CHƯƠNG V

TẬP HỢP SỐ NGUYÊN Z

I. SỰ CHIA HẾT CỦA SỐ NGUYÊN:

1.1/ ĐỊNH NGHĨA: Cho a, b $\in$ **Z**.

a) Ta nói a | b (a là *một ước số* của b hay a *chia hết* b) nếu $\exists \boldsymbol{k} \in \mathbf{Z}$, b = ***k***a.

Lúc đó ta cũng nói là b ⋮ a (b là *một bội số* của a hay b *chia hết cho* a).

b) Suy ra: a *không chia hết* b (hay b *không chia hết cho* a hay a *không là một ước số của* b hay b *không là một bội số của* a) nếu $\forall k \in \mathbf{Z}$, b $\neq$ ka. Lúc này ta dùng ký hiệu $\overline{a\,|\,b}$ hay $\overline{b \,\vdots\, a}$.

Ví dụ:

a) 12 | (– 48) [hay (– 48) ⋮ 12] vì $\exists(-4) \in \mathbf{Z}$, (– 48) = (– 4)12.

b) 17 không chia hết 65 (vì $\forall k \in \mathbf{Z}$, 65 > 17| k | nếu | k | $\leq$ 3 và 65 < 17| k | nếu | k | $\geq$ 4, nghĩa là $\forall k \in \mathbf{Z}$, 65 $\neq$ 17k).

1.2/ TÍNH CHẤT: Cho a, b, c, d $\in$ **Z**. Đặt **Z*** = **Z** \ { 0 }. Khi đó

a) a = ± 1 $\Leftrightarrow$ $\forall k \in \mathbf{Z}$, a | k. b) a $\neq$ 0 $\Leftrightarrow$ a chỉ có *hữu hạn ước số.*

c) a = 0 $\Leftrightarrow$ $\forall k \in \mathbf{Z}$, k | a $\Leftrightarrow$ a có *vô hạn ước số.*

a $\neq$ 0 $\Leftrightarrow$ $\exists k \in \mathbf{Z}$, $\overline{k\,|\,a}$ $\Leftrightarrow$ a có *chỉ có hữu hạn ước số.*

d) a | b $\Leftrightarrow$ (– a) | b $\Leftrightarrow$ a | (– b) $\Leftrightarrow$ (– a) | (– b).

e) Nếu a | b thì (b = 0 hay 0 < | a | $\leq$ | b |).

f) (a | b và b | a) $\Leftrightarrow$ a = ± b $\Leftrightarrow$ | a | = | b |.

g) (a | b , b | a và ab $\geq$ 0) $\Leftrightarrow$ a = b.

h) Nếu (a | **b** và **b** | c) thì a | c.

i) Nếu ($\mathbf{a} \mid b$ và $\mathbf{a} \mid c$) thì [$\mathbf{a} \mid (b \pm c)$ và $\mathbf{a} \mid bc$].

j) Nếu ($a \mid b$ và $c \mid d$) thì $ac \mid bd$.

k) $a \mid b \Leftrightarrow \forall k \in \mathbf{Z}, a \mid kb \Leftrightarrow \forall k \in \mathbf{Z}, ka \mid kb \Leftrightarrow$

$\Leftrightarrow \forall k \in \mathbf{Z^*}, a \mid kb \Leftrightarrow \forall k \in \mathbf{Z^*}, ka \mid kb \Leftrightarrow \exists k \in \mathbf{Z^*}, ka \mid kb$.

Việc chứng minh các tính chất trên là các bài tập đơn giản về số nguyên.

1.3/ <u>THUẬT CHIA EUCLIDE:</u> Cho $a, b \in \mathbf{Z}$ và $b \neq 0$.

Khi đó *có duy nhất* $\mathbf{q}, \mathbf{r} \in \mathbf{Z}$ thỏa $a = \mathbf{q}b + \mathbf{r}$ và $0 \leq \mathbf{r} < |b|$.

Ta nói a là *số bị chia*, b là *số chia*, **q** là *số thương* và **r** là *số dư*.

Ta ký hiệu $q = a$ *div* b, $r = a$ *mod* b và $a \equiv r \pmod{b}$.

<u>Ví dụ:</u> $140 = \mathbf{9}(15) + \mathbf{5}$ với $0 \leq \mathbf{5} < |15| = 15$ (phép chia Euclide).

