លឹម ផល្គុន និង សែន ពិសិដ្ឋ
បរិញ្ញាបត្រផ្នែកគណិតវិទ្យា

សិក្សាគណិតវិទ្យាដោយខ្លួនឯង

ទ្រឹស្ដីចំនួន

Number Theory

សម្រាប់ថ្នាក់ទី ១២

សិស្សពូកែ និង អាហារូបករណ៍

$$x^2 - d.y^2 = 1$$

1234567890

គណៈកម្មការនិពន្ធនិងរៀបរៀង

លោក លឹម ផល្គុន និង លោក សែន ពិសិដ្ឋ

គណៈកម្មការត្រួតពិនិត្យ

លោក លឹម ឆុន លោក អ៊ឹង សំណាង
លោក ឱត្យ ម៉េង អ្នកស្រី ឌុយ រីណា
លោក ព្រឹម សុនិត្យ លោក ផល ម៉ុនឆាយ
លោក លោក នន់ សុខណា

អ្នកត្រួតពិនិត្យអក្ខរាវិរុទ្ធ

លោក លឹម មិគ្គសិរ

ការីកុំព្យូទ័រ
កញ្ញា លី គុណ្ណាកា

អ្នករចនាក្រប
លោក លឹម ផល្គុន

អារម្ភកថា

សៀវភៅ **ទ្រឹស្តីចំនួន** ដែលអ្នកសិក្សាកំពុងកាន់នៅក្នុងដៃនេះ ខ្ញុំបាទបានរៀបរៀងឡើងក្នុងគោលបំនងទុកជាឯកសារ សម្រាប់ជាជំនួយដល់អ្នកសិក្សាយកទៅសិក្សាស្រាវជ្រាវដោយខ្លួនឯង និង ម្យ៉ាងទៀតក្នុងគោលបំនងចូលរួមលើកស្ទួយវិស័យគណិតវិទ្យានៅប្រទេសកម្ពុជាយើងឲ្យកាន់តែរីកចម្រើនថែមទៀតដើម្បីបង្កើនធនធានមនុស្សឲ្យមានកាន់តែច្រើនដើម្បីជួយអភិវឌ្ឍន៍ប្រទេសជាតិរបស់យើង ។

នៅក្នុងសៀវនេះរួមមាន មេរៀនសង្ខេប លំហាតគំរូ និង លំហាត់អនុវត្តន៍សម្រាប់អ្នកសិក្សាគិតដោយខ្លួនឯង ។
កំហុសឆ្គងដោយអចេតនាប្រាកដជាមានទាំងបច្ចេកទេស និង អក្ខរាវិរុទ្ធ ។ អាស្រ័យហេតុនេះ យើងខ្ញុំជាអ្នករៀបរៀងរង់ចាំដោយរីករាយជានិច្ចនូវមតិរិះគន់បែបស្ថាបនាពីសំណាក់អ្នកសិក្សាក្នុងគ្រប់មជ្ឈដ្ឋានដើម្បីជួយកែលំអ សៀវភៅនេះឲ្យបានកាន់តែសុក្រិត្រភាពថែមទៀត ។

ជាទីបញ្ចប់នេះយើងខ្ញុំអ្នករៀបរៀងសូមគោរពជូនពរដល់អ្នកសិក្សាទាំងអស់ឲ្យមានសុខភាពមាំមួន និង ទទួលជ័យជំនះគ្រប់ភារកិច្ច ។

បាត់ដំបងថ្ងៃទី ២៤ មីនា ២០១១

អ្នកនិពន្ធ លឹម ផល្គុន

Tel : 017 768 246

លឹម ផល្គុន និង សែន ពិសិដ្ឋ

សិក្សាគណិតវិទ្យាដោយខ្លួនឯង

ទ្រឹស្តីចំនួន

លក្ខណៈគ្រឹះនៃទ្រឹស្តីចំនួន

I. ភាពចែកដាច់ក្នុង $\mathbb{Z}$

1. សំណុំចំនួនគត់រឺឡាទីហ្វ

គេតាង $\mathbb{Z}$ ជាសំណុំនៃចំនួនគត់រឺឡាទីហ្វដែល :

$$\mathbb{Z}=\{\ .....-3,-2,-1,0\ ,1,\ 2\ ,\ 3\ ,\ .....\ \}$$

2. និយមន័យ

ឧបមាថា $\mathbf{a}$ និង $\mathbf{b}$ ជាចំនួនគត់រឺឡាទីហ្វ ។ បើ $\mathbf{a}=\mathbf{bq}$ ដែល $\mathbf{q}$ ជាចំនួនគត់រឺឡាទីហ្វនោះគេថា $\mathbf{a}$ ជាពហុគុណនៃ $\mathbf{b}$ ឬ គេថា $\mathbf{b}$ ជាតួចែកនៃ $\mathbf{a}$

ឬ គេថា $\mathbf{b}$ ចែកដាច់ $\mathbf{a}$ ។

គេកំណត់សរសេរ $\mathbf{b}\,|\,\mathbf{a}$ អានថា $\mathbf{b}$ ចែកដាច់ $\mathbf{a}$ ។

3. លក្ខណៈភាពចែកដាច់

តាង $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ ជាចំនួនគត់រឺឡាទីហ្វ ។ គេមានលក្ខណៈគ្រឹះដូចខាងក្រោម :

ក. $\mathbf{a}\,|\,\mathbf{a}$

ខ. បើ $\mathbf{b}\,|\,\mathbf{a}$ និង $\mathbf{a}\,|\,\mathbf{c}$ នោះ $\mathbf{b}\,|\,\mathbf{c}$

គ. បើ $\mathbf{b}\,|\,\mathbf{a}$ និង $\mathbf{a}\neq \mathbf{0}$ នោះ $|\,\mathbf{a}\,|\geq|\,\mathbf{b}\,|$

ឃ. បើ $\mathbf{b}\,|\,\mathbf{a}$ និង $\mathbf{b}\,|\,\mathbf{c}$ នោះ $\mathbf{b}\,|\,\mathbf{a}\alpha+\mathbf{c}\beta$ គ្រប់ចំនួនគត់រឺឡាទីហ្វ α,β ។

ង. បើ $\mathbf{b}\,|\,\mathbf{a}$ និង $\mathbf{b}\,|\,\mathbf{a}\pm\mathbf{c}$ នោះ $\mathbf{b}\,|\,\mathbf{c}$ ។

ច. បើ $\mathbf{b}\,|\,\mathbf{a}$ និង $\mathbf{a}\,|\,\mathbf{b}$ នោះ $|\,\mathbf{a}\,|=|\,\mathbf{b}\,|$

ឆ. បើ $b|a$ និង $a\neq 0$ នោះ $\frac{a}{b}|a$

ជ. ចំពោះ $c\neq 0$, $b|a$ លុះត្រាតែ $bc|ac$ ។

សម្រាយបញ្ជាក់

ក. $a|a$

យើងសម្គាល់ឃើញថា $a=1\times a$ ដូចនេះ $a|a$ ។

ខ. បើ $b|a$ និង $a|c$ នោះ $b|c$

បើ $b|a$ និង $a|c$ នាំឱ្យមាន $q_1,q_2\in Z$ ដែល $a=bq_1$ និង $c=aq_2$

គេទាញបាន $c=bq_1q_2$ ដូចនេះ $b|c$ ។

គ. បើ $b|a$ និង $a\neq 0$ នោះ $|a|\geq|b|$

បើ $b|a$ នាំឱ្យមាន $q\in Z$ ដែល $a=bq$ ហើយដោយសារតែ $a\neq 0$

នោះ $|q|\geq 1$ ហេតុនេះ $|a|=|q|.|b|\geq|b|$ ។

ឃ. បើ $b|a$ និង $b|c$ នោះ $b|a\alpha+c\beta$ គ្រប់ចំនួនគត់រ៉ឺឡាទីហ្វ α,β

បើ $b|a$ និង $a|c$ នាំឱ្យមាន $q_1,q_2\in Z$ ដែល $a=bq_1$ និង $c=bq_2$

គ្រប់ចំនួនគត់រ៉ឺឡាទីហ្វ α,β គេបាន $a\alpha+c\beta=(\alpha q_1+\beta q_2)b$

ដូចនេះ $b|a\alpha+c\beta$ ។

ង. បើ $b|a$ និង $b|a\pm c$ នោះ $b|c$

គេមាន $b|a$ និង $b|a\pm c$ នាំឱ្យមាន $q_1,q_2\in Z$ ដែល $a=bq_1$

និង $a\pm c=bq_2$ នោះគេទាញបាន $\pm c=bq_2-a=(q_2-q_1)b$

ដូចនេះ $b|c$ ។

ច. បើ $b|a$ និង $a|b$ នោះ $|a|=|b|$

បើ $b|a$ នោះ $|a|\geq|b|$ និង $a|b$ នោះ $|b|\geq|a|$ គ្រប់ $a,b\neq 0$

ដូចនេះ $|a|=|b|$ ។

ឆ. បើ $b|a$ និង $a\neq 0$ នោះ $\frac{a}{b}|a$

ដោយ $b|a$ នាំឱ្យ $a=bq$; $(q\in Z , q\neq 0)$ ឬ $\frac{a}{b}=q$

ដូចនេះ $q|a$ ឬ $\frac{a}{b}|a$ ។

ជ. ចំពោះ $c\neq 0$, $b|a$ លុះត្រាតែ $bc|ac$

ដោយ $c\neq 0$, $a\neq 0$ សមមូល $ac\neq 0$ ។

ដោយ $b|a$ នាំឱ្យ $a=bq$; $(q\in Z , q\neq 0)$

សមមូល $ac=bcq$

សមមូល $bc|ac$ ។

4. ចំនួនគត់គូ-ចំនួនគត់សេស និង លក្ខណៈ

ក. ចំនួនគត់គូមួយមានរាង $2k$ គ្រប់ចំនួនគតរឺឡាទីហ្វ k ។

ខ. ចំនួនគត់សេសមួយមានរាង $2k+1$ គ្រប់ចំនួនគតរឺឡាទីហ្វ k ។

គ. ផលបូករវាងពីចំនួនចំនួនគត់សេស ជាចំនួនគត់គូ ។

ឃ. ផលបូករវាងពីរចំនួនគត់គូ ជាចំនួនគត់គូ ។

ង. ផលបូករវាងចំនួនគត់គូ នឹង ចំនួនគត់សេស ជាចំនួនគត់សេស ។

ច. ផលគុណរវាងពីរចំនួនគត់សេស ជាចំនួនគត់សេស ។

ឆ. ផលគុណរវាងពីរចំនួនគត់ជាចំនួនគូ លុះត្រាតែមានចំនួនគត់មួយយ៉ាងតិចជា ចំនួនគូ ។

៥. លក្ខណៈចែកដាច់នឹងមួយចំនួន

ក. មួយចំនួនចែកដាច់នឹង **2** លុះត្រាតែលេខខ្ទង់រាយនៃចំនួននោះចែកដាច់នឹង **2** បានន័យថាចំនួននោះត្រូវមានលេខចុងក្រោយជាលេខគូ $\{0 , 2 , 4 , 6 , 8\}$ ។

ឧទាហរណ៍ : ចំនួន **714593168** ចែកដាច់នឹង **2** ព្រោះលេខខ្ទង់រាយ **8** ចែកដាច់នឹង **2** ។

ខ. មួយចំនួនចែកដាច់នឹង **3** លុះត្រាតែផលបូកនៃគ្រប់លេខខ្ទង់រាយនៃចំនួននោះ ចែកដាច់នឹង **3** ។

ឧទាហរណ៍ : ចំនួន **97543215168** ចែកដាច់នឹង **3**

ព្រោះ $9+7+5+4+3+2+1+5+1+6+8=51=3\times 17$

ចែកដាច់នឹង **3** ។

គ. មួយចំនួនចែកដាច់នឹង **4** លុះត្រាតែចំនួនពីរខ្ទង់ខាងចុងនៃចំនួននោះចែកដាច់ នឹង **4** ។

ឧទាហរណ៍ : ចំនួន **77168245948** ចែកដាច់នឹង **4** ព្រោះវាមានលេខពីរខ្ទង់ ចុងក្រោយ $48=4\times 12$ ចែកដាច់នឹង **4** ។

ឃ. មួយចំនួនចែកដាច់នឹង **5** លុះត្រាតែលេខខ្ទង់ចុងក្រោយនៃចំនួននោះជាលេខ **0** ឬ **5** ។

ឧទាហរណ៍ : ចំនួន **168277695** ចែកដាច់នឹង **5** ព្រោះមានលេខ **5** ចុងក្រោយ

ង. មួយចំនួនចែកដាច់នឹង 25 លុះត្រាតែលេខពីរខ្ទង់ចុងក្រោយនៃចំនួននោះ ចែកដាច់នឹង 25 គឺ { 00 , 25 , 50 , 75 } ។

ឧទាហរណ៍ : ចំនួន **2137486475** ចែកដាច់នឹង **25** ព្រោះវាមានលេខពីរខ្ទង់ចុងក្រោយ **75** ចែកដាច់នឹង **25** ។

ច.មួយចំនួនចែកដាច់នឹង **9** លុះត្រាតែផលបូកនៃគ្រប់លេខខ្ទង់វាយនៃចំនួននោះ ចែកដាច់នឹង **9** ។

ឧទាហរណ៍ : ចំនួន **1682751681** ចែកដាច់នឹង **9**

ព្រោះ $1+6+8+2+7+5+1+6+8+1=45$ ចែកដាច់នឹង **9** ។

ឆ.មួយចំួនចែកដាច់នឹង **11** លុះត្រាតែផលដករវាងផលបូកលេខខ្ទង់សេស និង ផលបូកលេខខ្ទង់គូនៃចំនួននោះ(រាប់ពីស្តាំទៅឆ្វេង) ចែកដាច់នឹង **11** ។

ឧទាហរណ៍ : ចំនួន **2990108** ចែកដាច់នឹង **11**

ព្រោះ $(8+1+9+2)-(0+0+9)=11$ ចែកដាច់នឹង **11** ។

៦. ការេប្រាកដនៃចំនួនគត់វិជ្ជមាន

☞ ចំនួនគត់វិជ្ជមាន $1 , 4 , 9 , 16 , 25 , 36 , ..., n^2 ,....$ ហៅថាការេប្រាកដ នៃចំនួនគត់វិជ្ជមាន $1 , 2 , 3 , 4 , 5 , 6,....., n$ ។

☞ គ្រប់ចំនួនដែលជាការេប្រាកដមានរាងតែពីរគត់គឺ $4m$ ឬ $4m+1$ គ្រប់ចំនួនគត់វិជ្ជមាន m ។

ឧទាហរណ៍ : ការេប្រាកដនៃចំនួនគត់គូ $(2n)^2 = 4n^2$ មានរាង $4m$

ហើយការេប្រាកដនៃចំនួនគត់សេស $(2n+1)^2 = 4n(n+1)+1$

មានរាង $4m+1$ ។

☞ លេខខ្ទង់ចុងក្រោយបង្អស់នៃការេរបស់មួយចំនួនគត់គឺ $1, 4, 5, 6, 9$ ឬ 0 ។

ឧទាហរណ៍ : ចំនួន 27945672168 មិនមែនជាការេប្រាកដនៃចំនួនគត់មួយទេ ព្រោះវាមានលេខចុងក្រោយ 8 ។

ជាទូទៅគ្រប់ចំនួនគត់ដែលមានលេខខ្ទង់ចុងក្រោយជាលេខ $2,3,7,8$ មិនមែនជាការេប្រាកដនៃមួយចំនួនគត់ទេ ។

សម្គាល់ :

ការេនៃគ្រប់ចំនួនគត់អាចមានលេខចុងក្រោយ $1, 4, 5, 6, 9$ ឬ 0

ប៉ុន្តែគ្រប់ចំនួនគត់ដែលមានលេខចុងក្រោយ $1, 4, 5, 6, 9$ ឬ 0 មិនសុទ្ធតែជាការេប្រាកដនៃមួយចំនួនគត់ទេ ។

II. វិធីចែកបែបអឺក្លីតក្នុង IN

1. ទ្រឹស្តីបទ

ឧបមាថា a និង b ជាពីរចំនួនគត់វិជ្ជមាន និង b ខុសពីសូន្យ នោះមានគូ (q,r) នៃចំនួនគត់វិជ្ជមានតែមួយគត់ដែល $a = bq + r$ និង $0 \le r < b$ ។

