7.កម្មសិទ្ធិ នៃ $P.G.C.D$ (*Propriété du P.G.C.D.*)

1°/ $\boldsymbol{P.G.C.D}$ **ជា វិធី គណនា មានលក្ខណៈ ត្រលប់** (*opération commutative*)។

ពីព្រោះតាម និយមន័យ នៃ $P.G.C.D.(a,b)$ ចំនួន a និង b មានមុខងារដូចគ្នា។

2°/ $\boldsymbol{P.G.C.D}$ **ជា វិធី គណនា មានលក្ខណៈ ផ្តុំ** (*opération associative*)

ចំនួន a b និង c គេឲ្យ ។ យើងតាងដោយ ៖

A សំនុំ នៃ តួចែកទាំងអស់ របស់ a B សំនុំ នៃ តួចែកទាំងអស់ របស់ b

C សំនុំ នៃ តួចែកទាំងអស់ របស់ c ។ ហើយ $x \wedge y$ តាង $P.G.C.D.$ របស់ x និង y ។

ដូច្នេះ $a \wedge b$ ជា ធាតុដែលធំជាងគេនៅក្នុង $A \cap B$ ហើយ $(a \wedge b) \wedge c$ ជា ធាតុដែលធំជាងគេនៅក្នុង $(A \cap B) \cap C$ ។ ហើយក៏ដូចគ្នាដែរ $a \wedge (b \wedge c)$ ជា ធាតុដែលធំជាងគេនៅក្នុង $A \cap (B \cap C)$ ។ ហើយដោយ ប្រសព្វ (*intersection*)នៃសំនុំ មានលក្ខណៈ ផ្តុំ នោះ គេបាន ៖ $(A \cap B) \cap C = A \cap (B \cap C)$ => $(a \wedge b) \wedge c = a \wedge (b \wedge c)$។

ដូច្នេះ ចំពោះ $P.G.C.D.$ នៃចំនួនជាច្រើនដូចជា $a_1, a_2, \ldots\ldots, a_n$ យើងអាចសរសេរ ដោយ $a_1 \wedge a_2 \wedge \ldots\ldots \wedge a_n$ ដោយមិនចាំបាច់ប្រើ វង្វង់ក្រចក (..) ហើយក៏មិនបាច់រវល់ ពី លំដាប់ ដែលត្រូវសរសេរ ចំនួនទាំងនោះទៀតផង។

3°/ <u>**ការស្មើ (IV,7,1)**</u>

បើ គេ គុណ គ្រប់ចំនួន $\boldsymbol{a_i}$ ដោយ ចំនួនដដែល $\boldsymbol{m}$ នោះ $\boldsymbol{P.G.C.D.}$ នៃចំនួនទាំងនោះ ក៏គុណនឹង $\boldsymbol{m}$ ដែរ ។

យើងបានឃើញ តាម <u>**ក្បួនដោះស្រាយអឺគ្លីត** (Algorithme d'Euclide)</u> កាលណាគេ គេគុណ ចំនួន a និង b ដោយ ចំនួន m តែមួយ នោះ សំណល់ នៃការចែក តៗ មក ក៏គុណនឹង m ដែរ ។ ដូច្នេះ សំណល់ចុងក្រោយ មិនសូន្យ ក៏គុណនឹង m ដែរ ។ ដូច្នេះ

យើង បានបង្ហាញ ការស្មើ ដោយ ពីរ ចំនួន។ ហើយលទ្ធផលនេះក៏អាចពង្រីកទៅ ករណី ជាទូទៅ។

<u>ទ្រឹស្តីបទ ប៊ីហ្សូត</u> **(<u>Théorème de Bezout</u>)**

បើ d ជា P.G.C.D. នៃ ចំនួន a និង b នៅពេលនោះគេអាច រកបានទូវចំនួនគត់ ធម្មជាតិពីរ x និង y ដែលឲ្យ d = ax – by ។