$-140 = \mathbf{-10}(15) + \mathbf{10}$ với $0 \leq \mathbf{10} < |15| = 15$ (phép chia Euclide).

$140 = \mathbf{-9}(-15) + \mathbf{5}$ với $0 \leq \mathbf{5} < |-15| = 15$ (phép chia Euclide).

$-140 = \mathbf{10}(-15) + \mathbf{10}$ với $0 \leq \mathbf{10} < |-15| = 15$ (phép chia Euclide).

$140 = \mathbf{8}(15) + \mathbf{20}$ và $-140 = \mathbf{9}(-15) - \mathbf{5}$ (không phải phép chia Euclide).

II. <u>ƯỚC SỐ CHUNG DƯƠNG LỚN NHẤT:</u>

2.1/ <u>ĐỊNH NGHĨA:</u> Cho $a, b \in \mathbf{Z^*}$.

Xét $S = \{ c \in \mathbf{Z} / c \mid a$ và $c \mid b \}$ = Tập hợp *các ước số chung* của a và b.

Ta có $S \neq \varnothing$ (vì $\pm 1 \in S$) và $\forall c \in S, 1 \leq |c| \leq \min\{ |a|, |b| \}$ nên S hữu hạn.

Đặt $\mathbf{d} = \max(S)$ và gọi **d** là *ước số chung dương lớn nhất* của a và b.

Ký hiệu $\mathbf{d} = (a, b) = (b, a)$. Ta có $1 \leq \mathbf{d} \leq \min\{ |a|, |b| \}$.

<u>Ví dụ:</u> Cho $a = -36$ và $b = 48$.

Xét $S = \{ c \in \mathbf{Z} / c \mid (-36)$ và $c \mid 48 \} = \{ \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12 \}$.

Đặt $d = \max(S) = 12$ thì $d = (-36, 48) = (48, -36) = 12$.

2.2/ <u>MỆNH ĐỀ:</u> Cho a, b $\in$ **Z*** và **d** $\in$ **N*** = **N** \ {0}. Khi đó

d = (a, b) $\Leftrightarrow$ [(**d** | a), (**d** | b) và $\forall$k $\in$ **Z**, (k | a và k | b) $\Rightarrow$ k | **d**].

(**d** là *một ước số chung* của a và b) và (**d** là *bội của mọi ước chung* của a và b).

<u>Ví dụ:</u> Cho a = 75, b = 100 và S = {c $\in$ **Z** / c | 75 và c | 100} = {$\pm$ 1, $\pm$ 5, $\pm$ 25}.

Ta có d = (75, 100) = 25 vì 25 $\in$ S $\cap$ **N*** và $\forall$k $\in$ S, k | 25.

2.3/ <u>MỆNH ĐỀ:</u> Cho a, b $\in$ **Z*** và **d** $\in$ **N***. Khi đó

d = (a, b) $\Leftrightarrow$ [(**d** | a), (**d** | b) và $\exists$*r*, *s* $\in$ **Z**, **d** = *r*a + *s*b (*r* và *s* *không duy nhất*)]

(**d** là *một ước số chung* của a và b) và (**d** là *một tổ hợp nguyên* của a và b).

<u>Ví dụ:</u>

a) (12, – 32) = **4** vì **4** | 12, **4** | (– 32) và $\exists$(–5), (–2) $\in$ **Z**, **4** = (–5)12 + (–2)(–32).

Ta cũng thấy $\exists$ 3, 1$\in$ **Z**, **4** = 3(12) + 1(– 32).

b) (9, 20) = **1** vì **1** | 9, **1** | 20 và $\exists$9, (– 4) $\in$ **Z**, **1** = (9)9 + (– 4)20.

Ta cũng thấy $\exists$ (– 11) , 5$\in$ **Z**, **1** = (– 11)9 + 5(20).

2.4/ <u>TÍNH CHẤT:</u> Cho a, b, λ $\in$ **Z***. Khi đó

a) (a, b) = (– a, b) = (a, – b) = (– a, – b) và (λa, λb) = | λ | (a, b).

b) Nếu a | b thì (a, b) = | a |. Đặc biệt ($\pm$ a, $\pm$ a) = | a |.