សម្រាយបញ្ជាក់

ដើម្បីបង្ហាញអត្ថិភាពនៃ (q,r) យើងនឹងសិក្សាបីករណីដូចខាងក្រោម :

☞ ក្នុងករណីនេះយើងសន្មតថា $a < b$

យើងអាចយក $q = 0$ និង $r = a < b$ នោះគេបាន $(q,r) = (0,a)$ ។

☞ ក្នុងករណីនេះយើងសន្មតថា $a = b$

យើងអាចយក $q=1$ និង $r=0<b$ នោះគេបាន $(q,r)=(1,0)$ ។

☞ ក្នុងករណីចុងក្រោយនេះយើងសន្មតថា $a>b$

មានចំនួនចំនួនគត់វិជ្ជមាន n ដែល $a<nb$ ។ យក q ជាចំនួនគត់វិជ្ជមានយ៉ាង

តិចដែល $(q+1)b>a$ នោះ $qb\le a$ ។

យក $r=a-bq$ នោះ $a=bq+r$ និង $0\le r<b$

សរុបទាំងបីករណីខាងលើនេះយើងអាចសន្និដ្ឋានថា ចំពោះ a និង b ជាពីរចំនួនគត់

វិជ្ជមាន និង b ខុសពីសូន្យ នោះមានគូ (q,r) នៃចំនួនគត់វិជ្ជមានដែល

$a=bq+r$ និង $0\le r<b$ ។

ជាបន្តទៅទៀតនេះយើងនឹងបង្ហាញភាពមានតែមួយគត់នៃគូ (q,r)

នៃចំនួនគត់វិជ្ជមានដែល $a=bq+r$ និង $0\le r<b$ ។

ឧបមាថា $a=bq'+r'$ ដែល (q',r') ជាគូនៃចំនួនគត់វិជ្ជមានផ្ទៀងផ្ទាត់

$0\le r'<b$ ។ ដោយ $a=bq+r$ នោះគេបាន $bq'+r'=bq+r$

គេទាញបាន $r-r'=(q'-q)b$ នោះ $b\,|\,r-r'$

ហេតុនេះ $|r-r'|\ge b$ ឬ $|r-r'|=0$ ព្រោះ $0\le r<b$ និង $0\le r'<b$

នោះ $-b<r-r'<b$ ឬ $|r-r'|<b$ ។

ដូចនេះ $|r-r'|=0$ នាំឱ្យ $r=r'$ ហើយ $q=q'$ ។

2. និយមន័យ

ធ្វើវិធីចែកបែបអឺគ្លីតក្នុងសំណុំ $\mathbb{N}$ នៃចំនួនគត់វិជ្ជមាន a នឹងចំនួនគត់វិជ្ជមាន b ដែល $b \neq 0$ គឺរកគូនៃចំនួនគត់វិជ្ជមាន(q,r) ដែល $a = bq + r$ និង $0 \leq r < b$ ចំនួនគត់ q ហៅថាផលចែកនៃវិធីចែកនេះ ហើយ r ហៅថាសំណល់ ។ b ហៅថាតួចែក និង a ហៅថាតំណាងចែក ។

សម្គាល់

☞ បើ $0 \leq a < b$ នោះ $q = 0\,;\ r = a$

☞ បើ $r = 0$ នោះ $a = bq$ ក្នុងករណីនេះ a ជាពហុគុណនៃ b ឬ b ចែកដាច់ a ហើយ q ជាផលចែកប្រាកដនៃ a និង b ។

ឧទាហរណ៍១: គេឱ្យ n ជាចំនួនគត់វិជ្ជមាន ។ គេដឹងថា n ចែកនឹង 5 ឱ្យសំណល់ 3 ។ បើគេចែកចំនួន n នោះនឹង 7 ឱ្យសំណល់ 2 ។

ក. រកសំណល់នៃវិធីចែកបែបអឺគ្លីតរវាង n នឹង 35

ខ. កំណត់ចំនួន n បើគេដឹងថា $70432 < n < 70456$ ។

ដំណោះស្រាយ

ក. រកសំណល់នៃវិធីចែកបែបអឺគ្លីតរវាង n នឹង 35

គេដឹងថា n ចែកនឹង 5 ឱ្យសំណល់ 3 នាំឱ្យមាន $q_1 \geq 0$ ដែល $n = 5q_1 + 3$

ហើយដោយគេចែកចំនួន n នោះនឹង 7 ឱ្យសំណល់ 2 នាំឱ្យមាន $q_2 \geq 0$

ដែល $n = 7q_2 + 2$ ។

គេបានប្រព័ន្ធ $\begin{cases} n = 5q_1 + 3 \\ n = 7q_2 + 2 \end{cases}$ ឬ $\begin{cases} 21n = 105q_1 + 63 \\ 20n = 140q_2 + 40 \end{cases}$

គេទាញ $21n - 20n = (105q_1 + 63) - (140q_2 + 40)$

$n = (3q_1 - 4q_2) \times 35 + 23$ តាង $q = 3q_1 - 4q_2 \geq 0$

គេបាន $n = 35q + 23$ ។

ដូចនេះសំណល់នៃវិធីចែកបែបអឺគ្លីតរវាង n នឹង 35 គឺ $r = 23$ ។

ខ. កំណត់ចំនួន n បើគេដឹងថា $70432 < n < 70456$

គេបាន $70432 < 35q + 23 < 70456$ នោះ $2011 + \frac{24}{35} < q < 2012 + \frac{13}{35}$

គេទាញបាន $q = 2012$ ហើយ $n = 35 \times 2012 + 23 = 70443$ ។

ឧទាហរណ៍២: ចូររកសំណល់នៃវិធីចែកបែបអឺគ្លីត រវាងចំនួន 2^{2012} និង 7

គេមាន $2^3 = 7 + 1$ នោះ $2^{2010} = (7+1)^{670}$

តាមរូបមន្តទ្វេធាញូតុន

$$(x+y)^n = C(n,0)x^n + C(n,1)x^{n-1}y + C(n,2)x^{n-2}y^2 + ... + C(n,n)y^n$$

យក $x = 7$, $y = 1$ និង $n = 670$

គេបាន $2^{2010} = (7+1)^{670} = 7q + 1$ ដែល q ជាចំនួនគត់វិជ្ជមានមួយ ។

គុណអង្គទាំងពីរនឹង $2^2 = 4$ គេបាន $2^{2012} = 7(4q) + 4$ ។

ដូចនេះ សំណល់នៃវិធីចែកបែបអឺគ្លីត រវាងចំនួន 2^{2012} និង 7 គឺ $r = 4$ ។

ឧទាហរណ៍៣: គេឱ្យចំនួនគត់វិជ្ជមាន $\mathbf{m}$ និង $\mathbf{n}$ ។

គេដឹងថា $\mathbf{m}$ ចែកនឹង $\mathbf{7}$ ឱ្យសំណល់ $\mathbf{2}$ ហើយ $\mathbf{n}$ ចែកនឹង $\mathbf{7}$ ឱ្យសំណល់ $\mathbf{3}$ ។

ក. រកសំណល់នៃវិធីចែករវាង $\mathbf{m^2+n^2}$ នឹង $\mathbf{7}$

ខ. បង្ហាញថា $\mathbf{7}$ ចែកដាច់ $\mathbf{m^3+n^3}$ ។

ដំណោះស្រាយ

ក. រកសំណល់នៃវិធីចែករវាង $\mathbf{m^2+n^2}$ នឹង $\mathbf{7}$

តាមបម្រាប់ $\mathbf{m}$ ចែកនឹង $\mathbf{7}$ ឱ្យសំណល់ $\mathbf{2}$ ហើយ $\mathbf{n}$ ចែកនឹង $\mathbf{7}$ ឱ្យសំណល់ $\mathbf{3}$

នាំឱ្យមានចំនួនគត់វិជ្ជមាន $\mathbf{q_1}$ និង $\mathbf{q_2}$ ដែល $\mathbf{m=7q_1+2}$ និង $\mathbf{n=7q_2+3}$

គេបាន $\mathbf{m^2+n^2=(7q_1+2)^2+(7q_2+3)^2}$

$$\mathbf{=7[7(q_1{}^2+q_2{}^2)+2(2q_1+3q_2)+1]+6}$$

ដូចនេះ សំណល់នៃវិធីចែករវាង $\mathbf{m^2+n^2}$ នឹង $\mathbf{7}$ គឺ $\mathbf{r=6}$ ។

ខ. បង្ហាញថា $\mathbf{7}$ ចែកដាច់ $\mathbf{m^3+n^3}$

តាមរូបមន្តទ្វេធាញូតុនគេមាន :

$$\mathbf{(bq+r)^n=\sum_{k=0}^{n}C(n,k)(bq)^{n-k}r^k=b\sum_{k=0}^{n-1}[C(n,k)b^{n-k-1}q^{n-k}r^k]+r^n}$$

ឬ $\mathbf{(bq+r)^n=bq_n+r^n}$ ដែល $\mathbf{q_n=\sum_{k=0}^{n-1}[C(n,k)b^{n-k-1}q^{n-k}r^k]}$

តាមសមភាពខាងលើនេះគេអាចសរសេរ :

$\mathbf{m^3=(7q_1+2)^3=7q_1'+2^3=7(q_1'+1)+1}$ ដែល $\mathbf{q_1'\in IN}$

$\mathbf{n^3=(7q_1+3)^3=7q_2'+3^3=7(q_2'+3)+6}$ ដែល $\mathbf{q_2'\in IN}$

គេបាន $m^3+n^3=7(q_1'+q_2'+4)+7=7(q_1'+q_2'+5)$

ដូចនេះ $7\,|\,m^3+n^3$ ។

ឧទាហរណ៍៤: គេឱ្យចំនួនគត់វិជ្ជមាន x , y និង z ។

គេដឹងថា x , y និង z ចែកនឹង 216 ឱ្យសំណល់រៀងគ្នា 3 , 4 និង 5 ។

កំណត់តម្លៃតូចជាងគេមួយនៃ n ដើម្បីឱ្យ $x^n+y^n+z^n$ ចែកដាច់នឹង 216 ។

តាមវិធីចែកបែបអឺគ្លីតបើ x , y និង z ចែកនឹង 216 ឱ្យសំណល់រៀងគ្នា 3 , 4 និង 5

នោះគេមាន $q_1, q_2, q_3 \in IN$ ដែល $x=216q_1+3$, $y=216q_2+4$

និង $z=216q_3+5$ ។ តាមទ្វេធាញូតុនគេអាចសរសេរ :

$x^n+y^n+z^n=216q_n+3^n+4^n+5^n$ ។

បើ $n=3$ នោះ $3^n+4^n+5^n=3^3+4^3+5^3=6^3=216$ ។

ដូចនេះតម្លៃតូចជាងគេនៃ n ដែល $216\,|\,x^n+y^n+z^n$ គឺ $n=3$ ។

III.វិធីចែកបែបអឺគ្លីតក្នុង $\mathbb{Z}$

ទ្រឹស្តីបទ

a និង b ជាពីរចំនួនគត់រ៉ឺឡាទីហ្វ និង b ខុសពីសូន្យ នោះវាមានចំនួនគត់រ៉ឺឡាទីហ្វ q តែមួយគត់ និង ចំនួនគត់រ៉ឺឡាទីហ្វ r តែមួយគត់ដែល $a=bq+r$ និង $0\le r<|b|$ ។

សម្រាយទ្រឹស្តីបទនេះទាញចេញពីសម្រាយទ្រឹស្តីបទវិធីចែកបែបអឺគ្លីតក្នុង IN រវាង $|a|$ និង $|b|$ ដែលយើងបានសិក្សារួចមកហើយ ។

ឧទាហរណ៍ ១ : ចូររកផលចែក និង សំណល់នៃវិធីចែកបែអឺគ្លីតរវាង 75 នឹង -11

គេមាន $75 = 11\times 6 + 9$ ឬ $75 = (-11)\times(-6) + 9$

ដូចនេះគេទាញផលចែក $q = -6$ និងសំណល់ $r = 9$ ។

ឧទាហរណ៍ ២ : ចូររកផលចែក និង សំណល់នៃវិធីចែកបែអឺគ្លីតរវាង -95 នឹង 7

គេមាន $95 = 7\times 13 + 4$

ឬ $-95 = 7\times(-13) - 4 = 7\times(-13) - 7 + 3 = 7\times(-14) + 3$

ដូចនេះគេទាញផលចែក $q = -14$ និងសំណល់ $r = 3$ ។

ឧទាហរណ៍ ៣ :

ចូររកផលចែក និង សំណល់នៃវិធីចែកបែអឺគ្លីតរវាង -61 នឹង -19 ។

គេមាន $61 = 19\times 3 + 4$

ឬ $-61 = -19\times 3 - 4 = -19\times 3 - 19 + 15 = -19\times 4 + 15$

ដូចនេះគេទាញផលចែក $q = 4$ និងសំណល់ $r = 15$ ។

IV~ចំនួនបឋម

1. *និយមន័យ*

☞ ចំនួនគត់ $p > 1$ ហៅថាចំនួនបឋមលុះត្រាតែគ្មានចំនួនគត់ d ដែល $d > 1$ និង $d \mid p$ ។

☞ បើ $p > 1$ ជាចំនួនបឋមនោះ p មានតួចែករួមតែពីរគត់គឺ 1 និង p ខ្លួនឯង ។ ក្នុងករណីផ្សេងពីនេះ គេហៅថាចំនួនមិនបឋម ។

ឧទាហរណ៍ $2 , 3 ,5,7 , 11 ,13 , 17,19,23,...$ ជាចំនួនបឋម ។

2. *ទ្រឹស្តីបទ*

គ្រប់ចំនួនគត់ $n>1$ មានតួចែកជាចំនួនបឋមយ៉ាងតិចមួយ ។

សម្រាយបញ្ជាក់

-បើ n ជាចំនួនបឋមនោះ n មានតួចែករួមពីរគឺ 1 និង n ខ្លួនឯង ។

-បើ n មិនមែនជាចំនួនបឋមនោះយ៉ាងតិចមាន $d>1$ ជាតួចែកតូចបំផុតនៃ n ដែល $n=bd$ និង $1<d\le b$ ។

សន្មតថា d មិនមែនជាចំនួនបឋមនោះ d មានតួចែក d_1 មួយទៀតដែល $d_1<d$ ហេតុនេះ $d_1\,|\,d$ និង $d\,|\,n$ នោះ $d_1\,|\,n$ ដែល $d_1<d$ នោះវាផ្ទុយពី d ដែលជាតួចែកតូចបំផុតនៃ n ។

ដូចនេះ d ជាតួចែកបឋមតូចបំផុតនៃ n ។

3. *ទ្រឹស្តីបទ*

គ្រប់ចំនួនគត់ $n>1$ មិនមែនជាចំនួនបឋមនោះមានចំនួនគត់ធម្មជាតិបឋម p ដែល $p\,|\,n$ និង $p^2\le n$ ។

សម្រាយបញ្ជាក់

បើ $n>1$ មិនមែនជាចំនួនបឋមនោះតាមទ្រឹស្តីបទខាងលើ n មានតួចែកជាចំនួនបឋមតូចជាងគេមួយដែលតាងដោយ p ។

គេបាន $n=pq$ ដែល $p\le q$ (ព្រោះ p ជាតួចែកតូចបំផុតនៃ n)

តាម $p\le q$ គេបាន $p^2\le pq=n$ ។

4. *ទ្រឹស្តីបទ*

គ្រប់ចំនួនគត់ $\mathbf{n > 1}$ ចែកមិនដាច់នឹងចំនួនបឋម $\mathbf{p}$ ដែល $\mathbf{p^2 \le n}$ នោះ $\mathbf{n}$ ជាចំនួនបឋម ។

សម្រាយបញ្ជាក់

ឧបមាថា $\mathbf{n > 1}$ ជាចំនួនគត់ធម្មជាតិមិនបឋម ។

តាមទ្រឹស្តីបទគេបាន $\mathbf{p \mid n}$ និង $\mathbf{p^2 \le n}$ ដែលផ្ទុយពីសម្មតិកម្មដែលថា $\mathbf{n}$ ចែកមិនដាច់នឹង $\mathbf{p}$ ។ ដូចនេះការដែលឧបមាថា $\mathbf{n}$ មិនមែនជាចំនួនបឋម មិនពិតទេ ។

ដូចនេះ $\mathbf{n}$ ជាចំនួនបឋម (ពិត) ។

ឧទាហរណ៍ ចូរស្រាយថា **1009** ជាចំនួនបឋម ?

