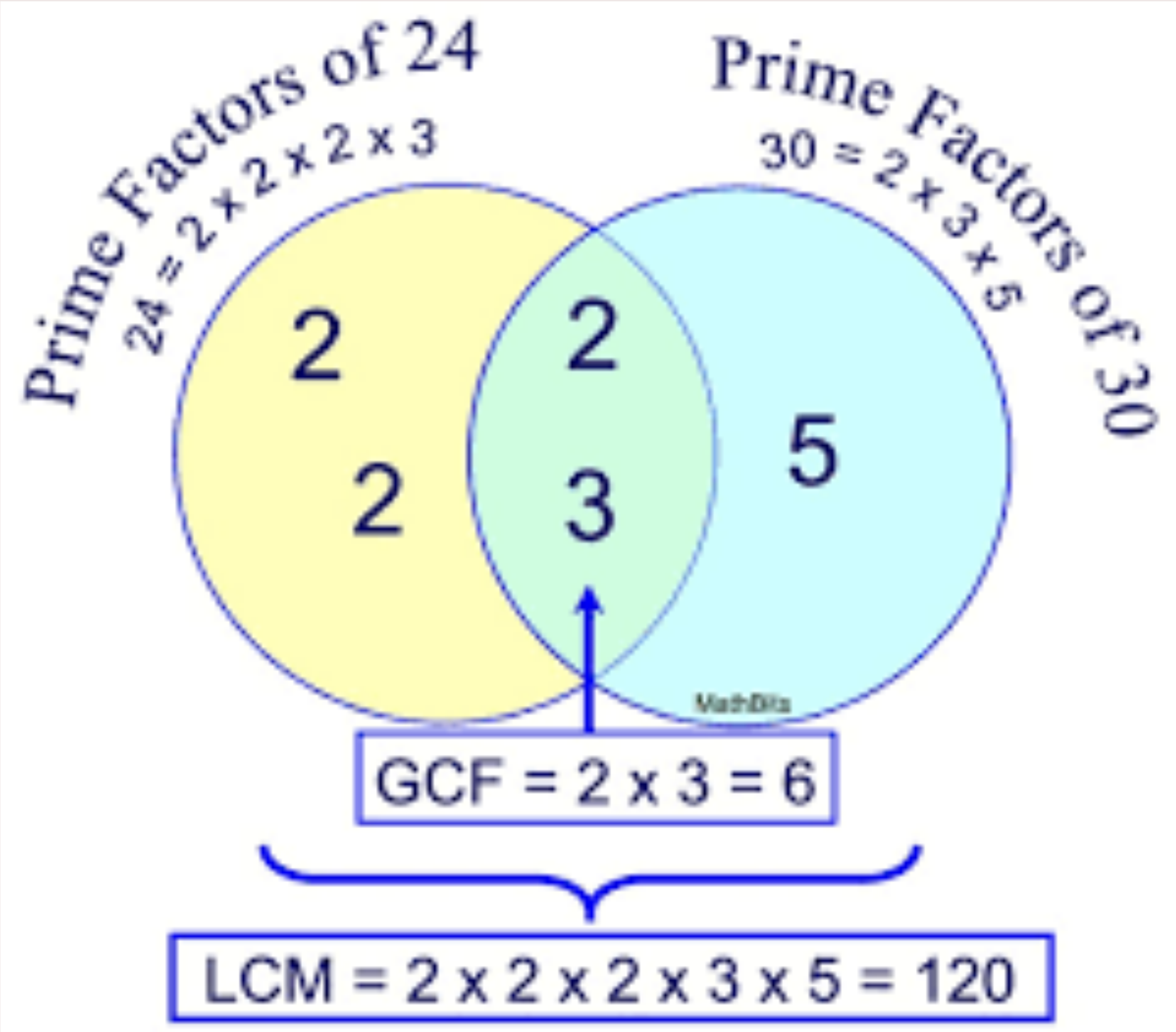
$m = 234500$

$n = 1260$

Mệnh đề Nếu $m = p_1^{h_1}.p_2^{h_2}\ldots p_t^{h_t}$ và $n = p_1^{k_1}.p_2^{k_2}\ldots p_t^{k_t}$

Thì $UCLN(m,n) = p_1^{u_1}.p_2^{u_2}\ldots p_t^{u_t}$ với $u_i = \min\{h_i, k_i\}$

$BCNN(m,n) = p_1^{b_1}.p_2^{b_2}\ldots p_t^{b_t}$ với $b_i = \max\{h_i, k_i\}$



Vô hạn số nguyên tố

Giả sử chỉ có hữu hạn các số nguyên tố là: $p_1, p_2, \ldots, p_n$. Ta xét

$$q = p_1 p_2 \ldots p_n + 1.$$

Ta có q là số nguyên tố hoặc có ước là số nguyên tố. Dễ thấy q không thể có ước là các số nguyên tố $p_1, p_2, \ldots, p_n$. Vậy q là số nguyên tố. Nhưng q không nằm trong tập các số nguyên tố ở trên. Điều này mâu thuẫn với giả thiết chỉ có hữu hạn các số nguyên tố $p_1, p_2, \ldots, p_n$.