<u>Ví dụ:</u>

a) (36, 48) = (– 36, 48) = (36, – 48) = (– 36, – 48) = 12.

b) (– **7** $\times$ 36, – **7** $\times$ 48) = | – **7** | (36, 48) = **7** $\times$ 12 = 84.

c) (– 15, 90) = | – 15 | = 15 vì (– 15) | 90. Đặc biệt ($\pm$ 57, $\pm$ 57) = | $\pm$ 57 | = 57.

2.5/ <u>BỔ ĐỀ:</u> Cho a, b $\in$ **Z*** thỏa | a | > | b | và b không chia hết a.

Chia Eucide **a** = q**b** + **r** với 0 < **r** < | **b** |. Khi đó (**a**, **b**) = (**b**, **r**).

$$\mathbf{a = qb + r} \quad \textbf{với} \;\; \mathbf{0 < r < |\, b\,|}$$

Ý nghĩa : Tìm (**b**, **r**) thay cho (**a**, **b**) với sự thuận lợi là **r** < | b | < | a |.

<u>Ví dụ:</u> Cho a = 79.822 và b = – 57.442 với | a | > | b |. Tính d = (a, b).

Chia Euclide liên tiếp (**số chia** và **số dư** *ở bước trước* lần lượt trở thành **<u>số bị chia</u>** và **<u>số chia</u>** *ở bước ngay sau*) và quá trình chia sẽ dừng khi số dư bằng 0 :

$$\mathbf{a = qb + r} \quad \textbf{với } \mathbf{0 < r < |\,b\,|}$$

$$\mathbf{b = sr + t} \quad \textbf{với } \mathbf{0 \leq t < |\,r\,|}$$

a = – **b** + **22.380** [1], **b** = – 3(**22.380**) + **9.698** [2],

22.380 = 2(**9.698**) + **2.984** [3], **9.698** = 3(**2.984**) + **746** [4] và

2.984 = 4(**746**) + **<u>0</u>** [5]. Từ [1], [2], [3], [4], [5], ta có

d = (**a**, **b**) = (**b**, **22.380**) = (**22.380**, **9.698**) = (**9.698**, **2.984**) = (**2.984**, **746**) = **746**.

2.6/ <u>THUẬT TOÁN TÌM ƯỚC SỐ CHUNG DƯƠNG LỚN NHẤT VÀ BIỂU DIỄN TỔ HỢP NGUYÊN:</u>

a) Vấn đề : Cho a, b $\in$ **Z*** thỏa | a | > | b |.

Tìm **d** = (a, b) và tìm $r, s \in \mathbf{Z}$ thỏa **d** = *r*a + *s*b.

b) Chia Euclide liên tiếp

$\mathbf{a} = \mathbf{q_o}.b + \mathbf{r_o}$ ($0 < \mathbf{r_o} < |\,b\,|$) [1].

$\mathbf{b} = \mathbf{q_1}.r_o + \mathbf{r_1}$ ($0 < \mathbf{r_1} < |\,r_o\,| = r_o$) [2].

$\mathbf{r_o} = \mathbf{q_2}.r_1 + \mathbf{r_2}$ ($0 < \mathbf{r_2} < |\,r_1\,| = r_1$) [3].

$\mathbf{r_1} = \mathbf{q_3}.r_2 + \mathbf{r_3}$ ($0 < r_3 < |\,r_2\,| = r_2$) [4].

$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$

$\mathbf{r_{n-4}} = \mathbf{q_{n-2}}.r_{n-3} + \mathbf{r_{n-2}}$ ($0 < r_{n-2} < |\,r_{n-3}\,| = r_{n-3}$) [n – 1].

$\mathbf{r_{n-3}} = \mathbf{q_{n-1}}.r_{n-2} + \mathbf{r_{n-1}}$ ($0 < r_{n-1} < |\,r_{n-2}\,| = r_{n-2}$) [n].

$\mathbf{r_{n-2}} = \mathbf{q_n}.r_{n-1} + \underline{\mathbf{0}}$ (*phép chia dừng* khi *số dư* $\mathbf{r_n} = \mathbf{0}$) [n + 1].

Từ các đẳng thức [1], [2], [3], … , [n], [n + 1] và theo (**2.5**), ta có

$\mathbf{d} = (a, b) = (b, r_o) = (r_o , r_1) = (r_1 , r_2) = \ldots = (r_{n-3} , r_{n-2}) = (r_{n-2} , r_{n-1}) = \mathbf{r_{n-1}}$.