បន្ទាប់ពីធ្វើវិធីចែកបែបអឺគ្លីតរវាងចំនួន **1009** ជាមួយចំនួនបឋម **2 , 3 , 5 , 7 , 11,13 , 19, 23, 29** និង **31** ឃើញថា **1009** ចែកមិនដាច់ជាមួយចំនួនបឋមទាំងនេះទេ ។ **31** ជាចំនួនបឋមធំជាងគេដែល $\mathbf{31^2 = 961 < 1009}$ ។

តាមទ្រឹស្តីបទខាងលើគេបាន **1009** ជាចំនួនបឋម ។

5. *ការបំបែកមួយចំនួនគត់ជាផលគុណកត្តាបឋម*

ក-អត្ថិភាព និង ភាពមានតែមួយគត់នៃការបំបែក

ទ្រឹស្តីបទ :

គ្រប់ចំនួនគត់ធម្មជាតិ $\mathbf{n > 1}$ មិនបឋមអាចបំបែកជាផលគុណកត្តាបឋមបាន ហើយបានតែមួយបែបគត់ ។

សម្រាយបញ្ជាក់

តាង $\mathbf{d}$ ជាតួចែកបឋមមួយនៃ $\mathbf{n}$ នោះគេបាន $\mathbf{n = dq}$ ដែល $\mathbf{q \in IN , q > 1}$

-បើ $\mathbf{q}$ ជាចំនួនបឋម នោះ $\mathbf{n}$ អាចសរសេរជាផលគុណនៃពីរកត្តាបឋមបាន ។

-បើ $\mathbf{q}$ មិនមែនជាចំនួនបឋមនោះ $\mathbf{q}$ អាចមានតួចែក $\mathbf{q_1}$ មួយដែល $\mathbf{q = q_1 q_2}$ និង $\mathbf{q_2 > 1}$ ។

បើ $\mathbf{q_2}$ មិនមែនជាចំនយនបឋមនោះ$\mathbf{q_2}$ អាចមានតួចែក $\mathbf{q_3}$ មួយដែល $\mathbf{q_2 = q_3 q_4}$ និង $\mathbf{q_4 > 1}$ ។

តាមលំនាំដដែលៗនេះគេអាចបង្កើតស្វ៊ីតនៃផលចែក $\mathbf{q, q_1, q_2, q_3, \ldots}$ ជាស្វ៊ីតចុះដែលមានតួចុងក្រោយជាចំនួនបឋម ។

តាង $\mathbf{p_1 , p_2 , p_3 , \ldots, p_k}$ ជាស្វ៊ីតតួចែកបឋមនៃ $\mathbf{n}$ ដូចនេះគេងាចសរសេរចំនួនគត់ធម្មជាតិ $\mathbf{n}$ ជាទម្រង់ $\mathbf{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \ldots \times p_k^{\alpha_k}}$

$\mathbf{p_k}$ ជាចំនួនបឋម និង $\alpha_{\mathbf{k}}$ ជាចំនួនគត់ធម្មជាតិធំជាងសូន្យ ($\mathbf{k = 1, 2, 3\ldots}$) ។

ឧទាហរណ៍ : បំបែកចំនួន $\mathbf{777}$ និង $\mathbf{2002}$ ជាផលគុណកត្តាបឋម ។

គេបាន $\mathbf{777 = 3 \times 7 \times 37}$ និង $\mathbf{2002 = 2 \times 7 \times 11 \times 13}$ ។

ខ-លក្ខខណ្ឌចែកដាច់

ទ្រឹស្តីបទ : ឧបមាថា $\mathbf{n}$ និង $\mathbf{p}$ ជាចំនួនគត់ធម្មជាតិធំជាង $\mathbf{1}$ ។

ដើម្បីឱ្យ $\mathbf{p}$ ជាតួចែកមួយនៃ $\mathbf{n}$ លុះត្រាតែគ្រប់តួចែកបឋមនៃ $\mathbf{p}$ ជាតួចែកនៃ $\mathbf{n}$ និងនិទស្សន្តនៃតួចែកនីមួយៗនៃ $\mathbf{p}$ មិនធំជាងនិទស្សន្តនៃតួចែកដែលដូចរៀងគ្នារបស់ $\mathbf{n}$

សម្រាយបញ្ជាក់

តាង $\mathbf{n = p_1^{\alpha 1} \times p_2^{\alpha 2} \times p_3^{\alpha 3} \times .... \times p_k^{\alpha k}}$

$\mathbf{p_k}$ ជាចំនួនបឋម និង α_k ជាចំនួនគត់ធម្មជាតិធំជាងសូន្យ ($\mathbf{k = 1,2,3...}$) ។

បើ $\mathbf{p}$ ជាតួចែកមួយនៃ $\mathbf{n}$ នោះមាន $\mathbf{q \ge 1}$ ដែល $\mathbf{n = p.q}$ ។

ការបំបែក $\mathbf{p.q}$ ជាផលគុណនៃកត្តាបឋមដូចគ្នានឹងការបំបែក $\mathbf{n}$ ជាកត្តាបឋមដែរ ។

ដូចនេះ $\mathbf{p}$ មិនអាចមានកត្តាបឋមផ្សេងទៀតក្រៅពី $\mathbf{p_1 , p_2 , p_3 , ..., p_k}$ ទេ ។

គេអាចយក $\mathbf{p = p_1^{\beta 1} \times p_2^{\beta 2} \times p_3^{\beta 3} \times .... \times p_k^{\beta k}}$ ដែល β_k ជាចំនួនគត់

ហើយ $\mathbf{0 \le \beta_k \le \alpha_k}$ និង $\mathbf{k = 1,2,3...}$ ។

គេមាន $\mathbf{n = p_1^{\alpha 1} \times p_2^{\alpha 2} \times p_3^{\alpha 3} \times .... \times p_k^{\alpha k} = \prod_{i=1}^{k} (p_i^{\alpha i})}$

$$\mathbf{n = \prod_{i=1}^{k} (p_i^{\alpha i - \beta i}) \times \prod_{i=1}^{k} (p_i^{\beta i}) = p \times \prod_{i=1}^{n} (p_i^{\alpha i - \beta i})}$$

ដូចនេះ $\mathbf{p}$ ជាតួចែកមួយនៃ $\mathbf{n}$ ។

គ-ចំនួននៃតួចែករបស់មួយចំនួន

តាង $\mathbf{n = p_1^{\alpha 1} \times p_2^{\alpha 2} \times p_3^{\alpha 3} \times .... \times p_k^{\alpha k}}$ ជាចំនួនគត់ធម្មជាតិមួយ

$\mathbf{p_k}$ ជាចំនួនបឋម និង α_k ជាចំនួនគត់ធម្មជាតិធំជាងសូន្យ ($\mathbf{k = 1,2,3...}$) ។

យើងបានដឹងរួចហើយថាបើ $\mathbf{p}$ ជាតួចែកមួយនៃ $\mathbf{n}$ នោះ $\mathbf{p}$ អាចសរសេរជាទូទៅ

$\mathbf{p = p_1^{\beta 1} \times p_2^{\beta 2} \times p_3^{\beta 3} \times .... \times p_k^{\beta k}}$ ដែល β_k ជាចំនួនគត់

ហើយ $\mathbf{0 \le \beta_k \le \alpha_k}$ និង $\mathbf{k = 1,2,3...}$ ។

ហេតុនេះតួចែកមួយនៃ $\mathbf{n}$ បានមកពីការជ្រើសរើស **Liste** មួយនៃ

$\beta_1, \beta_2, \beta_3, ...,\beta_k$ ដែលចំនួននីមួយៗនៃ β_k អាចយកពី $0, 1, 2, ..., \beta_k$ ។

ដូចនេះដោយផ្អែកលើគោលការណ៍រាប់គេអាចសន្និដ្ឋានថាចំនួនតួចែកនៃ n

កំណត់ដោយ $(\alpha_1 + 1)(\alpha_2 + 1).....(\alpha_k + 1)$ ។

ឧទាហរណ៍១ : ចូររកចំនួនតួចែកនៃ 31752 ?

គេមាន $31752 = 2^3 \times 3^4 \times 7^2$

ដូចនេះចំនួនតួចែកនៃ 31752 គឺ $(1+3)(1+4)(1+2) = 60$ ។

ឧទាហរណ៍២ : ចូរកំណត់ n ដើម្បីឱ្យចំនួនតួចែកនៃចំនួន $3^{2n+1}.4^n.7^{2n+2}$

ស្មើនឹង 1716 ។

គេមាន $3^{2n+1}.4^n.7^{2n+2} = 2^{2n+1}.2^{2n}.7^{2n+2}$ មានចំនួនតួចែកស្មើនឹង

$(2n+1)(2n+2)(2n+3) = 1716 = 11 \times 12 \times 13$

គេទាញបាន $n = 5$ ។

V~តួចែករួម និង ពហុគុណរួម

1. *តួចែករួមនៃពីរចំនួនគត់ធម្មជាតិ*

❀ និយមន័យ

គេយក a និង b ជាពីរចំនួនកត់ធម្មជាតិ ។ គេថា d ជាតួចែករួមនៃ a និង b កាលណា d ជាតួចែកនៃ a ផង និង ជាតួចែកនៃ b ផង ។

ឧទាហរណ៍ :

7 ជាតួចែករួមនៃ 42 និង 70 ព្រោះ $7 | 42$ និង $7 | 70$ ។

2. *តួចែករួមធំបំផុតនៃពីរចំនួនគត់ធម្មជាតិ*

❀ **និយមន័យ :**

គេយក **a** និង **b** ជាពីរចំនួនគត់ធម្មជាតិ ។

តួចែករួមធំបំផុតនៃ **a** និង **b** ជាចំនួនគត់ធម្មជាតិដែលធំជាងគេ ក្នុងចំណោមតួចែករួមនៃ **a** និង **b** ដែលកំណត់តាងដោយ $\delta = \mathbf{GCD(a,b)}$ ។

ឧទាហរណ៍ : រកតួចែករួមធំបំផុតនៃ **70** និង **84** ?

គេមាន $\mathbf{70 = 2\times 5\times 7}$ និង $\mathbf{84 = 2^2\times 3\times 7}$

ដូចនេះ $\delta = \mathbf{GCD(70,84) = 2\times 7 = 14}$ ។

3. *ចំនួនបឋមរវាងគ្នា*

❀ **និយមន័យ :**

ពីរចំនួនគត់ធម្មជាតិ **a** និង **b** ជាចំនួនបឋមរវាងគ្នាលុះត្រាតែ $\mathbf{GCD(a,a) = 1}$

ឧទាហរណ៍ : បង្ហាញថា **42** និង **55** ជាចំនួនបឋមរវាងគ្នា ?

គេមាន $\mathbf{42 = 2\times 3\times 7}$ និង $\mathbf{55 = 5\times 11}$ គេបាន $\mathbf{GCD(42,55) = 1}$ ។

ដូចនេះ **42** និង **55** ជាចំនួនបឋមរវាងគ្នា ។

4. *លក្ខណៈ និង ទ្រឹស្តីបទនៃតួចែករួមធំបំផុត*

គេយក **a** និង **b** ជាពីរចំនួនគត់ធម្មជាតិ ។

☞ បើ **a** ចែកដាច់នឹង **b** នោះ $\mathbf{GCD(a,b) = b}$ ។

☞ បើ **a** ចែកមិនដាច់នឹង **b** នោះមានគូ $\mathbf{(q,r)}$ នៃចំនួនគត់ធម្មជាតិតែមួយគត់

ដែល $\mathbf{a = bq + r}$ ឬ $\mathbf{r = a - bq}$ ។

តាង d ជាតួចែករួមមួយនៃ a និង b នោះ $a = dq_1$ និង $b = dq_2$

គេបាន $r = a - bq = dq_1 - qdq_2 = d.(q_1 - qq_2)$ ។

ដូចនេះគ្រប់តួចែករួមនៃ a និង b ជាតួចែកនៃសំណល់ r ។

ទ្រឹស្តីបទ :

បើ a និង b ជាចំនួនគត់ធម្មជាតិដែល $a = bq + r$ និង $0 \le r < b$

នោះគេបាន $GCD(a,b) = GCD(b,r)$ ។

សម្រាយបញ្ជាក់

តាង $\delta = GCD(a,b)$ នាំឱ្យមានចំនួនគត់ធម្មជាតិ x, y ដែល $a = \delta x$

និង $b = \delta y$ ហើយ $GCD(x,y) = 1$ ។

ដោយ $a = bq + r$ នោះ $r = a - bq = (x - qy).\delta$

ដោយ $GCD(x - qy, y) = 1$ នោះ $GCD(b,r) = \delta = GCD(a,b)$ ។

5. *អាល់កូរីតអឺគ្លីត (Algorithme d'Eclide)*

ឧបមាថា a និង b ជាចំនួនគត់ធម្មជាតិដែល $a = bq + r$ និង $0 \le r < b$

នោះគេបាន $GCD(a,b) = GCD(b,r)$

-បើ $r = 0$ នោះ $b \mid a$ នាំឱ្យ $GCD(a,b) = b$ ។

-បើ $r > 0$ និង $r \mid b$ នោះ $GCD(a,b) = GCD(b,r) = r$ ។

-បើ b ចែកមិនដាច់នឹង r នាំឱ្យមានគូ (q_1, r_1) ដែល $b = rq_1 + r_1$

គេបាន $GCD(a,b) = GCD(b,r) = GCD(r, r_1)$

-បើ r ចែកមិនដាច់នឹង r_1 នាំឱ្យមានគូ (q_2, r_2) ដែល $r = r_1q_2 + r_2$

គេបាន $\mathbf{GCD(a,b)=GCD(b,r)=GCD(r,r_1)=GCD(r_1,r_2)}$

តាមរបៀបដូចគ្នានេះគេបានលក្ខណៈទូទៅ :

$$\mathbf{GCD(a,b)=GCD(b,r)=GCD(r,r_1)=....=GCD(r_{k-1},r_k)}$$

បើ $\mathbf{r_k \mid r_{k-1}}$ នោះ $\mathbf{GCD(r_{k-1},r_k)=r_k}$ ។

ប្រតិបត្តិវិធីចែកបន្តបន្ទាប់បែបនេះហៅថា អាល់កូរីតអឺគ្លីត ។

ទ្រឹស្តីបទ :

GCD នៃចំនួនគត់ធម្មជាតិ **a** និង **b** គឺជាសំណល់ចុងក្រោយបំផុតខុសពីសូន្យក្នុងវិធីចែកបន្តបន្ទាប់គ្នា ឬ អាល់កូរីតអឺគ្លីត ។

សម្គាល់ : បើ $\mathbf{r_k = 1}$ នោះ **a** និង **b** ជាចំនួនបឋមរវាងគ្នា ។

ឧទាហរណ៍១ :

ដោយប្រើ អាល់កូរីតអឺគ្លីតចូររកតួចែកធំបំផុតនៃពីរចំនួន **18480** និង **13104**

គេមាន $\mathbf{18480 = 13104 \times 1 + 5376}$

$\mathbf{13104 = 2 \times 5376 + 2352}$

$\mathbf{5376 = 2 \times 2352 + 672}$

$\mathbf{2352 = 3 \times 672 + 336}$

$\mathbf{672 = 2 \times 336 + 0}$

ដូចនេះ $\mathbf{GCD(18480;13104)=336}$ ។

ឧទាហរណ៍២ :(**IMO 1959**)

ចូរស្រាយថា $\dfrac{21n+4}{14n+3}$ ជាប្រភាគសម្រួលមិនបានគ្រប់ចំនួនគត់ធម្មជាតិ n ។

តាមអាល់កូរីតអឺគ្លីតគេបាន :

$$21n+4=(14n+3)\times 1+(7n+1)$$

$$14n+3=(7n+1)\times 2+1$$

$$7n+1=(7n+1)\times 1+0$$

គេបាន $GCD(21n+4,14n+3)=1$

ហេតុនេះ $21n+4$ និង $14n+3$ ជាចំនួនបឋមរវាងគ្នាគ្រប់ ចំនួនគត់ធម្មជាតិ n ។

ដូចនេះ $\dfrac{21n+4}{14n+3}$ ជាប្រភាគសម្រួលមិនបាន ។

ទ្រឹស្តីបទ :

សំណុំតួចែករួមនៃពីរចំនួនគត់ធម្មជាតិ a និង b ស្មើនឹងសំណុំតួចែករួមធំបំផុតរបស់វា ។

សម្រាយបញ្ជាក់

តាមអាល់កូរីតអឺគ្លីតគេបាន :

$$GCD(a,b)=GCD(b,r)=GCD(r,r_1)=....=GCD(r_{k-1},r_k)=r_k$$

ដែល $r_k \mid r_{k-1}$ ។

ដូចនេះ សំណុំតួចែករួមនៃ $a\ \&\ b=$ សំណុំតួចែករួមនៃ $b\ \&\ r=.....$

$=.$ សំណុំតួចែកនៃ $r_{k-1}\ \&\ r_k=r_k$ ដែល $r_k=GCD(a,b)$ ។

ឧទាហរណ៍ :

គេឱ្យចំនួន $\mathbf{a=74}$ និង $\mathbf{b=102}$ ។ ចូររកសំណុំតួចែករវាង $\mathbf{a}$ និង $\mathbf{b}$?