*ដើម្បី បង្ហាញ ទ្រឹស្តីបទនេះ គេគ្រាន់តែ ប្រើឡើងវិញ **<u>ក្បួនដោះស្រាយអឺគ្លីត</u>*** <u>(Algorithme d'Euclide)</u> *ដោយបង្ហាញថា សំណល់* y_i *នីមួយៗ បានមកពីការចែក តៗគ្នានោះ គេអាចសរសេរ ជារាង* $y_i = u_i a - v_i b$ *ដោយយកចំនួន ដ៏សមរម្យ ចំពោះ* u_i *និង* v_i *។ ហើយបន្ទាប់មក យើងប្រើ ការបង្ហាញដោយ រ៉េការ៉េង់ ។*

<u>ឧទាហរណ៍ ជាជំនួយ</u>

មុននឹងបន្តទៅមុខទៀត ខ្ញុំសូមលើកជាឧទាហរណ៍ខ្លះដូចតទៅនេះ ៖

<u>A – ឧទាហរណ៍ទី១</u> *ស្តីពី ក្បួនដោះស្រាយ អឺគ្លីត* (Algorithme d'Euclide)

ក្បួននេះ អាចឲ្យ $P.G.C.D.$ *នៃ ចំនួន a និង b។ ឥឡូវនេះ យើងរក* $P.G.C.D.$ *នៃ ចំនួន a និង b ដោយ សន្មត ថា* $a > b$ *ហើយ សំណល់ នៃការចែក ទី ៥ ស្មើនឹងសូន្យ ។*

ក្បួនដោះស្រាយអឺគ្លីត ប្រើរូបមន្ត ៖ $a = bq + r$ *ដោយ* $r < b$ *។*

តទៅនេះ យើងតាង a, b, r *ដោយប្រើ សន្ទស្សន៍ ហើយយើងបាន៖*

$a = b_0$
$b = b_1$
$r = b_2$ *ដូច្នេះ*

$b_0 = b_1 q_1 + b_2$ *ដោយ* $b_2 < b_1$

$b_1 = b_2 q_2 + b_3$ *ដោយ* $b_3 < b_2$

$b_2 = b_3 q_3 + b_4$ *ដោយ* $b_4 < b_3$

$b_3 = b_4 q_4 + b_5$ ដោយ $b_5 < b_4$

ដោយ $b_1 > b_2 > b_3 > b_4 > b_5 > \cdots$ ដូច្នេះ សំណល់ $\boldsymbol{b_i}$ ត្រូវតែសូន្យកាលណា យើងចេះតែ បន្តលេខចែកនោះ តទៅទៀត ។ ដោយយើងបានសន្មតថា សំណល់ $b_5 = 0$ ទំនាក់ទំនង ខាងលើ ទៅជា

(1) $b_2 = b_0 - b_1 q_1$
(2) $b_3 = b_1 - b_2 q_2$
(3) $b_4 = b_2 - b_3 q_3$
(4) $0 = b_3 - b_4 q_4$

(4) => $b_3 = b_4 q_4$ => b_4 ជាតួចែក មួយ របស់ b_3 (5)

(3) => b_4 ជាតួចែក របស់ $(b_2 - b_3 q_3)$
តែដោយ b_4 ជាតួចែក មួយ របស់ b_3
ដូច្នេះ b_4 ជាតួចែក មួយ របស់ b_2 [1] (6)

ដោយ (5) និង (6) =>

b_4 ជាតួចែក មួយ របស់ b_2 និង b_3
ដូច្នេះដោយ (2)
b_4 ជាតួ ចែក មួយ របស់ b_1 (7)

ដោយ (6) និង (7) =>

b_4 ជាតួចែក មួយ របស់ b_2 និង b_1
ដូច្នេះដោយ (1)
b_4 ជាតួ ចែក មួយ របស់ b_0 (8) ។

រួមសេចក្តីទៅ បើ សំណល់ $b_5 = 0$ នោះ b_4 ជាតួចែក រួម នៃ b_0 និង b_1 ហើយ b_4 ក៏ជាតួចែក រួម នៃ (b_1,b_2), (b_2,b_3), (b_3,b_4) ដែរ ។ ហើយ ដោយ ក្នុង (b_3,b_4) b_4 ជាតួចែករួម ធំ ជាងគេ ក្នុងចំណោម តួចែករួម ឯទៀតៗ ដូច្នេះ យើងបាន P.G.C.D. ដោយប្រើ ក្បួនដោះស្រាយ អឺក្លីត នេះ។