Từ các đẳng thức [n], [n – 1], … , [3], [2] và [1], ta biểu diễn các số dư

$\mathbf{d} = \mathbf{r_{n-1}} = 1.\mathbf{r_{n-3}} - q_{n-1}.\mathbf{r_{n-2}} = 1.\mathbf{r_{n-3}} - q_{n-1}(\mathbf{r_{n-4}} - q_{n-2}.\mathbf{r_{n-3}}) =$

$= - q_{n-1}.\mathbf{r_{n-4}} + (1 + q_{n-1}.q_{n-2})\mathbf{r_{n-3}} = \ldots ,$

d lần lượt được biểu diễn là một tổ hợp nguyên của $\{ \mathbf{r_{n-2}} , \mathbf{r_{n-3}} \}$, của

$\{ \mathbf{r_{n-3}} , \mathbf{r_{n-4}} \}$, … , của $\{ \mathbf{r_1} , \mathbf{r_o} \}$, của $\{ \mathbf{r_0} , \mathbf{b} \}$ và sau hết là của $\{ \mathbf{b}, \mathbf{a} \}$.

<u>Ví dụ:</u> Cho a = – 718.729 và b = 397.386 với | a | > | b |.

Tính d = (a, b) và tìm r, s ∈ **Z** thỏa d = ra + sb.

Chia Euclide liên tiếp : **a** = **– 2b** + **76.043** [1], **b** = 5(**76.043**) + **17.171** [2],

76.043 = 4(**17.171**) + **7.359** [3], **17.171** = 2(**7.359**) + **2.453** [4] và

7.359 = 3(**2.453**) + **<u>0</u>** [5]. Từ [1], [2], [3], [4] và [5], ta có **d** = (**a**, **b**) =

= (**b**, **76.043**) = (**76.043**, **17.171**) = (**17.171**, **7.359**) = (**7.359**, **2.453**) = **2.453**.

Từ [4], [3], [2] và [1], ta biểu diễn liên tiếp các số dư **d** = **2453** =

= **17.171** – 2(**7.359**) = **17.171** – 2[**76.043** – 4(**17.171**)] = – 2(**76.043**) + 9(**17.171**)

= – 2(**76.043**) + 9[**b** – 5(**76.043**)] = 9**b** – 47(**76.043**) = 9**b** – 47(**a** + 2**b**)] =

= – 47**a** – 85**b**. Vậy **d** = **2.453** = **ra** + s**b** với r = – 47 và s = – 85.

III. <u>BỘI SỐ CHUNG DƯƠNG NHỎ NHẤT:</u>

3.1/ <u>ĐỊNH NGHĨA:</u> Cho a, b ∈ **Z*** và

T = { c ∈ **N*** / c⋮a và c⋮b } = Tập hợp *các bội số chung dương* của a và b.

Ta có T ≠ ∅ (vì | ab | ∈ T) và ∀c ∈ T, c ≥ max { | a |, | b | }.

Đặt **e** = min(T) và gọi **e** là *bội số chung dương nhỏ nhất* của a và b.

Ký hiệu **e** = [a, b] = [b, a]. Ta có max { | a |, | b | } ≤ **e** ≤ | ab |.

Ví dụ: Cho $a = -36 = -2^2.3^2$ và $b = 48 = 2^4.3^1$.

Xét $T = \{ c \in \mathbf{N^*} / c \vdots (-36)$ và $c \vdots 48 \} = \{ 2^4.3^2.t \ / \ t \in \mathbf{N^*} \}$.

Đặt $e = \min(T) = 2^4.3^2 = 144$ (với $t = 1$) thì $e = [-36, 48] = [48, -36] = 144$.

3.2/ MỆNH ĐỀ: Cho $a, b \in \mathbf{Z^*}$ và $\mathbf{e} \in \mathbf{N^*}$. Khi đó

$\mathbf{e} = [a, b] \Leftrightarrow [(\mathbf{e} \vdots a), (\mathbf{e} \vdots b)$ và $\forall k \in \mathbf{Z}, (k \vdots a$ và $k \vdots b) \Rightarrow k \vdots \mathbf{e}]$.