តាង $\mathbf{D(a)}$ និង $\mathbf{D(b)}$ ជាសំណុំតួចែកនៃ $\mathbf{a}$ និង $\mathbf{b}$ ។

ដោយ $\mathbf{a=74=1\times 2^2\times 3\times 7}$ និង $\mathbf{b=102=1\times 2\times 3\times 17}$

គេបាន $\mathbf{D(a)=\{1,2,3,4,6,7,12,14,21,28,74\}}$

និង $\mathbf{D(b)=\{1,2,3,6,17,34,51,102\}}$

បើ $\mathbf{D(a,b)}$ ជាសំណុំតួចែករួមនៃ $\mathbf{a}$ និង $\mathbf{b}$ នោះគេបាន :

$\mathbf{D(a,b)=D(a)\cap D(b)=\{1,2,3,6\}}$ ។

ម្យ៉ាងទៀត $\mathbf{\delta=GCD(a,b)=2\times 3=6}$ នោះ $\mathbf{D(\delta)=\{1,2,3,6\}}$

ដូចនេះ $\mathbf{D(a,b)=D(\delta)=\{1,2,3,6\}}$ ។

ទ្រឹស្តីបទ :

គ្រប់ចំនួនគត់ធម្មជាតិ $\mathbf{a,b,k}$ និង គ្រប់តួចែករួម $\mathbf{d}$ នៃ $\mathbf{a}$ និង $\mathbf{b}$ គេមាន

ក. $\mathbf{GCD(ka,kb)=k.GCD(a,b)}$

ខ. $\mathbf{GCD(\frac{a}{d},\frac{b}{d})=\frac{GCD(a,b)}{d}}$

សម្រាយបញ្ជាក់

ក. $\mathbf{GCD(ka,kb)=k.GCD(a,b)}$

តាង $\mathbf{\delta=GCD(a,b)}$ នាំឱ្យមានពីចំនួនគត់ធម្មជាតិ $\mathbf{x}$ និង $\mathbf{y}$ បឋមរវាងគ្នាដែល

$\mathbf{a=\delta.x}$ និង $\mathbf{b=\delta.y}$ នោះ $\mathbf{ka=k.\delta.x}$ និង $\mathbf{k.\delta.y}$

គេបាន $\mathbf{GCD(ka,kb)=k.\delta=k.GCD(a,b)}$

ខ. $\mathbf{GCD(\frac{a}{d},\frac{b}{d}) = \frac{GCD(a,b)}{d}}$

តាមទ្រឹស្តបទខាងលើគេបាន :

$$\mathbf{d.GCD(\frac{a}{d},\frac{b}{d}) = GCD(\frac{a.d}{d},\frac{b.d}{d}) = GCD(a,b)}$$

ដូចនេះ $\mathbf{GCD(\frac{a}{d},\frac{b}{d}) = \frac{GCD(a,b)}{d}}$ ។

ទ្រឹស្តីបទ :

a និង **b** ជាពីរចំនួនគត់ធម្មជាតិហើយ δ ជាតួចែករួមនៃ **a** និង **b** ។

δ ជាតួចែករួមធំបំផុតនៃ **a** និង **b** លុះត្រាតែ $\mathbf{\frac{a}{\delta}}$ និង $\mathbf{\frac{b}{\delta}}$ បឋមរវាងគ្នា ។

-ឧបមាថា $\mathbf{\frac{a}{\delta}}$ និង $\mathbf{\frac{b}{\delta}}$ បឋមរវាងគ្នានោះ $\mathbf{GCD(\frac{a}{\delta},\frac{b}{\delta}) = 1}$

គេបាន $\mathbf{\delta.GCD(\frac{a}{\delta},\frac{b}{\delta}) = 1.\delta = \delta}$ ដោយ $\mathbf{\delta.GCD(\frac{a}{\delta},\frac{b}{\delta}) = GCD(a,b)}$

នោះគេបាន $\mathbf{GCD(a,b) = \delta}$ ។

-បើ $\mathbf{GCD(a,b) = \delta}$ នោះ $\mathbf{\frac{GCD(a,b)}{\delta} = \frac{\delta}{\delta} = 1}$

តែ $\mathbf{GCD(\frac{a}{\delta},\frac{b}{\delta}) = \frac{GCD(a,b)}{\delta}}$ នោះ $\mathbf{GCD(\frac{a}{\delta},\frac{b}{\delta}) = 1}$ នោះ $\mathbf{\frac{a}{\delta}}$ និង $\mathbf{\frac{b}{\delta}}$

ជាចំនួនគត់បឋមរវាងគ្នា ។

6. *សមភាពបឺស៊ូ* (Bezout's Indentity)

ចំពោះគ្រប់ចំនួនគត់ធម្មជាតិ $\mathbf{a}$ និង $\mathbf{b}$ មានចំនួនគត់រ៉ឺឡាទីហ្វ $\mathbf{u}$ និង $\mathbf{v}$ ដែល $\mathbf{au+bv=GCD(a,b)}$ ។

សម្រាយបញ្ជាក់ :

តាមអាល់កូរីតអឺគ្លីតគេបាន :

$\mathbf{a=bq_1+r_1}$ ឬ $\mathbf{r_1=a-bq_1}$ ដែល $\mathbf{0\le r_1<b}$

$\mathbf{b=r_1q_2+r_2}$ ឬ $\mathbf{r_2=b-r_1q_2=a(-q_2)+b(1+q_1q_2)}$

$$\mathbf{r_1=r_2q_3+r_3} \text{ ឬ } \mathbf{r_3=r_1-r_2q_3}$$
$$\mathbf{=a-bq_1+aq_2q_3-bq_3(1+q_1q_2)}$$
$$\mathbf{=a(1+q_2q_3)+b(-q_1-q_3-q_1q_2q_3)}$$

យើងសង្កេតឃើញថា $\mathbf{r_1=a\alpha_1+b\beta_1}$ ដែល $\mathbf{\alpha_1=1\,,\beta_1=-q_1}$

$\mathbf{r_2=a\alpha_2+b\beta_2}$ ដែល $\mathbf{\alpha_2=-q_2\,,\beta_2=1+q_1q_2}$

$\mathbf{r_3=a\alpha_3+b\beta_3}$ ដែល $\mathbf{\alpha_3=1+q_2q_3}$

$\mathbf{\beta_3=-q_1-q_3-q_1q_2q_3}$ ។

ឧបមាថា $\mathbf{r_k=a\alpha_k+b\beta_k}$ ពិត

យើងនឹងស្រាយថា $\mathbf{r_{k+1}=a\alpha_{k+1}+b\beta_{k+1}}$ ពិតទៀត ។

គេមាន $\mathbf{r_{k-1}=r_kq_{k+1}+r_{k+1}}$ នោះ $\mathbf{r_{k+1}=r_{k-1}-r_kq_{k+1}}$

តែតាមការឧបមាគេមាន $r_k = a\alpha_k + b\beta_k$ និង $r_{k-1} = a\alpha_{k-1} + b\beta_{k-1}$

គេបាន $r_{k+1} = a\alpha_{k-1} + b\beta_{k-1} - a\alpha_k q_{k+1} - b\beta_k q_{k+1}$

$$r_{k+1} = a(\alpha_{k-1} - \alpha_k q_{k+1}) + b(\beta_{k-1} - \beta_k q_{k+1})$$

ដោយយក $\alpha_{k+1} = \alpha_{k-1} - \alpha_k q_{k+1}$ និង $\beta_{k+1} = \beta_{k-1} - \beta_k q_{k+1}$

គេបាន $r_{k+1} = a\alpha_{k+1} + b\beta_{k+1}$ ពិត ។

ដូចនេះ $GCD(a,b) = r_k = a\alpha_k + b\beta_k$ ។

សរុបមកចំពោះគ្រប់ចំនួនគត់ធម្មជាតិ a និង b មានចំនួនគត់រឺឡាទីហ្វ u និង v ដែល

$au + bv = GCD(a,b)$ ។

7. *ទ្រឹស្តីបទបឺស៊ូ (Bezout's theory)*

ពីរចំនួនគត់ធម្មជាតិ a និង b បឋមរវាងគ្នាលុះត្រាតែមានពីរចំនួនគត់រឺឡាទីហ្វ u និង v ដែល $au + bv = 1$ ។

សម្រាយបញ្ជាក់ :

តាម ***Bezout's Indentity***

ចំពោះគ្រប់ចំនួនគត់ធម្មជាតិ a និង b មានចំនួនគត់រឺឡាទីហ្វ u និង v ដែល

$au + bv = GCD(a,b)$ ។

-បើ $au + bv = 1$ នោះ $GCD(a,b) = 1$ នាំឱ្យ a និង b បឋមរវាងគ្នា ។

-បើ a និង b បឋមរវាងគ្នានោះ $GCD(a,b) = 1$ ហើយ $au + bv = 1$ ។

ឧទាហរណ៍១ : ចូរស្រាយពីរចំនួនគត់ធម្មជាតិបន្តគ្នាជាចំនួនបឋម ។

តាង $\mathbf{n}$ និង $\mathbf{n+1}$ ជាពីរចំនួនគត់បន្តគ្នា ។

ដោយ $\mathbf{(n+1)\times 1+n\times(-1)=n+1-n=1}$ នោះតាមទ្រឹស្តីបទ**Bezout**

គេបាន $\mathbf{n}$ និង $\mathbf{n+1}$ ជាពីរចំនួនគត់ធម្មជាតិបឋមរវាងគ្នា ។

ឧទាហរណ៍ ២ : **(IMO 1959)**

គ្រប់ចំនួនគត់ធម្មជាតិ $\mathbf{n}$ បង្ហាញថា $\mathbf{\dfrac{21n+4}{14n+3}}$ ជាប្រភាគសម្រួលមិនបាន ។

គេមាន $\mathbf{(14n+3)(3)+(21n+4)(-2)=42n+9-42n-8=1}$

នោះតាមទ្រឹស្តីបទ**Bezout** គេបាន $\mathbf{21n+4}$ និង $\mathbf{14n+3}$ ជាពីរចំនួនគត់ធម្មជាតិបឋមរវាងគ្នា ។

ដូចនេះ $\mathbf{\dfrac{21n+4}{14n+3}}$ ជាប្រភាគសម្រួលមិនបាន ។

8. *ទ្រឹស្តីបទហ្គោស (Gauss's theory)*

បើផលគុណ $\mathbf{ab}$ ចែកដាច់នឹង $\mathbf{c}$ ហើយ $\mathbf{c}$ និង $\mathbf{a}$ បឋមរវាងគ្នានោះ $\mathbf{b}$ ចែកដាច់នឹង $\mathbf{c}$ ។

សម្រាយបញ្ជាក់

បើ $\mathbf{c}$ និង $\mathbf{a}$ បឋមរវាងគ្នានោះ $\mathbf{GCD(c,a)=1}$ ។

តាមទ្រឹស្តីបទ **Bezout** នាំឱ្យមានចំនួនគត់រ៉ឺទ្បាទីហ្វ $\mathbf{u}$ និង $\mathbf{v}$ ដែល $\mathbf{au+cv=1}$

នាំឱ្យ $\mathbf{abu+bcv=b}$ ។

ដោយ $\mathbf{c\,|\,ab}$ នោះ $\mathbf{c\,|\,abu+bcv}$ ឬ $\mathbf{c\,|\,b}$ ។

ដូចនេះ បើ $c|ab$ និង $GCD(a,c)=1$ នោះ $c|b$ ។

ឧទាហរណ៍ :

គ្រប់ចំនួនគត់ធម្មជាតិ n បើ $GCD(n+1;6)=1$ នោះចូរស្រាយថា :

ចំនួន $2n^2+n$ ចែកដាច់នឹង 6 ។

គេមាន $n(n+1)(2n+1)=6(1^2+2^2+...+n^2)$

គេបាន $6|n(n+1)(2n+1)$ តែតាមបម្រាប់ $GCD(n+1,6)=1$

តាមទ្រឹស្តីបទហ្គោសគេបាន $6|n(2n+1)$ ។

វិបាក :

បើ $a|n$, $b|n$ និង $GCD(a,b)=1$ នោះ $ab|n$ ។

សម្រាយបញ្ជាក់

បើ $a|n$ នោះមាន $q\in IN$ ដែល $n=aq$

ហើយ $b|n$ នោះ $b|aq$

ដោយ $GCD(a,b)=1$ នោះមាន $q'\in IN$ ដែល $q=bq'$

ហេតុនេះ $n=aq=abq'$ នាំឱ្យ $ab|n$ ។

ឧទាហរណ៍ : (Eötvös Competition 1899)

Show that $2903^n - 803^n - 464^n + 261^n$ is divisible by 1897

គេមាន $1897=7\times 271$ ដែល $GCD(7,271)=1$

តាមសមភាព $a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+....+b^{n-1})$

$2903^n-803^n=(2903-803)q_1=7\times 300q_1$

$464^n-261^n=(464-261)q_2=7\times 29q_2$

គេបាន $2903^n - 803^2 - 464^n + 261^n = 7(300q_1 - 29q_2)$

នាំឱ្យ $7 \mid 2903^n - 803^n - 464^n + 261^n$ ។

ម្យ៉ាងទៀត $2903^n - 464^n = (2903 - 464)q_3 = 271 \times 9q_3$

និង $803^n - 261^n = (803 - 261)q_4 = 271 \times 2q_4$

នាំឱ្យ$271 \mid 2903^n - 803^n - 464^n + 261^n$ ។

ដូចនេះ $2903^n - 803^n - 464^n + 261^n$ ចែកដាច់នឹង 1897 ។

VI~ពហុគុណរួមតូចបំផុត

1. *ពហុគុណរួមតូចបំផុតនៃពីរចំនួនគត់ធម្មជាតិ*

ក. និយមន័យ :

គេយក a និង b ជាពីរចំនួនកត់ធម្មជាតិ ។ ពហុគុណរួមតូចបំផុតនៃ a និង b គឺជាចំនួនគត់ធម្មជាតិដែលជាពហុគុណរួមវិជ្ជមាន និងតូចជាងគេនៃ a និង b ។

គេកំណត់តាង$\mu = \mathrm{LCM}(a,b)$ ជាពហុគុណរួមនៃ a និង b ។

ឧទាហរណ៍ : $\mathrm{LCM}(20,30) = 60$ ។

ខ. ទ្រឹស្តីបទ :

គ្រប់ពហុគុណនៃ $\mu = \mathrm{LCM}(a,b)$ គឺជាពហុគុណរួមនៃ a និង b ។

សម្រាយបញ្ជាក់ :

បើ $\mu = \mathrm{LCM}(a,b)$ នាំឱ្យមានគូ (α,β) នៃចំនួនគត់វិជ្ជមានដែល :

$\mu = a\alpha = b\beta$ ។

ចំពោះគ្រប់ចំនួនគត់ធម្មជាតិ k គេមាន $k\mu$ ជាពហុគុណនៃ μ ។

តាមសមភាព $\mu = a\alpha = b\beta$ គេបាន $k\mu = a(k\alpha) = b(k\beta)$

សមភាពចុងក្រោយនេះបញ្ជាក់ថា $k\mu$ គឺជាពហុគុណនៃ a និងជាពហុគុណនៃ b ។

ឧទាហរណ៍ : $\mathrm{LCM}(20,30) = 60$ ហើយ 360 ជាពហុគុណនៃ 60

ដូចនេះ 360 ជាពហុគុណរួមនៃ 20 និង 30 ព្រោះ $360 = 20\times 18$

និង $360 = 30\times 12$ ។

2. *លក្ខណៈនៃពហុគុណរួមតូចបំផុតនៃពីរចំនួនគត់ធម្មជាតិ*

តាង a , b និង n ជាចំនួនគត់ធម្មជាតិ និង d ជាតួចែករួមនៃ a និង b ។

គេមានលក្ខណៈសំខាន់ៗដូចខាងក្រោម :