[1] b_4 ជាតួចែករបស់ b_3 => $b_3 = k.b_4$ ហើយ b_4 ជាតួចែក របស់ $(b_2 - b_3 q_3)$ =>
$(b_2 - b_3 q_3) = h.b_4$ => $b_2 = h.b_4 + b_3 q_3 = h.b_4 + k.b_4.q_3 = b_4(h + k.q_3)$ ។

<u>ឧបមា យើងរក $\text{P.G.C.D}(156,84)$</u>

ដោយធ្វើលេខចែក ជម្មតា តៗគ្នា យើងបាន ៖

$156 = 84 \times 1 + 72$ (72 សំណល់)

$84 = 72 \times 1 + 12$ (12 សំណល់)

$72 = 12 \times 6$ (0 សំណល់)

នៅក្នុងនេះ ៖

$b_0 = 156\,;\ b_1 = 84\,;\ b_2 = 72\,;\ b_3 = 12\,;\ b_4 = 0$

ដូច្នេះ $\text{P.G.C.D}(156,84) = 12$ ហើយ 12 ចែកនឹង b_0, b_1, b_2, b_3 ដាច់ទាំងអស់ ។ ដោយ

12 = 4 x 3 = 2 x 2 x 3 ដូច្នេះ ចំនួន 2, 3, 4, 12 ក៏ជា តួចែករួម ដែរ ។

<u>បន្ថែម</u>

ដោយសម័យនេះ ជាសម័យ computer ពត៌មានវិជ្ជា យើងអាចប្រើ ម៉ាស៊ីន ឲ្យគណនា។

ដូច្នេះ ក្បួនដោះស្រាយ អឺគ្លីត អាចសរសេរ ដូចជា៖

<u>រក PGCD(a,b) ដោយ $a > b$</u>

<u>1/សេចក្តីផ្តើម</u>

$$\boldsymbol{A = a}$$
$$\boldsymbol{B = b}$$
$$\boldsymbol{R1 = B}$$

<u>2/ ការគណនា</u>

BOUCLE:

$\boldsymbol{R = A - INT(A/B) \times B}$ ដោយ $INT(A/B)$ គឺចំនួនគត់ បានមកពី

ការចែក A ដោយ B (partie entière de A/B)

បើ $\boldsymbol{R = 0}$ ទៅ ***FIN***

$$\boldsymbol{R1 = R}$$
$$\boldsymbol{A = B}$$
$$\boldsymbol{B = R}$$

ទៅ ***BOUCLE***

FIN :

$\boldsymbol{PGCD \ = R1}$ (ចប់តែប៉ុណ្ណេះ) ។

(ចំពោះ **programme** នេះ បើមានខុសសូមជួយ កែរផង)

<u>*B-ឧទាហរណ៍ទី២*</u> ស្តីពី ទ្រឹស្តីបទ បឺហ្សូត (Théorème de Bezout)

ដែលចែងថា មាន ចំនួន x និង y ដែលឲ្យ $\mathrm{PGCD(a,b) = ax \ - by}$

យើងយក ចំនួន a និង b និងការសន្មត $b_5 = 0$ ដូចគ្នានឹង ឧទាហរណ៍ទី១

ដូច្នេះ $b_4 = PGCD(a, b)$ ហើយយើងបាន៖

(1) $b_2 = b_0 - b_1q_1$

(2) $b_3 = b_1 - b_2q_2$

(3) $b_4 = b_2 - b_3q_3$

ដូច្នេះ ៖

$$b_4 = b_2 - b_3q_3 = (b_0 - b_1q_1) - (b_1 - b_2q_2)q_3 = (b_0 - b_1q_1) - b_1q_3 + b_2q_2q_3$$

$$b_4 = b_0 - b_1q_1 - b_1q_3 + (b_0 - b_1q_1)\, q_2q_3$$

$$b_4 = b_0\,(1 + q_2q_3) - b_1(q_1 + q_3 + q_1q_2q_3)$$

ដូច្នេះ យើងបាន ៖

$\mathrm{PGCD(a,b) = ax \ - by}$ ដោយ $\mathrm{a = b_0}$; $\mathrm{b = b_1}$; $\mathrm{x} = 1 + q_2q_3$ និង