(**e** là *một bội số chung* của a và b) và (**e** là *ước của mọi bội chung* của a và b).

Ví dụ: Cho $a = 75 = 3.5^2$, $b = 100 = 2^2 5^2$ và

$L = \{ c \in \mathbf{Z} / c \vdots 75$ và $c \vdots 100 \} = \{ 2^2.3.5^2.t \ / \ t \in \mathbf{Z^*} \} = \{ 300t \ / \ t \in \mathbf{Z^*} \}$.

Ta có $e = [75, 100] = 300$ vì $300 \in L \cap \mathbf{N^*}$ và $\forall k \in L, 300 \mid k$.

3.3/ MỆNH ĐỀ: Cho $a, b \in \mathbf{Z^*}$ và $\mathbf{e} \in \mathbf{N^*}$. Khi đó

$\mathbf{e} = [a, b] \Leftrightarrow [(\mathbf{e} \vdots a), (\mathbf{e} \vdots b)$ và $\exists u, v \in \mathbf{Z}, \frac{1}{e} = \frac{u}{a} + \frac{v}{b}$ (u và v *không duy nhất*)].

(e là *một bội số chung* của a và b) và ($\frac{1}{e}$ là *một tổ hợp nguyên* của $\frac{1}{a}$ và $\frac{1}{b}$).

Ví dụ:

$[12, -32] = 96$ vì $\mathbf{96} \vdots 12, \mathbf{96} \vdots (-32)$ và $\exists (-1), (-3) \in \mathbf{Z}, \frac{1}{96} = \frac{(-1)}{12} + \frac{(-3)}{(-32)}$.

Ta cũng thấy $\exists\, 2, 5 \in \mathbf{Z}, \frac{1}{96} = \frac{2}{12} + \frac{5}{(-32)}$.

3.4/ TÍNH CHẤT: Cho $a, b, \lambda \in \mathbf{Z^*}$. Khi đó

a) $[a, b] = [-a, b] = [a, -b] = [-a, -b]$ và $[\lambda a, \lambda b] = |\lambda| [a, b]$.

b) Nếu $a \mid b$ thì $[a, b] = |b|$. Đặc biệt $[\pm a, \pm a] = |a|$.

Ví dụ:

a) $[36, 48] = [-36, 48] = [36, -48] = [-36, -48] = 144$.

b) $[-\mathbf{7} \times 36, -\mathbf{7} \times 48] = |-\mathbf{7}| [36, 48] = \mathbf{7} \times 144 = 1.008$.

c) $[15, -90] = |-90| = 90$ vì $15 \mid (-90)$. Đặc biệt $[\pm 57, \pm 57] = |\pm 57| = 57$.

3.5/ <u>ĐỊNH LÝ:</u> Cho a, b $\in$ **Z*** với **d** = (a, b) và **e** = [a, b]. Khi đó

a) **de** = | ab | . Suy ra **e** $= \frac{|ab|}{d}$. (nên tính **e** $= \frac{|a|}{d}.|b|$ thì thuận tiện hơn).

b) Chọn $r, s \in \mathbf{Z}$ thỏa **d** = ra + sb thì $\frac{1}{e} = \frac{d}{|ab|} = \frac{ra+sb}{|ab|} = \frac{u}{a} + \frac{v}{b}$ trong đó

* Nếu ab > 0 thì $\frac{1}{e} = \frac{ra+sb}{ab} = \frac{s}{a} + \frac{r}{b}$ ($u = s$ và $v = r$).

* Nếu ab < 0 thì $\frac{1}{e} = \frac{ra+sb}{-ab} = \frac{(-s)}{a} + \frac{(-r)}{b}$ ($u = -s$ và $v = -r$).

<u>**Ví dụ:**</u> a = – 718.729 và b = 397.386 có d = (a, b) = 2453 nên

e = [a, b] = $\frac{|ab|}{d} = \frac{|a|}{d}.|b|$ = 293 × 397.386 = 116.434.098.

Hơn nữa do ab < 0 và d = ra + sb với r = – 47 và s = – 85 nên

$\frac{1}{e} = \frac{d}{|ab|} = \frac{-47a-85b}{-ab} = \frac{85}{a} + \frac{47}{b}$. Vậy $\frac{1}{e} = \frac{u}{a} + \frac{v}{b}$ với u = 85 và v = 47.