ក. $\mathrm{LCM}(a,b) = \mathrm{LCM}(b,a)$

ខ. $\mathrm{LCM}(a,a) = a$

គ. $\mathrm{LCM}(1,a) = a$

ឃ. $\mathrm{LCM}(a,na) = na$

ង. $\mathrm{LCM}(na,nb) = n.\mathrm{LCM}(a,b)$

ច. $\mathrm{LCM}(\frac{a}{d},\frac{b}{d}) = \frac{\mathrm{LCM}(a,b)}{d}$

3. *ទំនាក់ទំនងរវាង* LCM(a,b) *និង* GCD(a,b)

ក. ពហុគុណរួមតូចបំផុតនៃពីរចំនួនគត់បឋមរវាងគ្នា :

ទ្រឹស្តីបទ :

បើ a និង b ជាពីរចំនួនគត់ធម្មជាតិបឋមរវាងគ្នានោះ $\mathrm{LCM}(a,b) = a.b$ ។

សម្រាយបញ្ជាក់ :

តាង $\mu = \mathbf{LCM(a,b)}$ នាំឱ្យមានគូ (α,β) នៃចំនួនគត់វិជ្ជមានដែល :

$\mu = \mathbf{a}\alpha = \mathbf{b}\beta$ ដោយ $\mathbf{GCD(a,b) = 1}$ នោះ $\mathbf{b}|\alpha$ នាំឱ្យមាន λ មួយ

ដែល $\alpha = \lambda\mathbf{b}$ ។ ហេតុនេះ $\mu = \mathbf{a}\alpha = \mathbf{b}\beta = \lambda\mathbf{ab}$ ។

ដោយ $\mu = \mathbf{LCM(a,b)}$ តូចបំផុតនោះ $\lambda = \mathbf{1}$ ។ដូចនេះ$\mathbf{LCM(a,b) = ab}$

ខ. ផលគុណរវាង LCM(a,b) និង GCD(a,b) :

ទ្រឹស្តីបទ :

បើ $\mathbf{a}$ និង $\mathbf{b}$ ជាពីរចំនួនគត់ធម្មជាតិ នោះគេបាន :

$\mathbf{GCD(a,b) \times LCM(a,b) = a \times b}$ ។

សម្រាយបញ្ជាក់ :

តាង $\mu = \mathbf{LCM(a,b)}$

បើ $\mathbf{GCD(a,b)} = \delta$ នោះមានគូ (α,β) នៃចំនួនគត់វិជ្ជមានបឋមរវាងគ្នា

ដែល $\mathbf{a} = \alpha\delta$ និង $\mathbf{b} = \beta\delta$ ។

គេបាន $\mu = \mathbf{LCM(a,b)} = \mathbf{LCM}(\alpha\delta\,,\,\beta\delta) = \delta \times \mathbf{LCM}(\alpha,\beta)$

ដោយ $\mathbf{GCD}(\alpha,\beta) = \mathbf{1}$ នោះ $\mathbf{LCM}(\alpha,\beta) = \alpha \times \beta$

ហេតុនេះ $\mu = \mathbf{LCM(a,b)} = \delta \times \alpha\beta = \dfrac{(\alpha\delta).(\beta\delta)}{\delta} = \dfrac{\mathbf{ab}}{\delta}$

គេទាញ $\mu \times \delta = \mathbf{a \times b}$ ។

ដូចនេះ $\mathbf{GCD(a,b) \times LCM(a,b) = a \times b}$ ។

ឧទាហរណ៍១ : ចូរដោះស្រាយក្នុង $\mathbf{IN^2}$ នូវប្រព័ន្ធសមីការ :

$$\begin{cases} \mathbf{GCD(x,y)=28} \\ \mathbf{LCM(x,y)=420} \end{cases}$$

គេមាន $\mathbf{xy = GCD(x,y)\times LCM(x,y) = 28\times 420 = 11760}$

ដោយ $\mathbf{GCD(x,y)=28}$ នាំឱ្យមានគូ (α,β) នៃចំនួនគត់វិជ្ជមានបឋមរវាង

គ្នាដែល $\mathbf{x = 28\alpha}$ និង $\mathbf{y = 28\beta}$

គេបាន $\mathbf{xy = 28^2\alpha\beta = 11760}$ នោះ $\alpha\beta = \mathbf{\dfrac{11760}{784} = 15}$

គេទាញ $(\alpha,\beta)\in\{(3,5);(5,3);(1,15);(15,1)\}$ ។

ដោយ $\mathbf{x = 28\alpha}$ និង $\mathbf{y = 28\beta}$ នោះគេបានគូចម្លើយ :

$\mathbf{(x,y);(y,x)\in\{(84,140);(28,420)\}}$ ។

ឧទាហរណ៍២ : ចូរដោះស្រាយក្នុង $\mathbf{IN^2}$ នូវប្រព័ន្ធសមីការ :

$$\begin{cases} \mathbf{x+y=276} \\ \mathbf{LCM(x,y)=1440} \end{cases}$$

តាង $\mathbf{GCD(x,y)=\delta}$ នោះមានគូ (α,β) នៃចំនួនគត់វិជ្ជមានបឋមរវាងគ្នា

ដែល $\mathbf{x=\alpha\delta}$ និង $\mathbf{y=\beta\delta}$ ។

គេបាន $\mathbf{x+y=\alpha\delta+\beta\delta=276}$ នោះ $\alpha+\beta = \mathbf{\dfrac{276}{\delta}}$ **(1)**

ដោយ $\mathbf{xy = GCD(x,y)\times LCM(x,y)}$

គេបាន $\mathbf{\alpha\beta\delta^2 = 1440\delta}$ នោះ $\alpha\beta = \mathbf{\dfrac{1440}{\delta}}$ **(2)**

ចែកសមីការ **(2) & (1)** អង្គ និង អង្គ គេបាន $\dfrac{\alpha\beta}{\alpha+\beta} = \mathbf{\dfrac{1440}{276} = \dfrac{120}{23}}$ **(3)**

ដោយ $\mathbf{GCD(\alpha,\beta)=1}$ នោះ $\mathbf{GCD(\alpha\beta,\alpha+\beta)=1}$ ។

តាម **(3)** គេទាញបាន $\alpha\beta = \mathbf{120}$ និង $\alpha+\beta = \mathbf{23}$ ។

គេបានគូចម្លើយ $\alpha = \mathbf{8}$, $\beta = \mathbf{15}$ ឬ $\alpha = \mathbf{15}$,$\beta = \mathbf{8}$ និង $\delta = \dfrac{\mathbf{1440}}{\alpha\beta} = \mathbf{12}$

ដូចនេះ $\mathbf{x = 96}$, $\mathbf{y = 180}$ ឬ $\mathbf{x = 180}$, $\mathbf{y = 96}$ ។

គ. ទ្រឹស្តីបទ

គ្រប់ចំនួនគត់ធម្មជាតិ $\mathbf{a}$ និង $\mathbf{b}$ បើ $\mathbf{LCM(a,b)} = \mu$ លុះត្រាតែ $\dfrac{\mu}{\mathbf{a}}$ និង $\dfrac{\mu}{\mathbf{b}}$ ជាចំនួនបឋមរវាងគ្នា ។

សម្រាយបញ្ជាក់

តាង $\delta = \mathbf{GCD(a,b)}$

-បើ $\mathbf{LCM(a,b)} = \mu$ នោះ $\mu\times\delta = \mathbf{a}\times\mathbf{b}$

គេទាញបាន $\dfrac{\mu}{\mathbf{a}} = \dfrac{\mathbf{b}}{\delta}$ និង $\dfrac{\mu}{\mathbf{b}} = \dfrac{\mathbf{a}}{\delta}$

ដោយ $\delta = \mathbf{GCD(a,b)}$ នោះ $\mathbf{GCD}(\dfrac{\mathbf{a}}{\delta}, \dfrac{\mathbf{b}}{\delta}) = \mathbf{1}$ នាំឱ្យ $\dfrac{\mathbf{a}}{\delta}$ និង $\dfrac{\mathbf{b}}{\delta}$ ជាចំនួនគត់ធម្មជាតិបឋមរវាងគ្នា ។

ដូចនេះ $\dfrac{\mu}{\mathbf{a}}$ និង $\dfrac{\mu}{\mathbf{b}}$ ក៏ជាចំនួនបឋមរវាងគ្នា ។

-ឧបមាថា μ' ជាពហុគុណនៃ $\mathbf{a}$ និង $\mathbf{b}$ ដែល $\dfrac{\mu'}{\mathbf{a}}$ និង $\dfrac{\mu'}{\mathbf{b}}$ ជាចំនួនបឋមរវាងគ្នា។

យើងនឹងស្រាយថា μ' ជា $\mathbf{LCM}$ នៃ $\mathbf{a}$ និង $\mathbf{b}$ ។

μ' ជាពហុគុណនៃ $\mu = \mathbf{LCM(a,b)}$ នាំឱ្យមាន $\lambda \in \mathbf{IN}$ ដែល $\mu' = \lambda\mu$

ហើយ $\frac{\mu'}{a}=\lambda\frac{\mu}{a}$ និង $\frac{\mu'}{b}=\lambda\frac{\mu}{b}$ នោះ λ ជាតួចែកនៃ $\frac{\mu'}{a}$ និង $\frac{\mu'}{b}$

ដោយ $\frac{\mu'}{a}$ និង $\frac{\mu'}{b}$ ជាចំនួនបឋមរវាងគ្នានោះ $\lambda=1$ ។

ដូចនេះ $\mu'=\mu=LCM(a,b)$ ។

ឧទាហរណ៍ ១ : ចូរដោះស្រាយក្នុង IN^2 នូវប្រព័ន្ធសមីការ :

$$\begin{cases} xy=1512 \\ LCM(x,y)=252 \end{cases}$$

តាង $a=\frac{LCM(x,y)}{x}=\frac{252}{x}$ និង $b=\frac{LCM(x,y)}{y}=\frac{252}{y}$

គេបាន $GCD(a,b)=1$ នោះ a និង b ជាចំនួនបឋមរវាងគ្នា ។

គេមាន $ab=\frac{252^2}{xy}=\frac{252^2}{1512}=42$

គេទាញបាន $(a,b);(b,a)=\{(6,7);(2,21);(3,14);(1,42)\}$

ដោយ $a=\frac{252}{x}$ នោះ $x=\frac{252}{a}$ និង $b=\frac{252}{y}$ នោះ $y=\frac{252}{a}$

ដូចនេះ $(x,y);(y,x)=\{(42,36);(126,12);(84,18);(252,6)\}$ ។

ឧទាហរណ៍ ២ : ចូរដោះស្រាយក្នុង IN^2 នូវប្រព័ន្ធសមីការ :

$$\begin{cases} x+y=36 \\ LCM(x,y)=105 \end{cases}$$

តាង $a=\frac{LCM(x,y)}{x}=\frac{105}{x}$ និង $b=\frac{LCM(x,y)}{y}=\frac{105}{y}$

គេបាន $GCD(a,b)=1$ នោះ a និង b ជាចំនួនបឋមរវាងគ្នា ។

មាន $x+y=\frac{105}{a}+\frac{105}{b}=36$ ឬ $\frac{a+b}{ab}=\frac{36}{105}=\frac{12}{35}$

គេទាញបាន $a+b=12$ និង $ab=35$ នោះ $a=5,b=7$ ឬ $a=7,b=5$

ដូចនេះ $x=21,y=15$ ឬ $x=15,y=21$ ។

VII. Modular Arithmetic

1. និយមន័យ ភាពសមមូល

គេយក a , b និង r ជាចំនួនគត់ដែល $b\neq 0$ ។

គេកំណត់សរសេរ $a\equiv r\ (\bmod b)$ អានថា a សមមូល r តាម b មានន័យថា $b\,|\,a-r$ (b ចែកដាច់ $a-r$) ឬមានន័យម្យ៉ាងទៀតថា a និង r មានសំណល់ដូចគ្នាពេលចែកជាមួយb ។

បើ $a-r$ ចែកមិនដាច់នឹង b នោះគេកំណត់សរសេរ $a\not\equiv r\ (\bmod b)$ ។

$a\equiv r\ (\bmod b)$ កាលណា r ជាសំណល់នៃវិធីចែករវាង a និង b ។

ឧទាហរណ៍ : ក. $17\equiv 3\ (\bmod 7)$ ព្រោះ $17=7\times 2+3$

ខ. $38\equiv 5\ (\bmod 11)$ ព្រោះ $38=11\times 3+5$

2. លក្ខណៈគ្រឹះ និង ទ្រឹស្តីបទ នៃភាពសមមូល

ក. $a\equiv a\ (\bmod b)$

ខ. បើ $a\equiv r\ (\bmod b)$ និង $r\equiv s\ (\bmod b)$ នោះ $a\equiv s\ (\bmod b)$

គ. បើ $a\equiv r\ (\bmod b)$ នោះ $r\equiv a\ (\bmod b)$

ឃ. បើ $\mathbf{a_1 \equiv r_1 \pmod b}$ និង $\mathbf{a_2 \equiv r_2 \pmod b}$

នោះ $\mathbf{a_1 + a_2 \equiv r_1 + r_2 \pmod b}$ និង $\mathbf{a_1 - a_2 \equiv r_1 - r_2 \pmod b}$

ង. បើ $\mathbf{a \equiv r \pmod b}$ នោះគ្រប់ចំនួនគត់ λ គេបាន $\mathbf{\lambda a \equiv \lambda r \pmod b}$

ច. បើ $\mathbf{a_1 \equiv r_1 \pmod b}$ និង $\mathbf{a_2 \equiv r_2 \pmod b}$

នោះ $\mathbf{a_1 a_2 \equiv r_1 r_2 \pmod b}$ ។

ឆ. បើ $\mathbf{a \equiv r \pmod b}$ នោះគ្រប់ចំនួនគត់ $\mathbf{k \geq 1}$ គេបាន $\mathbf{a^k \equiv r^k \pmod b}$

ជ. បើ $\mathbf{\mu = LCM(b_1, b_2, ..., b_n)}$ ហើយ $\mathbf{a \equiv r \pmod{b_k}; k = 1,2,...}$

លុះត្រាតែ $\mathbf{a \equiv r \pmod \mu}$ ។

ឈ. យក $\mathbf{f}$ ជាពហុធាមានមេគុណជាចំនួនគត់ ។

$\mathbf{a \equiv r \pmod b}$ នោះ $\mathbf{f(a) \equiv f(r) \pmod b}$ ។

2. *ទ្រឹស្តីបទ ក្នុងភាពសមមូល*

ទ្រឹស្តីបទទី១

គេយក $\mathbf{p}$ ជាចំនួនបឋម ។

បើ $\mathbf{a}$ និង $\mathbf{b}$ ជាពីរចំនួនគត់ដែល $\mathbf{ab \equiv 0 \pmod p}$ នោះគេទាញបាន

$\mathbf{a \equiv 0 \pmod p}$ ឬ $\mathbf{b \equiv 0 \pmod b}$ ។

ទ្រឹស្តីបទទី២

យក $\mathbf{m}$ ជាចំនួនគត់វិជ្ជមាន ហើយ $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ ជាបីចំនួនគត់ដែល $\mathbf{c \neq 0}$ ។

បើ $\mathbf{ac \equiv bc \pmod m}$ នោះ $\mathbf{a \equiv b \pmod{\frac{m}{gcd(c,m)}}}$

ក្ទ្រឹស្តីបទទី៣

តាង m ជាចំនួនគត់វិជ្ជមាន ហើយ a និង b ជាចំនួនគត់បឋមទៅនឹង m ។

ចំពោះគ្រប់ចំនួនគត់ x និង y បើ $a^x \equiv b^x \pmod{m}$

និង$a^y \equiv b^y \pmod{m}$ នោះ $a^{GCD(x,y)} \equiv b^{GCD(x,y)} \pmod{m}$

3. *សំណល់ក្នុងវិធីចែក*

ខាងក្រោមនេះជាឧទាហរណ៍នៃការសិក្សាអំពីសំណល់នៃវិធីចែករវាងចំនួនរាង n^k ជាមួយចំនួនគត់វិជ្ជមាន b ណាមួយ ។

1. $n^2 \equiv 0$ ឬ $1 \pmod{2}$
2. $n^2 \equiv 0$ ឬ $1 \pmod{3}$
3. $n^2 \equiv 0$ ឬ $\pm 1 \pmod{5}$
4. $n^2 \equiv 0$ ឬ 1 ឬ $4 \pmod{8}$
5. $n^3 \equiv 0$ ឬ $\pm 1 \pmod{9}$