Vậy tập hợp các số nguyên tố là vô hạn.

Nguyên tố cùng nhau

Định nghĩa. Các số nguyên a và b là nguyên tố cùng nhau, nếu chúng không có ước số nguyên tố chung, hay ước chung duy nhất của chúng là 1. gcd(a, b) = 1.

Ví dụ: Số 8 và số 15 là các số nguyên tố cùng nhau, bởi vì ước số của 8 là 1, 2, 4 và 8, còn các ước số của 15 là 1, 3, 5 và 15.

Như vậy, 1 là ước số chung duy nhất của hai số này.

Hàm Euler

$\Phi(n)$

- Số các số nguyên trong [1, n]
- Nguyên tố cùng nhau với n
- Nếu p là số nguyên tố thì $\Phi(p) = p - 1$
- Nếu p, q nguyên tố cùng nhau thì $\Phi(p\,.\,q) = \Phi(p)\Phi(q)$
- $\Phi(p^s) = p^{s-1}(p - 1)$

n	ϕ(n)	n	ϕ(n)	n	ϕ(n)
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

Đồng dư

Hai số a và b gọi là đồng dư theo modun p nếu như chúng có cùng số dư khi chia cho p. Kí hiệu là $a \equiv b \mod p$

- Ví dụ 11 đồng dư với 8 theo mod 3
- Trong $a = qb + r$ thì $a \equiv r \mod p$
- Số chẵn, số lẻ. 0 và 1. Con trai, con gái. Các thứ trong tuần, các tháng trong năm.

Tính chất:

- Nếu $a_1 \equiv b_1 (\text{mod } p)$ và $a_2 \equiv b_2 (\text{mod } p)$ thì $a_1 + a_2 \equiv b_1 + b_2 (\text{mod } p)$
- Nếu $a_1 \equiv b_1 (\text{mod } p)$ và $a_2 \equiv b_2 (\text{mod } p)$ thì $a_1 * a_2 \equiv b_1 * b_2 (\text{mod } p)$
- Nếu như $gcd(d, p) = 1$ và $a \equiv b (\text{mod } p)$, $a = a_1 d$ và $b = b_1 d$ thì $a_1 \equiv b_1 (\text{mod } p)$

Đồng dư

- Một số khi chia cho n có các số dư 0,1,2,...$n-1$
- $Z_n = \{\bar{0}, \bar{1}, \ldots \overline{n-1}\}$
- Trong Z_{13} thì $\overline{7} = \overline{7}$, $\overline{25} = \overline{12}$
- Các phép toán trên Z_n định nghĩa như sau:

  $\bar{x} + \bar{y} = \overline{x+y}$

  $\bar{x} - \bar{y} = \overline{x-y}$

  $\bar{x} \,.\, \bar{y} = \overline{x \,.\, y}$

Trong Z_9 thì $\overline{5} \,.\, \overline{6} + \overline{7} = ?$

UPCs

Chữ số kiểm tra

EXAMPLE 5 **UPCs** Retail products are identified by their **Universal Product Codes (UPCs)**. The most common form of a UPC has 12 decimal digits: the first digit identifies the product category, the next five digits identify the manufacturer, the following five identify the particular product, and the last digit is a check digit. The check digit is determined by the congruence

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

Answer these questions:

(a) Suppose that the first 11 digits of a UPC are 79357343104. What is the check digit?
(b) Is 041331021641 a valid UPC?

Khả nghịch trong Z_n

Định nghĩa. Cho số nguyên $n \geq 2$ và $x \in Z_n$. Phần tử $\overline{x}$được gọi là khả nghịch nếu tồn tại $\overline{y} \in Z_n$ sao cho $\overline{x}\overline{y} = \overline{1}$. Phần tử $\overline{y}$ được gọi là nghịch đảo của $\overline{x}$. Kí hiệu $\overline{x}^{-1}$.

Ví dụ Trong Z_9 thì $\overline{4}$ khả nghịch vì $\overline{4}\,.\,\overline{7} = \overline{1}$.

$\overline{3}$ không khả nghịch vì sao?

Mệnh đề Cho $\overline{x} \in Z_n$. Chứng minh rằng $\overline{x}$ khả nghịch khi và chỉ khi $gcd(x, n) = 1$

gcd(x,n)=1 suy ra $1 = xa + nb$ suy ra $\bar{x}b = 1$ suy ra x khả nghịch

Dùng thuật toán Euclide mở rộng để tìm khả nghịch

Bài tập

- Xét Z_{25}^{*} gồm tất các các số tự nhiên khác 0 nhỏ hơn 25 và nguyên tố cùng nhau với 25.
- Liệt kê các phần tử của Z_{25}^{*}
- Liệt kê các phần tử khả nghịch của Z_{25}^{*}
- Tìm khả nghịch của các phần tử này.

Chuẩn bị

1. Bút màu, bút chì, bút vẽ….
2. Chuẩn 3G, máy tính, smartphone
3. Đọc trước bài chương 6 Quan hệ
4. Chuẩn bị tinh thần chiến đấu!!!