IV. <u>SỰ NGUYÊN TỐ CÙNG NHAU:</u>

4.1/ <u>ĐỊNH NGHĨA:</u> Cho a, b $\in$ **Z***.

a) Ta nói a và b là hai số *nguyên tố cùng nhau* nếu a và b chỉ có hai ước số chung là ± 1, nghĩa là (a, b) = 1.

b) Suy ra a và b là hai số *không nguyên tố cùng nhau* nếu (a, b) ≥ 2.

<u>**Ví dụ:**</u> Do (– 25, 42) = 1 nên – 25 và 42 là hai số nguyên tố cùng nhau.

Do (84, 56) = 28 ≥ 2 nên 84 và 56 là hai số không nguyên tố cùng nhau.

4.2/ <u>MỆNH ĐỀ:</u> Cho a, b $\in$ **Z***. Khi đó

(a, b) = **1** $\Leftrightarrow$ $\exists r, s \in \mathbf{Z}$ thỏa **1** = ra + sb.

<u>**Ví dụ:**</u> Ta có 5(17) + (– 12)7 = **1** nên ta thấy có 16 cặp số nguyên tố cùng nhau là (± 5, ± 12) = (± 5, ± 7) = (± 17, ± 12) = (± 17, ± 7) = **1**.

4.3/ <u>MỆNH ĐỀ:</u> Cho a, b, c $\in$ **Z***.

a) Nếu (**a**, b) = 1 = (**a**, c) thì (**a**, bc) = 1.

b) Nếu [**a** | bc và (**a**, b) = **1**] thì **a** | c.

c) Nếu [a | **c** , b | **c** và (a, b) = **1**] thì ab | **c**.

Ví dụ:

a) (**12**, 25) = 1 = (**12**, – 47) nên (**12**, 25 × [– 47]) = 1.

b) **19** | (76 × 31) và (**19**, 31) = 1 nên **19** | 76.

c) 9 | **1188**, – 22 | **1188** và (9, – 22) = 1 nên 9(– 22) | **1188**.

4.4/ DẠNG TỐI GIẢN CỦA MỘT SỐ HỮU TỈ :

Cho a, b ∈ **Z*** và $\frac{a}{b}$ ∈ **Q*** = **Q** \ { 0 }. Đặt d = (a, b) và viết a = da’, b = db’.

Ta có $\frac{a}{b} = \frac{a'}{b'} = \frac{-a'}{-b'}$ với (a’, b’) = (– a’, – b’) = **1**.

Ta nói $\frac{a}{b}$ có *hai dạng tối giản* (không giản ước được) là $\frac{a'}{b'}$ và $\frac{-a'}{-b'}$.

Ví dụ:

a = 79.822 và b = – 57.442. Ta có d = (a, b) = 746, a = 107d và b = – 77d.

Suy ra $\frac{a}{b} = \frac{107d}{-77d} = \frac{107}{-77} = \frac{-107}{77}$. Vậy $\frac{a}{b}$ có hai dạng tối giản là $\frac{-107}{77}$ và $\frac{107}{-77}$

vì (– 107, 77) = (107, – 77) = 1.

V. SỰ PHÂN TÍCH NGUYÊN TỐ:

5.1/ SỐ NGUYÊN TỐ : Cho p ∈ **Z** và | p | ≥ 2 (nghĩa là 0 ≠ p ≠ ± 1).

a) Ta nói p là *một số nguyên tố* nếu p chỉ có hai ước số dương là 1 và | p |
(nghĩa là p chỉ có 4 ước số là ± 1 và ± p).

b) Suy ra q là một số *không nguyên tố* (còn gọi là *hợp số*) nếu q có hơn hai ước số dương.

Ví dụ:

Các số nguyên tố đầu tiên ± 2, ± 3, ± 5, ± 7, ± 11, ± 13, ± 17, ± 19, ± 23, ± 29, ...

Tập hợp các số nguyên tố là một tập hợp vô hạn (một bài tập hay).

Ta có ± 28 là một hợp số vì ± 28 có hơn hai ước số dương là 1, 2, 4, ...