VIII_គោលការណ៍នៃប្រព័ន្ធរាប់

1. *និយមន័យ*

✍ ប្រពន្ធ័រាប់ ជាសំណុំនៃការសន្មតទាំងអស់ដែលសម្រាប់សរសេរចំនួនគត់ ។

✍ គោលនៃប្រពន្ធ័រាប់ ជាចំនួនលេខដែលប្រើក្នុងប្រពន្ធ័នោះ ។

✍ ក្នុងប្រពន្ធ័រាប់គោល x ដែល x ជាចំនួនគត់ធំជាង 1 ដាច់ខាត ។

គេប្រើ x លេខ គឺ : $\{ 0 , 1 , 2 , 3 , ..., (x-1) \}$ ។

✍ តាមសន្មតចំនួនគត់ធម្មជាតិតូចជាងគោលដែលតាងលេខតែមួយ ។

-ប្រពន្ធ័គោល **2** ប្រើលេខ **0** និង **1** ដែលតាងចំនួនសូន្យ និង មួយ ។

-ប្រពន្ធ័គោល **10** ប្រើលេខ **0 , 1 ,2 , 3 , 4 ,5 ,6 , 7 ,8** និង **9** ដែលតាងចំនួន : សូន្យ-មួយ-ពីរ-បី-បួន-ប្រាំ-ប្រាំមួយ-ប្រាំពីរ-ប្រាំបី និង ប្រាំបួន ។

2. *ការសរសេរមួយចំនួននៅក្នុងប្រពន្ធ័រាប់គោល* x

ក. អត្ថិភាព :

ចំនួនសញ្ញាប្រើគឺ $0,1,2,3,....,(x-1)$

ដែល $0<1<2<3<...<x-1$ ។ យក N ជាចំនួនគត់ណាមួយ ។

✍ បើ $N<x$ នោះ N តាងដោយសញ្ញាណាមួយក្នុងចំណោមលេខដូចខាងលើ ។

✍ បើ $N\geq x$ នោះមានគូ (q_1,r_o) ដែល $N=q_1x+r_o$, $0\leq r_o<x$

ដែល r_0 តាងឱ្យលេខណាមួយក្នុងចំណោមលេខខាងលើ និង $q_1\neq 0$ ។

a/ បើ $q_1<x$ នោះមានសញ្ញាមួយសម្រាប់សម្គាល់ q_1 ដែលគេសន្មតសរសេរ :

$$N=q_1x+r_0=\overline{q_1r_o}$$ ។

ឧទាហរណ៍ :

ក្នុងប្រពន្ធ័គោលដប់ $N=79$ មានន័យថា $N=\overline{79}=7x+9$

ដែល x ស្មើនឹង 10 ។

ក្នុងប្រពន្ធ័គោលប្រាំពីរ $N=24$ មានន័យថា $N=\overline{24}=2x+4$

ដែល x ស្មើនឹង 7 ។

b/ បើ $q_1\geq x$ នោះមានគូ (q_2,r_1) ដែល $q_1=q_2x+r_1$

ដែល $q_2\neq 0$, $0\leq r_1<x$ ហើយ :

$$N=(q_2x+r_1)x+r_o=q_2x^2+r_1x+r_0=\overline{q_2r_1r_o}$$ ។

c/ បើ $q_2\ge x$ នោះមានគូ $(q_3\,,r_2)$ ដែល $q_2=q_3x+r_2$

ដែល $q_3\ne 0$, $0\le r_2<x$ ហើយ :

$$N=(q_3x+r_2)x^2+r_1x+r_0$$
$$=q_3x^3+r_2x^2+r_1x+r_o$$
$$=\overline{q_3r_2r_1r_0}$$

យើងធ្វើរបៀបនេះដដែលៗ រហូតដល់ពេលដែលបានផលចែក $q_n<x$ នោះគេបាន

$$N=q_nx^n+r_{n-1}x^{n-1}+....+r_1x+r_0$$
$$=\overline{q_nr_{n-1}r_{n-2}.....r_2r_1r_o}$$

ដែល $r_0\,,r_1\,,r_2\,,....,r_{n-1}$ និង q_n សុទ្ធតែជាលេខដែលតូចជាង x ដាច់ខាត ។

ក្នុងន័យនេះគេអាចសរសេរ : $\begin{cases} q_n\le x-1 \\ r_{n-1}\le x-1 \\ ----- \\ ----- \\ r_0\le x-1 \end{cases}$

គេបាន $N\le(x-1)x^n+(x-1)x^{n-1}+...+(x-1)x+(x-1)$

$$N\le x^{n+1}-1<x^{n+1}$$

ដូចនេះ $N<x^{n+1}$ ។

ឧទាហរណ៍

ក្នុងប្រពន្ធ័គោល 5 ចំនួន $N = \overline{24031} < 5^6 = 15625$

ព្រោះ $\overline{24031} = 2\times 5^4 + 4\times 5^3 + 0\times 5^2 + 3\times 5^1 + 1$

$= 1250 + 500 + 0 + 15 + 1 = 1766$ ។

ខ. ភាពមានតែមួយ :

យើងបានសិក្សារួចមកហើយថាវិធីចែកអឺក្លីតរវាង N នឹង x វាផ្តល់គូ (q_1, r_o) តែមួយគត់ដែល $N = q_1x + r_0$, $0 \le r_0 < x$ ។ អាស្រ័យហេតុនេះគេក៏បានគូ $(q_2, r_1), (q_3, r_2), ..., (q_n, r_{n-1})$ តែមួយគត់ដែរ ។

ដូចនេះចំនួននីមួយៗនៃបណ្តាចំនួន $r_0, r_1, ..., r_{n-1}, q_n$ មានតែមួយគត់ចំពោះចំនួនគត់ N គឺបានន័យថាគេអាចសរសេរ N បានតែមួយបែបគត់ ។

គ. ទ្រឹស្តីបទ

គ្រប់ចំនួនគត់ N មានតំណាងតែមួយគត់នៅក្នុងប្រពន្ធ័របាប់នៃគោល x ។

ជាពិសេស ចំពោះគ្រប់គោល x គេបាន $x = 1.x + 0 = \overline{10}$

ដូចនេះចំពោះគ្រប់គោល x គេបាន :

$$N = \overline{q_n r_{n-1} .... r_1 r_0} = q_n x^n + r_{n-1}x^{n-1} + ... + r_1 z + r_0$$

ឬគេអាចសរសេរ :

$$N = (q_n x^{n-k} + r_{n-1}x^{n-k-1} + ... + r_k)x^k + (r_{k-1}x^{k-1} + ... + r_0)$$

តាង $Q = q_n x^{n-k} + ... + r_k$; $R = r_{k-1}x^{k-1} + ... + r_0$

គេបាន $N = Q.x^k + R$ ដែល $R = \overline{r_{k-1} r_{k-2} .... r_0} < x^k$ ។

ដូចនេះ **Q** ជាផលចែក និង **R** ជាសំណល់នៃវិធីចែករវាង **N** នឹង $\mathbf{x^k}$ ។

ឃ. កំណត់សម្គាល់

គេកំណត់សម្គាល់ $\mathbf{(N)_a}$ **:** បានន័យថា **N** សរសេរក្នុងប្រព័ន្ធគោល **a** ហើយ **a** សរសេរក្នុងប្រពន្ធ័គោល **10** ។

បើគ្មាន **a** បានន័យថា **N** សរសេរក្នុងប្រព័ន្ធគោល **10** ។

ឧទាហរណ៍ ១: គេសរសេរ $\mathbf{(2133042)_5}$ មានន័យថាសរសេរក្នុងប្រពន្ធ័គោល **5** ។

បើគេសរសេរ **2133042** មានន័យថាគេសរសេរក្នុងប្រពន្ធ័គោល **10** ។

ឧទាហរណ៍២ : ចូរសរសេរ $\mathbf{(21304)_6}$ ក្នុងប្រពន្ធ័គោល **10** ។

គេបាន $\mathbf{(21304)_6 = 2\times 6^4 + 1\times 6^3 + 3\times 6^2 + 0\times 6 + 4 = 2920}$ ។

IX~ទ្រឹស្តីបទក្នុងលក្ខណៈភាពចែកដាច់នៃមួយចំនួន

1. *ភាពចែកដាច់នឹង* 2 *ឬ នឹង* 5

ទ្រឹស្តីបទ :

-មួយចំនួនចែកដាច់នឹង **2** លុះត្រាតែលេខខ្ទង់រាយនៃចំនួននោះចែកដាច់នឹង **2** បានន័យថាចំនួននោះត្រូវមានលេខចុងក្រោយជាលេខគូ $\mathbf{\{0 , 2 , 4 , 6 , 8\}}$ ។

-មួយចំនួនចែកដាច់នឹង **5** លុះត្រាតែលេខខ្ទង់ចុងក្រោយនៃចំនួននោះជាលេខ **0** ឬ **5** ។

សម្រាយបញ្ជាក់ :

តាង $\mathbf{N = \overline{a_n a_{n-1}.....a_2 a_1 a_0}}$ ជាចំនួនគត់សរសេរក្នុងប្រព័ន្ធគោល **10** ។

គេអាចសរសេរចំនួន **N** ជា $\mathbf{N = \overline{a_n a_{n-1}....a_2 a_1}\times 10 + a_o}$

គេបាន $N \equiv a_0 \pmod{2}$ និង $N \equiv a_0 \pmod{5}$

ដូចនេះ $2|N$ លុះត្រាតែ $2|a_0$ ហើយ $5|N$ លុះត្រាតែ $5|a_0$ ។

2. *ភាពចែកដាច់នឹង* 4 *ឬ នឹង* 25

ទ្រឹស្តីបទ :

-មួយចំនួនចែកដាច់នឹង **4** លុះត្រាតែចំនួនពីរខ្ទង់ខាងចុងនៃចំនួននោះចែកដាច់នឹង **4**

-មួយចំនួនចែកដាច់នឹង **25** លុះត្រាតែលេខពីរខ្ទង់ចុងក្រោយនៃចំនួននោះ
ចែកដាច់នឹង **25** គឺ **{ 00 , 25 , 50 , 75 }** ។

សម្រាយបញ្ជាក់ :

តាង $N = \overline{a_n a_{n-1} .....a_2 a_1 a_0}$ ជាចំនួនគត់សរសេរក្នុងប្រព័ន្ធគោល **10** ។

គេអាចសរសេរចំនួន N ជា $N = \overline{a_n a_{n-1}....a_2} \times 100 + \overline{a_1 a_o}$

គេបាន $N \equiv \overline{a_1 a_0} \pmod{4}$ និង $N \equiv \overline{a_1 a_0} \pmod{25}$

ដូចនេះ $4|N$ លុះត្រាតែ $4|\overline{a_1 a_0}$ ហើយ $25|N$ លុះត្រាតែ $25|\overline{a_1 a_0}$ ។

3. *ភាពចែកដាច់នឹង* 3 *ឬ នឹង* 9

ទ្រឹស្តីបទ :

-មួយចំនួនចែកដាច់នឹង **3** លុះត្រាតែផលបូកនៃគ្រប់លេខខ្ទង់រាយនៃចំនួននោះ
ចែកដាច់នឹង **3** ។

-មួយចំនួនចែកដាច់នឹង **9** លុះត្រាតែផលបូកនៃគ្រប់លេខខ្ទង់រាយនៃចំនួននោះ
ចែកដាច់នឹង **9** ។

សម្រាយបញ្ជាក់ :

តាង $N=\overline{a_n a_{n-1}.....a_2 a_1 a_0}$ ជាចំនួនគត់សរសេរក្នុងប្រព័ន្ធគោល **10** ។

គេអាចសរសេរចំនួន N ជា $N=\sum_{k=0}^{n}(a_{n-k}\times 10^{n-k})$

ដោយ $10^{n-k}\equiv 1 \pmod 3$ និង $10^{n-k}\equiv 1 \pmod 9$

គេបាន $N\equiv \sum_{k=0}^{n}(a_{n-k}) \pmod 3$ និង $N\equiv \sum_{k=0}^{n}(a_{n-k}) \pmod 9$

ដែល $\sum_{k=0}^{n}(a_{n-k})=\sum_{k=0}^{n}(a_k)=a_0+a_1+....+a_n$ ។

ដូចនេះ $3|N$ លុះត្រាតែ $3|\sum_{k=0}^{n}(a_k)$ ហើយ $9|N$ លុះត្រាតែ $9|\sum_{k=0}^{n}(a_k)$ ។

4. ***ភាពចែកដាច់នឹង*** **11**

ទ្រឹស្តីបទ :

មួយចំនួនចែកដាច់នឹង **11** លុះត្រាតែផលដករវាងផលបូកលេខខ្ទង់សេស និង ផលបូកលេខខ្ទង់គូនៃចំនួននោះ(រាប់ពីស្តាំទៅឆ្វេង) ចែកដាច់នឹង **11** ។

សម្រាយបញ្ជាក់ :

តាង $N=\overline{a_n a_{n-1}.....a_2 a_1 a_0}$ ជាចំនួនគត់សរសេរក្នុងប្រព័ន្ធគោល **10** ។

គេអាចសរសេរចំនួន N ជា $N=\sum_{k=0}^{n}(a_{n-k}\times 10^{n-k})=\sum_{k=0}^{n}(a_k\times 10^{k})$

ដោយ $10^k\equiv(-1)^k \pmod{11}$

គេបាន $N \equiv \sum_{k=0}^{n}(-1)^k a_k \pmod{11}$

ដែល $\sum_{k=0}^{n}(-1)^k a_k = (a_0 + a_2 + ...) - (a_1 + a_3 + ...)$

ដូចនេះ $11 | N$ លុះត្រាតែ $11 | (a_0 + a_2 + ...) - (a_1 + a_3 + ...)$ ។

X~ទ្រឹស្តីបទហ្វែម៉ាត និង វិលសុន

ក. ទ្រឹស្តីបទហ្វែម៉ាត (Fermat's Theorem)

បើ p ជាចំនួនបឋម និង a ជាចំនួនគត់ធម្មជាតិចែកមិនដាច់នឹង p នោះគេបាន

$a^p - a$ ចែកដាច់នឹង p ឬ $a^p \equiv a \pmod p$ ។

-ចំពោះ $a = 1$ គេបាន $1^p - 1 \equiv 0$ (mpd p) ពិត

-យើងឧបមាថាវាពិតចំពោះ $a = m$ គឺ $m^p - m \equiv 0 \pmod p$

ដែល m ចែកមិនដាច់នឹង p ។

-យើងនឹងស្រាយថាវាពិតចំពោះ $a = m + 1$ ទៀតគឺ :

$(m+1)^p - (m+1) \equiv 0 \pmod p$ ។

តាមរូបមន្តទ្វេធាញូតុនគេមាន :

$$(m+1)^p = \sum_{k=0}^{p} C_p^k m^k = \sum_{k=1}^{p-1}(C_p^k m^k) + m^p + 1$$

គេមាន $C_p^k = \dfrac{p!}{k!(p-k)!} = \dfrac{p}{k}\cdot\dfrac{(p-1)!}{(k-1)!(p-k)!} = \dfrac{p}{k} C_{p-1}^{k-1}$

ឬ $kC_p^k = pC_{p-1}^{k-1}$ នោះ $p | kC_p^k$ តែដោយ $GCD(p,k) = 1$

នោះគេទាញ $p \mid C_p^k$ នាំឱ្យ $p \mid \sum_{k=1}^{p-1} C_p^k m^k$

ហេតុនេះ $(m+1)^p \equiv m^p + 1 \pmod p$

តែតាមការឧបមា $m^p - m \equiv 0 \pmod p$

គេបាន $(m+1)^p - (m+1) \equiv (m^p - m) \equiv 0 \pmod p$ ពិត ។

ដូចនេះ $a^p \equiv a \pmod p$ ដែល a ចែកមិនដាច់នឹង p ។

វិធាក :

តាមទ្រឹស្តីបទខាងលើគេអាចសរសេរ $a^p - a = a(a^{p-1} - 1) \equiv 0 \pmod p$

បើ $GCD(a,p) = 1$ នោះ $p \mid (a^{p-1} - 1)$ ។

ដូចនេះ $a^{p-1} \equiv 1 \pmod p$ ដែល a និង p បឋមរវាងគ្នា ។

ខ. ទ្រឹស្តីបទវិលសុន (Willson's Theorem)