$y = q_1 + q_3 + q_1q_2q_3$ ។

<u>***C – ឧទាហរណ៍ទី៣***</u> រីឡាស្យុង លំដាប់លើផ្នែក (Relation d'ordre partiel)

យើងធ្លាប់ឃើញ រីឡាស្យុង លំដាប់ (*Relation d'ordre*) លើសំនុំ។ ឥឡូវនេះ

យើងនឹងឃើញ រីឡាស្យុង លំដាប់លើផ្នែក(*Relation d'ordre partiel*) ដែល ជា

រីឡាស្យុង លំដាប់ លើ ផ្នែកមួយនៃសំនុំ ។ ឧទាហរណ៍ ៖

រីឡាស្យុង « *a* ចែកនឹង *b* ដាច់ » សរសេរកាត់ជា « *a / b* " នោះ ជា រីឡាស្យុង

លំដាប់លើផ្នែក ពីព្រោះ ៖

1/ « *a / a* " ត្រូវ ពីព្រោះ « *a* ចែកនឹង *a* ដាច់ » ត្រូវ ដូច្នេះ រីឡាស្យុងរ៉េផ្លិចស៊ីវ ។

2/ « a / b » និង « b / a " => $a = b$ ត្រូវ ពីព្រោះ

« a / b » => $a = bq$ ⎫ $a = (aq')q = = aqq'$ => $qq' = 1$ ដូច្នេះ $q = q' = 1$

« b / a " => $b = aq'$ ⎭ ដោយ $a = bq$ ហើយ $q = 1$ ដូច្នេះ $a = b$ ហើយ

ទំនាក់ទំនង ប្រឆាំងធ្លុះ (*antisymétrique*).

3/ « a / b » និង « b / c " => « a / c » ត្រូវ ពីព្រោះ

« a / b » => $a = kb$ ⎫ $a = k(lc) = (kl)c$

« b / c " => $b = lc$ ⎭ $a = klc$ ⇔ « a / c » ដូច្នេះ ទំនាក់ទំនង ត្រង់ស៊ីទីវ

(*transitive*).

ដូច្នេះ « a ចែកនឹង b ដាច់ » ជាទំនាក់ទំនង លំដាប់ តែ ដោយ មានចំនួន គត់ ខ្លះ ដូចជា 2 និង 3 ដែល ចែកនឹងគ្នាមិនដាច់ នោះ ទំនាក់ទំនង « a ចែកនឹង b ដាច់ » ជា ទំនាក់ទំនង លំដាប់លើផ្នែក នៃសំនុំ N^* (*Relation d'ordre partiel sur* N^*) ។

<u>សង្កេត</u>

ពាក្យថាលំដាប់ គឺបានន័យថា វត្ថុពីរ ជាទូទៅនៅក្នុងសំនុំ អាចប្រៀបធៀបនឹងគ្នាបាន <u>ជានិច្ច</u> ។ ដូចជា a និង b អាចប្រៀបធៀបនឹងគ្នាបានជានិច្ច ចំពោះ ទំនាក់ទំនង « $\leq$ » តែពុំអាច អាចប្រៀបធៀបនឹងគ្នាបាន ជានិច្ចទេ ចំពោះ ទំនាក់ទំនង « a / b » ។

<u>***D* – ឧទាហរណ៍ទី៤**</u>

ដោយ ទំនាក់ទំនង « a ចែកនឹង b ដាច់ » ត្រង់ស៊ីទីវ គឺថា ៖

« a ចែកនឹង b ដាច់ » និង « b ចែកនឹង c ដាច់ » => « a ចែកនឹង c ដាច់ »

បានន័យថា a ចែកនឹង a, b, c ដាច់ ហើយ យើងអាចនិយាយ អំពី ***P.G.C.D.***

នៃ $\boldsymbol{n}$ ចំនួន $\boldsymbol{a_i}$ គឺ ជាចំនួនដែល ធំជាងគេ ក្នុងបណ្តាល ចំនួនដែល តូចជាង ចំនួន $(a_1, a_2, \dots., a_n)$ ។