5.2/ <u>MỆNH ĐỀ:</u> Cho $p \in \mathbf{Z}$ và $| p | \geq 2$. Các phát biểu sau là *tương đương* :

a) p nguyên tố.

b) $\forall k \in \mathbf{Z}^*$, $\overline{p \mid k} \Rightarrow (p, k) = \mathbf{1}$.

c) $\forall k \in \mathbf{Z}^*$, $(p, k) \neq \mathbf{1} \Rightarrow p \mid k$.

d) $\forall a, b \in \mathbf{Z}^*$, $p \mid ab \Rightarrow (p \mid a$ hay $p \mid b)$.

e) $\forall a, b \in \mathbf{Z}^*$, $(\overline{p \mid a}$ và $\overline{p \mid b}) \Rightarrow \overline{p \mid ab}$.

<u>Ví dụ:</u> 83 là số nguyên tố, $\overline{83 \mid 724}$ và $\overline{83 \mid 615}$ nên $(83, 724) = \mathbf{1}$ và $\overline{83 \mid (724).(615)}$.

5.3/ <u>ĐỊNH LÝ PHÂN TÍCH NGUYÊN TỐ:</u> Cho $k \in \mathbf{Z}$ và $| k | \geq 2$.

Khi đó k được phân tích một cách duy nhất dưới dạng $k = \pm p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ (*)

trong đó $p_1 < p_2 < \cdots < p_m$ là các số nguyên tố > 0 và $r_1, r_2, \ldots, r_m \in \mathbf{N}^*$.

(*) được gọi là *sự phân tích nguyên tố* của k.

<u>Ví dụ:</u> $178.200 = 2^3.3^4.5^2.11^1$ và $-102.375 = -3^2.5^3.7^1.13^1$.

5.4/ <u>MỆNH ĐỀ:</u> Cho $a, b \in \mathbf{Z} \setminus \{0, \pm 1\}$.

Phân tích nguyên tố $a = \pm p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ và $b = \pm q_1^{s_1} q_2^{s_2} \ldots q_n^{s_n}$. Khi đó

a) $(a, b) = \mathbf{1} \Leftrightarrow \{ p_1, p_2, \ldots, p_m \} \cap \{ q_1, q_2, \ldots, q_n \} = \varnothing$.

b) $(a, b) \geq 2 \Leftrightarrow \{ p_1, p_2, \ldots, p_m \} \cap \{ q_1, q_2, \ldots, q_n \} \neq \varnothing$.

<u>Ví dụ:</u> Ta có $(\pm 2^3.5^4.11^2.19^8.29^5, \pm 3^6.7^{10}.13^2.17^7.23^1.31^4) = \mathbf{1}$ vì

$$\{ 2, 5, 11, 19, 29 \} \cap \{ 3, 7, 13, 17, 23, 31 \} = \varnothing.$$

Ta có $(\pm 2^2.3^4.11^1.13^5.29^4, \pm 3^3.5^2.7^8.17^4.29^6) \geq 2$ vì

$$\{ 2, 3, 11, 13, 29 \} \cap \{ 3, 5, 7, 17, 29 \} = \{ 3, 29 \} \neq \varnothing.$$

5.5/ <u>ÁP DỤNG:</u> Cho $a, b \in \mathbf{Z} \setminus \{0, \pm 1\}$. Ta có thể tìm $\mathbf{d} = (a, b)$, $\mathbf{e} = [a, b]$ và các dạng tối giản của phân số $\frac{a}{b}$ dựa theo sự phân tích nguyên tố của a và b.

Phân tích nguyên tố một cách " thỏa hiệp " giữa a và b như sau:

$a = \pm\, p_1^{r_1} p_2^{r_2} ... p_m^{r_m}$ và $b = \pm\, p_1^{s_1} p_2^{s_2} ... p_m^{s_m}$ trong đó $p_1 < p_2 < \cdots < p_m$ là các số nguyên tố > 0 và $r_1, s_1, r_2, s_2, \ldots, r_m, s_m \in \mathbf{N}$ sao cho $r_i + s_i \geq 1$ $(1 \leq i \leq m)$.

Đặt $u_i = \min\{ r_i, s_i \}$ và $v_i = \max\{ r_i, s_i \}$ $(1 \leq i \leq m)$.