បើ p ជាចំនួនបឋមនោះ $(p-1)! \equiv -1 \pmod p$

XI. ទ្រឹស្តីបទអឺលែ Euler's Theorem

1. អនុគមន៍អឺលែ

និយមន័យ :

ចំពោះគ្រប់ចំនួនគត់ធម្មជាតិ n គេតាង $\varphi(n)$ ជាគ្រប់ចំនួនគត់ធម្មជាតិ k តូចជាង n ដែលបឋមរវាងគ្នាជាមួយនឹង n ។ អនុគមន៍ $\varphi(n)$ ហៅថាអនុគមន៍អឺលែ (**Euler's totient function**) ហើយដែល $\varphi(1) = 1$ និងគ្រប់ចំនួនបឋម p គេមាន $\varphi(p) = p - 1$ ។

ឧទាហរណ៍ $\varphi(7)=7-1=6$, $\varphi(11)=11-1=0$ ។

✍ **លក្ខណ: និង ទ្រឹស្តីបទ**

ក. $\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}$

ដែល p ជាចំនួនបឋម និង $\alpha\geq 1$ ជាចំនួនគត់ធម្មជាតិ ។

ខ. $\varphi(a.b)=\varphi(a).\varphi(b)$ ដែល $GCD(a,b)=1$ ។

គ. $\varphi(p_1{}^{\alpha 1}.p_2{}^{\alpha 2}....p_k{}^{\alpha k})=\varphi(p_1{}^{\alpha 1}).\varphi(p_2{}^{\alpha 2})...\varphi(p_k{}^{\alpha k})$

ដែល p_k ជាចំនួនបឋមខុសគ្នា និង $\alpha_k\geq 1$ ជាចំនួនគត់ធម្មជាតិ ។

ឃ. $\varphi[LCM(a,b)]\times\varphi[GCD(a,b)]=\varphi(a)\times\varphi(b)$

ង. បើ $b\,|\,a$ នោះ $\varphi(b)\,|\,\varphi(a)$

ឧទាហរណ៍ :

$$\varphi(343)=\varphi(7^3)=7^3-7^2=294$$

$$\varphi(72)=\varphi(2^3.3^2)=\varphi(2^3).\varphi(3^2)=(2^3-2^2)(3^2-3)=24$$

2.ទ្រឹស្តីបទ

បើ a និង n ជាចំនួនគត់វិជ្ជមានបឋមរវាងគ្នានោះគេបាន :

$a^{\varphi(n)}\equiv 1\pmod{n}$ ។

ឧទាហរណ៍ : ចូររកលេខពីរខ្ទង់ចុងក្រោយនៃ 3^{1000} ?

គេមាន $\varphi(100)=\varphi(2^2.5^2)=(2^2-2)(5^2-5)=40$

គេបាន $3^{40}\equiv 1\pmod{100}$ នោះ $3^{1000}=(3^{40})^{25}\equiv 1\pmod{100}$

ដូចនេះចំនួន 3^{1000} មានលេខពីខ្ទង់ចុងក្រោយ 01 ។

XII. សមីការឌីយ៉ូផង់លីនេអ៊ែ (Linear Diophantine Equation)

1. និយមន័យ

សមីការដែលមារាង $a_1x_1 + a_2x_2 + ... + a_kx_k = b$ (*)

ដែលមេគុណ $a_1, a_2, ..., a_k$ និង b ជាចំនួនគត់ថេរ ។

2. ទ្រឹស្តីបទ

សមីការមានចម្លើយលុះត្រាតែ $GCD(a_1, a_2, a_3, ..., a_n) | b$ ។

ឧទាហរណ៍ : សមីការ $48x + 36y = 17$ គ្មានចម្លើយក្នុងសំណុំនៃចំនួនគត់ទេ

ព្រោះ $GCD(48, 36) = 12$ ហើយ 17 ចែកមិនដាច់នឹង 12 ។

3. ដំណោះស្រាយសមីការរាង **ax + by = c**

ទ្រឹស្តីបទ :

សន្មតថា a, b, c ជាចំនួនគត់ដែល $GCD(a,b) | c$ ហើយយក (x_o, y_o)

ជាចម្លើយមួយនៃសមីការ $ax + by = c$ ។

គ្រប់ចម្លើយដ៏ទៃទៀតនៃសមីការនេះក្នុងសំណុំចំនួនគត់ឱ្យតាមទម្រង់ :

$$x = x_0 + \frac{b}{\delta}t \ , \ y = y_0 - \frac{a}{\delta}t$$ ដែល $\delta = GCD(a,b)$, $t \in \mathbb{Z}$ ។

សម្រាយបញ្ជាក់

បើ (x_o, y_o) ជាចម្លើយមួយនៃសមីការ $ax + by = c$ នោះគេបាន :

$$ax_0 + by_0 = c \quad (1)$$

យក (x', y') ជាចម្លើយផ្សេងទៀតនៃ $ax + by = c$ នោះគេបាន :

$ax'+by'=c \quad (2)$

ធ្វើផលសងសមីការ **(2)** និង **(1)** គេបាន :

$a(x'-x_0)+b(y'-y_0)=0$

$$a(x'-x_0)=b(y_0-y')$$

ចែកអង្គទាំងពីរនៃសមីការនឹង $\delta=GCD(a,b)$ គេបាន :

$\frac{a}{\delta}(x'-x_0)=\frac{b}{\delta}(y_0-y')$ ដោយ $GCD(\frac{a}{\delta},\frac{b}{\delta})=1$

នោះគេបាន $\frac{a}{\delta}\,|\,(y_0-y')$ នាំឱ្យមាន $t\in Z$ ដែល $y_0-y'=\frac{a}{\delta}t$

គេទាញបាន $y'=y_0-\frac{a}{\delta}t$ ហើយ $\frac{a}{\delta}(x'-x_0)=\frac{b}{\delta}.\frac{a}{\delta}t$

គេទាញ $x'=x_0+\frac{b}{\delta}t$ ។

ដូចនេះ $x=x_0+\frac{b}{\delta}t$, $y=y_0-\frac{a}{\delta}t$ ដែល $\delta=GCD(a,b)$, $t\in Z$ ។

ឧទាហរណ៍ ១: ដោះស្រាយសមីការ $7x+4y=15$ ក្នុងសំណុំចំនួនគត់ ។

ចំពោះ $x=1$, $y=2$ គេបាន $7(1)+4(2)=15$ ពិត

ដូចនេះគូ **(1 ,2)** ជាចម្លើយមួយរបស់សមីការ ។

ដោយ $GCD(7,4)=1$ នោះតាមទ្រឹស្តីបទខាងលើគេបានចម្លើយ :

$x=1+4t$, $y=2-7t$ ដែល $t\in Z$ ។

ឧទាហរណ៍ ២:

គេមានស្វ៊ីតនព្វន្តពីរ $(x_n)_{n\geq 1}$ និង $(y_n)_{n\geq 1}$ កំណត់ដោយ :

$(x_n): 3, 7, 11, 15, ...$ និង $(y_n): 11\ ,\ 20\ ,\ 29\ , 38, ...$

តើក្នុងចំណោម 2012 តួដំបូងនៃស្វ៊ីត (x_n) និង (y_n) មានប៉ុន្មានតួដែលស្មើគ្នា ?

ដំណោះស្រាយ

តួទី p នៃស្វ៊ីតនព្វន្ត (x_n) គឺ $x_p = 3 + (7-3)(p-1) = 4p-1$

តួទី k នៃស្វ៊ីតនព្វន្ត (y_k) គឺ $y_k = 11 + (20-11)(k-1) = 9k+2$

បើ $x_p = y_k$ គេបាន $4p-1 = 9k+2$ ឬ $4p-9k = 3$

ចំពោះ $p = 3\ ,\ k = 1$ គេបាន $4(3) - 9(1) = 3$ ពិត

នោះគូ $p = 3\ ,\ k = 1$ ជាចម្លើយមួយនៃសមីការ ។

សមីការ $4p - 9k = 3$ អាចសរសេរ $4(p-3) = 9(k-1)$

ដោយ $GCD(4,9) = 1$ នាំឱ្យមាន $t \geq 0\ ,\ t \in IN$ ដែល

$p - 3 = 9t$ និង $k - 1 = 4t$ ឬ $p = 9t + 3\ ,\ k = 4t + 1$

ចំពោះ $1 \leq p \leq 2012$ និង $1 \leq k \leq 2012$ គេទាញបាន

$\begin{cases} 1 \leq 9t + 3 \leq 2012 \\ 1 \leq 4t + 1 \leq 2012 \end{cases}$ នាំឱ្យ $0 \leq t \leq 223$ ឬ $t = 0, 1, 2, ..., 223$ ។

ដូចនេះក្នុងចំណោម 2012 តួដំបូងនៃស្វ៊ីត(x_n)និង(y_n)មាន224តួស្មើគ្នា ។

៤. ដំណោះស្រាយសមីការរាង $ax+by=\delta=GCD(a,b)$

គេឱ្យសមីការ $ax+by=\delta$ ដែល $GCD(a,b)=\delta$

បើ (x_o,y_o) ជាចម្លើយមួយនៃសមីការ $ax+by=\delta$ នោះគេបាន :

$ax_0+by_0=\delta$ (1)

យក (x',y') ជាចម្លើយផ្សេងទៀតនៃ $ax+by=\delta$ នោះគេបាន :

$ax'+by'=\delta$ (2)

ធ្វើផលសងសមីការ (2) និង (1) គេបាន :

$a(x'-x_0)+b(y'-y_0)=0$

$$a(x'-x_0)=b(y_0-y')$$

ចែកអង្គទាំងពីរនៃសមីការនឹង $\delta=GCD(a,b)$ គេបាន :

$\frac{a}{\delta}(x'-x_0)=\frac{b}{\delta}(y_0-y')$ ដោយ $GCD(\frac{a}{\delta},\frac{b}{\delta})=1$

នោះគេបាន $\frac{a}{\delta}\,|\,(y_0-y')$ នាំឱ្យមាន $t\in Z$ ដែល $y_0-y'=\frac{a}{\delta}t$

គេទាញបាន $y'=y_0-\frac{a}{\delta}t$ ហើយ $\frac{a}{\delta}(x'-x_0)=\frac{b}{\delta}.\frac{a}{\delta}t$

គេទាញ $x'=x_0+\frac{b}{\delta}t$ ។

ដូចនេះ $x=x_0+\frac{b}{\delta}t$, $y=y_0-\frac{a}{\delta}t$ ដែល $\delta=GCD(a,b)$, $t\in Z$ ។

ឧទាហរណ៍ : ដោះស្រាយសមីការ $42x+66y=6$ ក្នុងសំណុំចំនួនគត់ ។

គេមាន $GCD(42,66)=6$ ។

ចំពោះ $x=-3\ ,y=2$ គេបាន $42(-3)+66(2)=6$ ពិត

នោះ $x=-3\ ,\ y=2$ ជាគូចម្លើយមួយនៃសមីការ ។

តាមទ្រឹស្តីបទគេបានចម្លើយទូទៅនៃសមីការគឺ :

$x=-3+11t\ \ ,\ y=2-7t$ ចំពោះគ្រប់ $t\in Z$ ។

៤. ដំណោះស្រាយសមីការរាង $ax+by=1$ *ដែល* $GCD(a,b)=1$

ដោះស្រាយសមីការ $226x+175y=1$

គេមាន $226=2^3\times3\times11\ \ ,\ 175=5^2\times7$ នោះ $GCD(226,175)=1$

តាមវិធីចែកអឺគ្លីតគេបាន :

$226=175\times1+51$ ឬ $51=226-175\times1$

$175=51\times3+22$ ឬ $22=175-51\times3$

$$22=175-(226-175\times1)\times3$$

$$22=-226\times3+175\times4$$

$51=22\times2+7$ ឬ $7=51-22\times2$

$$7=226-175\times1-(-226\times3+175\times4)\times2$$

$$7=226\times7-175\times9$$

$22=7\times3+1$ ឬ $1=22-7\times3$

$$1=-226\times3+175\times4-(226\times7-175\times9)\times3$$

$$1=226\times(-24)+175\times(31)$$

គេទាញបាន $x=-24\ ,y=31$ ជាចម្លើយមួយរបស់សមីការ ។

សមីការអាចសរសេរ $226(x+4)+175(y-31)=0$

ឬ $226(x+4)=175(31-y)$ នាំឱ្យមានចំនួនគត់ t ដែល

$x+4=175t$ និង $31-y=226t$

ដូចនេះ $x=175t-4$, $y=31-226t$ ដែល $t\in Z$ ។

XIII. សមីការពីតាគ័រ (Pythagore’s Equation)

ទ្រឹស្តីបទ

យក x , y , z ជាចំនួនគត់ធម្មជាតិដែលមានតួចែករួមស្មើ 1 ដែលផ្ទៀងផ្ទាត់ $x^2+y^2=z^2$ ។ ហេតុនេះ ក្នុងចំណោម x ឬ y ត្រូវមានមួយជាចំនួនគូយ៉ាងតិច ។ ក្នុងករណីដែល x ជាចំនួនគូនោះគេមានចំនួនគត់ធម្មជាតិបឋមរវាងគ្នា u និង v ហើយមានភាពគូសេសផ្ទុយគ្នាដែល :

$x=2uv$, $y=m^2-n^2$, $z=m^2+n^2$ ។

សម្រាយបញ្ជាក់

យក d ជាតួចែករួមរបស់ x និង y នោះ $d^2\,|\,x^2+y^2$

ដូចនេះ $d^2\,|\,z^2$ ឬ $d\,|\,z$ នោះ d ជាតួចែករួមនៃ x , y , z ។

ដោយបម្រាប់គេមាន $d=1$ នោះ x និង y បឋមរវាងគ្នា ហើយ x,y,z បឋមរវាងគ្នាពីៗ ។

បើ x និង y ជាចំនួនសេសទាំងពីរនោះ $x^2\equiv y^2\equiv 1\ (\text{mod } 4)$

គេបាន $z^2=x^2+y^2\equiv 2\ (\text{mod } 4)$ មិនអាចមាន ។

ដូចនេះ x និង y មិនអាចជាចំនួនសេទាំងពីរទេ ។ សន្មតថា x ជាចំនួនគត់វិជ្ជមានគូ

នោះគេយក $\mathbf{x = 2w}$ គ្រប់ចំនួនកត់ធម្មជាតិ $\mathbf{w}$ ។

សមីការ $\mathbf{x^2 + y^2 = z^2}$ ក្លាយជា $\mathbf{4w^2 + y^2 = z^2}$

ឬ $\mathbf{(z-y)(z+y) = 4w^2}$

តាង δ ជាតួចែករួមរវាង $\mathbf{z-y}$ និង $\mathbf{z+y}$ ។

គេមាន $\mathbf{z-y}$ និង $\mathbf{z+y}$ មានលក្ខណៈគូសេសដូចគ្នាគ្រប់ចំនួនគត់ធម្មជាតិ $\mathbf{y, z}$ ។

តាង δ ជាតួចែករួមរវាង $\mathbf{z-y}$ និង $\mathbf{z+y}$ នោះ δ ក៏ត្រូវតែជាតួចែករួមរវាង

$\mathbf{(z-y)+(z+y) = 2z}$ និង $\mathbf{(z+y)-(z-y) = 2y}$ នោះ $\mathbf{\delta = 1}$

ឬ $\mathbf{\delta = 2}$ នោះគេបាន $\mathbf{GCD(\frac{z-y}{2}, \frac{z+y}{2}) = 1}$ ។

ពីសមីកា $\mathbf{(z-y)(z+y) = 4w^2}$ គេអាចសរសេរ :

$\mathbf{\frac{z-y}{2} . \frac{z+y}{2} = w^2}$ នាំឱ្យមានចំនួនគត់បឋមរវាងគ្នា $\mathbf{u}$ និង $\mathbf{v}$ ដែល

$\mathbf{\frac{z+y}{2} = u^2}$ និង $\mathbf{\frac{z-y}{2} = v^2}$ ហើយ $\mathbf{w^2 = u^2 v^2}$

គេទាញ $\mathbf{w = uv}$, $\mathbf{z = u^2 + v^2}$ និង $\mathbf{y = u^2 - v^2}$

ដូចនេះ $\mathbf{x = 2uv}$, $\mathbf{y = m^2 - n^2}$, $\mathbf{z = m^2 + n^2}$ ។

ឧទាហរណ៍ :

បើ $\mathbf{(a_1, b_1, c_1)}$ និង $\mathbf{(a_2, b_2, c_2)}$ ជាត្រីធាតុរបស់ពីតាគ័រនោះស្រាយថា :