Khi đó $\mathbf{d} = (a, b) = p_1^{u_1} p_2^{u_2} ... p_m^{u_m}$, $\mathbf{e} = [\, a, b \,] = p_1^{v_1} p_2^{v_2} ... p_m^{v_m}$ và các dạng tối giản của $\frac{a}{b}$ lần lượt là

$$\frac{a}{b} = \frac{\operatorname{sgn}(a) p_1^{r_1 - u_1} p_2^{r_2 - u_2} ... p_m^{r_m - u_m}}{\operatorname{sgn}(b) p_1^{s_1 - u_1} p_2^{s_2 - u_2} ... p_m^{s_m - u_m}} \text{ hay } \frac{a}{b} = \frac{-\operatorname{sgn}(a) p_1^{r_1 - u_1} p_2^{r_2 - u_2} ... p_m^{r_m - u_m}}{-\operatorname{sgn}(b) p_1^{s_1 - u_1} p_2^{s_2 - u_2} ... p_m^{s_m - u_m}} \text{ trong đó}$$

sgn(a) và sgn(b) là dấu của a và b.

<u>Ví dụ:</u> $a = 2^3.3^5.7^4.13^2.17^3$ và $b = -\, 2^8.5^2.7^2.11^3.17^9.19^1$ có các dạng phân tích nguyên tố một cách " thỏa hiệp " lần lượt là

$a = 2^3.3^5.5^0.7^4.11^0.13^2.17^3.19^0$ và $b = -\, 2^8.3^0.5^2.7^2.11^3.13^0.17^9.19^1$. Ta suy ra

$d = (a, b) = 2^3 3^0 5^0 7^2 11^0 13^0 17^3 19^0 = 2^3 7^2 17^3$ và $e = [\, a, b \,] = 2^8 3^5 5^2 7^4 11^3 13^2 17^9 19^1$

Các dạng tối giản của số hữu tỉ $\frac{a}{b}$ lần lượt là $\frac{3^5.7^2.13^2}{-2^5.5^2.11^3.17^6.19^1}$ và $\frac{-3^5.7^2.13^2}{2^5.5^2.11^3.17^6.19^1}$.

5.6/ <u>MÔ TẢ CÁC ƯỚC SỐ CỦA SỐ NGUYÊN:</u> Cho $k \in \mathbf{Z}$ với $|\, k \,| \geq 2$.

Phân tích nguyên tố $k = \pm\, p_1^{r_1} p_2^{r_2} ... p_m^{r_m}$. Khi đó

a) Tập hợp *các ước số nguyên dương* và tập hợp *các ước số nguyên* của k lần lượt là

$A = \{\, p_1^{t_1} p_2^{t_2} ... p_m^{t_m} \;/\; t_1, t_2, \ldots, t_m \in \mathbf{N}$ và $0 \leq t_j \leq r_j \;(1 \leq j \leq m) \,\}$ và

$B = \{\, \pm\, p_1^{t_1} p_2^{t_2} ... p_m^{t_m} \;/\; t_1, t_2, \ldots, t_m \in \mathbf{N}$ và $0 \leq t_j \leq r_j \;(1 \leq j \leq m) \,\}$.

b) Dùng nguyên lý nhân cho đồng thời các số nguyên $t_1, t_2, \ldots, t_m \in \mathbf{N}$, ta có

$|\, A \,| = (r_1 + 1)(r_2 + 1)\ldots(r_m + 1)$ và $|\, B \,| = 2.|\, A \,| = 2(r_1 + 1)(r_2 + 1)\ldots(r_m + 1)$.

<u>Ví dụ:</u> $k = -\,2^5.3^2.5^4.11^3.19^4$ có tập hợp các ước số nguyên dương và tập hợp các ước số nguyên lần lượt là

$A = \{\ 2^a.3^b.5^c.11^d.19^e$ / a, b, c, d, e $\in$ **N** và $a \le 5, b \le 2, c \le 4, d \le 3$ và $e \le 4\ \}$

và $B = \{\pm\ 2^a.3^b.5^c.11^d.19^e$ / a, b, c, d, e $\in$ **N** và $a \le 5, b \le 2, c \le 4, d \le 3$ và $e \le 4\}$

Suy ra $|\,A\,| = (5 + 1)(2 + 1)(4 + 1)(3 + 1)(4 + 1) = 1.800$ và $|\,B\,| = 2.|\,A\,| = 3.600$.