$\mathbf{(a_1 a_2 + b_1 b_2, a_2 b_1 - a_1 b_2, c_1 c_2)}$ ក៏ជាត្រីធាតុរបស់ពីតាគ័រដែរ ។

ដំណោះស្រាយ

$\mathbf{(a_1, b_1, c_1)}$ និង $\mathbf{(a_2, b_2, c_2)}$ ជាត្រីធាតុរបស់ពីតាគ័រនោះគេបាន

$a_1^2+b_1^2=c_1^2$ និង $a_2^2+b_2^2=c_2^2$

គេមាន $a_1^2+b_1^2=(a_1+ib_1)(a_1-ib_1)=z_1.\overline{z_1}$

និង $a_2^2+b_2^2=(a_2-ib_2)(a_2+ib_2)=z_2.\overline{z_2}$

ដែល $z_1=a_1+ib_1$ និង $z_2=a_2+ib_2$

គេបាន $(a_1^2+b_1^2)(a_2^2+b_2^2)=z_1.\overline{z_1}.z_2.\overline{z_2}=(z_1\overline{z_2})(\overline{z_1}z_2)$

តាង $z=z_1.\overline{z_2}$ នោះ $\overline{z}=\overline{z_1}.z_2$ ព្រោះ $\overline{\overline{z_2}}=z_2$

គេបាន $c_1^2c_2^2=(a_1^2+b_1^2)(a_2^2+b_2^2)=z.\overline{z}=|z|^2$ (1)

ដោយ $z=(a_1+ib_1)(a_2-ib_2)=(a_1a_2+b_1b_2)+i(a_2b_1-a_1b_2)$

នោះ $|z|^2=(a_1a_2+b_1b_2)^2+(a_2b_1-a_1b_2)^2$ (2)

តាម (1) និង (2) គេបាន :

$(a_1a_2+b_1b_2)^2+(a_2b_1-a_1b_2)^2=(c_1c_2)^2$ ។

ទំនាក់ទំនងនេះបញ្ជាក់ថាត្រីធាតុ $(a_1a_2+b_1b_2\,,a_2b_1-a_1b_2\,,c_1c_2)$

ជាត្រីធាតុរបស់ពីតាគ័រ ។

XIV-សមីការផែល (Pell's equation)

1. និយមន័យ

សមីការ **Diophantine** ទាំងឡាយណាដែលមានរាង $x^2-dy^2=1$ ហៅថាសមីការផែល (**Pell's equation**) ដែល d ជាចំនួនគត់វិជ្ជមានមិនមែនជាការេប្រាកដ ។

ឧទាហរណ៍ : $x^2-3y^2=1$, $x^2-29y^2=1$ ហៅថាសមីការផែល ។

២. *ទ្រឹស្តីបទ*

បើ (x_0, y_0) ជាចម្លើយគោលនៃសមីការ ផែល $x^2 - dy^2 = 1$
គ្រប់ចម្លើយវិជ្ជមានរបស់វាមានទម្រង់ (x_n, y_n) ដែល $x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$
ចម្លើយ (x_n, y_n) អាចគណនាតាមរូបមន្ត :

$$x = \frac{(x_0 + \sqrt{d}y_0)^n + (x_0 - \sqrt{d}y_0)^n}{2}$$

$$y = \frac{(x_0 + \sqrt{d}y_0)^n - (x_0 - \sqrt{d}y_0)^n}{2\sqrt{d}}$$ ។

ឬអាចគណនាបានតាមទំនាក់ទំនងកំណើន $\begin{cases} x_{n+1} = x_0 x_n + dy_0 y_n \\ y_{n+1} = x_0 y_n + x_n y_0 \end{cases}$

សម្រាយបញ្ជាក់

បើ (x_0, y_0) ជាចម្លើយគោលនៃសមីការផែល $x^2 - dy^2 = 1$ នោះគេបាន

$x_0{}^2 - dy_0{}^2 = 1$ (i)

គេមាន $x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$ (ii)

តាមទ្វេធាញូតុនគេទាញបាន $x_n - y_n\sqrt{d} = (x_0 - y_0\sqrt{d})^n$ (iii)

ផលគុណ (ii) & (iii) អង្គនិងអង្គគេបាន :

$$(x_n + \sqrt{d}y_n)(x_n - \sqrt{d}y_n) = (x_0 + \sqrt{d}y_0)^n (x_0 - \sqrt{d}y_0)^n$$

$$x_n{}^2 - dy_n{}^2 = (x_0{}^2 - dy_0{}^2)^n \quad \text{(iv)}$$

តាម (i) & (iv) គេបាន $x_n{}^2 - dy_n{}^2 = 1$ ។

ដូចនេះគ្រប់គូចំនួនគត់វិជ្ជមាន (x_n, y_n) ដែល $x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$ ជាចម្លើយ

របស់សមីការ $x^2-dy^2=1$ ដែល (x_0,y_0) ជាចម្លើយគោលរបស់វា ។

បូកសមីការ (ii) និង (iii) គេបាន $x_n=\frac{1}{2}[(x_0+\sqrt{d}y_0)^n+(x_0-\sqrt{d}y_0)^n]$

ដកសមីការ (ii) និង (iii) គេបាន $y_n=\frac{1}{2\sqrt{d}}[(x_0+\sqrt{d}y_0)^n-(x_0-\sqrt{d}y_0)^n]$

ដូចនេះ $$x=\frac{(x_0+\sqrt{d}y_0)^n+(x_0-\sqrt{d}y_0)^n}{2}$$

$$y=\frac{(x_0+\sqrt{d}y_0)^n-(x_0-\sqrt{d}y_0)^n}{2\sqrt{d}}$$ ។

ម្យ៉ាងទៀតគេមាន $x_n+\sqrt{d}y_n=(x_0+\sqrt{d}y_0)^n$

គេបាន $x_{n+1}+\sqrt{d}y_{n+1}=(x_0+\sqrt{d}y_0)^{n+1}$

$$x_{n+1}+\sqrt{d}y_{n+1}=(x_0+\sqrt{d}y_0)(x_n+\sqrt{d}y_n)$$

$$x_{n+1}+\sqrt{d}y_{n+1}=(x_0x_n+dy_0y_n)+\sqrt{d}(x_ny_0+x_0y_n)$$

គេទាញ $\begin{cases} x_{n+1}=x_0x_n+dy_0y_n \\ y_{n+1}=x_0y_n+x_ny_0 \end{cases}$ ជាទំនាក់ទំនងកំណើន ។

ឧទាហរណ៍ ១

ដោះស្រាយសមីការ $x^2-2y^2=1$ ក្នុងសំណុំចំនួនគត់វិជ្ជមាន ។

ចំពោះ $x=3$, $y=2$ គេបាន $3^2-2\times2^2=1$ ពិត

នោះ $(3,2)$ ជាចម្លើយមួយរបស់សមីការ ។

តាង (x_n,y_n) គូចម្លើយវិជ្ជមានរបស់សមីការ $x^2-2y^2=1$ នោះតាមទ្រឹស្តីបទ

គេបាន $x_n+\sqrt{2}y_n=(3+2\sqrt{2})^n$ (1)

ហើយ $x_n-\sqrt{2}y_n=(3-2\sqrt{2})^n$ (2)

បូកសមីការ(1) & (2) គេបាន $x_n = \dfrac{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n}{2}$

ដកសមីការ (1) & (2) គេបាន $y_n = \dfrac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{2\sqrt{2}}$

ដូចនេះ $x_n = \dfrac{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n}{2}$

$y_n = \dfrac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{2\sqrt{2}}$ ដែល $n = 1\ ,\ 2\ ,....$ ។

ឧទាហរណ៍២

គេឱ្យ n ជាចំនួនគត់វិជ្ជមានដោយដឹងថា $2+2\sqrt{28n^2+1}$ ជាចំនួនគត់ ។

ចូរស្រាយថា $2+2\sqrt{28n^2+1}$ ជាការេប្រាកដនៃចំនួនគត់មួយ ។

ដំណោះស្រាយ

ស្រាយថា $2+2\sqrt{28n^2+1}$ ជាការេប្រាកដនៃចំនួនគត់

តាមបម្រាប់ $2+2\sqrt{28n^2+1}$ ជាចំនួនគត់នាំឱ្យមាន $m \in IN$ ដែល

$28n^2+1 = m^2$ ឬ $m^2 - 28n^2 = 1$ ជាសមីការ Pell ។

គូចម្លើយដំបូងនៃសមីការនេះគឺ $m = 127\ ,\ n = 24$

ព្រោះ $127^2 - 28\times 24^2 = 1$ ។ ចំពោះគ្រប់ $k \ge 1$ គេអាចសរសេរ :

$$m^2 - 28n^2 = 127^2 - 28\times 24^2 = (127 - 28\times 24^2)^k$$

$$(m-2\sqrt{7}n)(m+2\sqrt{7}n) = (127-48\sqrt{7})^k(127+48\sqrt{7})^k$$

គេទាញ $\begin{cases} m-2\sqrt{7}n = (127-48\sqrt{7})^k \\ m+2\sqrt{7}n = (127+48\sqrt{7})^k \end{cases}$

គេបានចម្លើយទូទៅនៃសមីការ :

$$m=\frac{(127-48\sqrt{7})^k+(127+48\sqrt{7})^k}{2}$$

$$n=\frac{(127+48\sqrt{7})^k-(127-48\sqrt{7})^k}{4\sqrt{7}}$$

ក្នុងករណីនេះគេបាន $2+2\sqrt{28n^2+1}=2+2m$

$$2+2\sqrt{28n^2+1}=2+(127+48\sqrt{7})^k+(127-48\sqrt{7})^k$$

ដោយ $127\pm48\sqrt{7}=(8\pm3\sqrt{7})^2$

និង $(8+3\sqrt{7})(8-3\sqrt{7})=1$ នោះគេបាន

$$2+(127+48\sqrt{7})^k+(127-48\sqrt{7})^k=\left[(8+3\sqrt{7})^k+(8-3\sqrt{7})^k\right]^2$$

គេបាន $2+2\sqrt{28n^2+1}=[(8+3\sqrt{7})^k+(8-3\sqrt{7})^k]^2$

ជាការេប្រាកដនៃចំនួនគត់ព្រោះ $(8+3\sqrt{7})^k+(8-3\sqrt{7})^k$ ជាចំនួនគត់

ដូចនេះបើ $2+2\sqrt{28n^2+1}$ ជាចំនួនគត់នោះ $2+2\sqrt{28n^2+1}$

ជាការេប្រាកដនៃចំនួនគត់ ។

ឧទាហរណ៍៣

គេឱ្យសមីការ $x^2-2(4a+1)x+4a^2+8a=0$

ចូរកំណត់គ្រប់ចំនួនគត់វិជ្ជមាន a ដើម្បីឱ្យសមីការនេះមានឫសជាចំនួនគត់វិជ្ជមាន ។

ដំណោះស្រាយ

កំណត់ចំនួនគត់វិជ្ជមាន a

ឌីសគ្រីមីណង់បង្រួមសមីការ $\Delta'=(4a+1)^2-(4a^2+8a)=12a^2+1$

ដើម្បីឱ្យសមីការនេះមានឫសជាចំនួនគត់វិជ្ជមានលុះត្រាតែ Δ' ជាការេប្រាកដ

ព្រោះផលបូក និង ផលគុណនៃឫសសមីការនេះស្មើរៀងគ្នា $\mathbf{2(4a+1)}$ និង $\mathbf{4a^2+8a}$

សុទ្ធតែវិជ្ជមានគ្រប់ចំនួនគត់វិជ្ជមាន $\mathbf{a}$ ។

តាង $\mathbf{k}$ ជាចំនួនគត់វិជ្ជមានដែល $\mathbf{12a^2+1=k^2}$

គេបាន $\mathbf{k^2-12a^2=1}$ ជាសមីការផែល (**Pell's equation**)

ចំពោះ $\mathbf{k=7}$, $\mathbf{a=2}$ គេបាន $\mathbf{7^2-12\times 2^2=1}$ ផ្ទៀងផ្ទាត់

នោះគូ $\mathbf{(k,a)=(7,2)}$ ជាចម្លើយមួយនៃសមីការ ។

តាមទ្រឹស្តីបទចម្លើយទូទៅនៃសមីការ $\mathbf{k^2-12a^2=1}$ គឺ

$$\mathbf{k=\frac{(7-4\sqrt{3})^n+(7+4\sqrt{3})^n}{2}\,,a=\frac{(7+4\sqrt{3})^n-(7-4\sqrt{3})^n}{4\sqrt{3}}}$$

ដូចនេះ $\mathbf{a=\dfrac{(7+4\sqrt{3})^n-(7-4\sqrt{3})^n}{4\sqrt{3}}}$ គ្រប់ $\mathbf{n=1,2,3,...}$ ។

ឧទាហរណ៍ ៤ . ចូរកំណត់គ្រប់ចម្លើយគត់វិជ្ជមាននៃសមីការ $\mathbf{x^2-4xy-3y^2=1}$

សមីការនេះអាចសរសេរ $\mathbf{(x-2y)^2-7y^2=1}$

តាង $\mathbf{x=s+2t}$, $\mathbf{y=t}$ គេបាន $\mathbf{s^2-7t^2=1}$

ចំពោះ $\mathbf{s=8}$, $\mathbf{t=3}$ គេបាន $\mathbf{8^2-7(3)^2=1}$ ផ្ទៀងផ្ទាត់

នោះគូ $\mathbf{(8,3)}$ ជាចម្លើយមួយនៃសមីការ ។

តាមរូបមន្តគេបានចម្លើយទូទៅរាង $\mathbf{s=\dfrac{(8-3\sqrt{7})^n+(8+3\sqrt{7})^n}{2}}$

និង $\mathbf{t=\dfrac{(8+3\sqrt{7})^n-(8-3\sqrt{7})^n}{2\sqrt{7}}}$ ដែល $\mathbf{n=1\ ,\ 2\ ,3,....}$

ដូចនេះ $\mathbf{x}=\dfrac{(\sqrt{7}+2)(8+3\sqrt{7})^{n}+(\sqrt{7}-2)(8-3\sqrt{7})^{n}}{2\sqrt{7}}$

$$\mathbf{y}=\frac{(8+3\sqrt{7})^{n}-(8-3\sqrt{7})^{n}}{2\sqrt{7}}$$ ។

កម្រងលំហាត់ជ្រើសរើស និង ដំណោះស្រាយ

លំហាត់ទី១

គេឱ្យ $\mathbf{p}$ និង $\mathbf{q}$ ជាចំនួនបឋម ។ កំណត់ $\mathbf{p}$ និង $\mathbf{q}$ ដើម្បីឱ្យសមីការ :

$\mathbf{x^2 - px + q = 0}$ មានឫសពីរផ្សេងគ្នាជាចំនួនគត់វិជ្ជមាន ។

ដំណោះស្រាយ

កំណត់ $\mathbf{p}$ និង $\mathbf{q}$

យក $\mathbf{x_1}$ និង $\mathbf{x_2}$ ដែល $\mathbf{x_1 < x_2}$ ជាឫសគត់វិជ្ជមាននៃសមីការ ។

គេបាន $\mathbf{x^2 - px + q = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2}$

គេទាញ $\mathbf{x_1 + x_2 = p}$ និង $\mathbf{x_1.x_2 = q}$

ដោយ $\mathbf{q}$ ជាចំនួនបឋមនោះ $\mathbf{x_1 = 1}$ ។

គេបាន $\mathbf{q = x_2}$, $\mathbf{p = x_2 + 1}$ ជាចំនួនគត់បន្តគ្នា ។ ដោយ $\mathbf{p}$ និង $\mathbf{q}$ ជាចំនួនបឋម

នោះ $\mathbf{q = 2}$ ហើយ $\mathbf{p = x_2 + 1 = q + 1 = 3}$

ដូចនេះ $\mathbf{p = 3}$, $\mathbf{q = 2}$ ។

លំហាត់ទី២

គេឱ្យ $\mathbf{p}$ ជាចំនួនបឋម ហើយ $\mathbf{k}$ ជាចំនួនគត់ដែល $1 \le k < p$ ។

ចូរស្រាយថា $C_p^k = \dfrac{p!}{k!(p-k)!}$ ចែកដាច់នឹង $\mathbf{p}$ ។

ដំណោះស្រាយ

ស្រាយថា $C_p^k = \dfrac{p!}{k!(p-k)!}$ ចែកដាច់នឹង $\mathbf{p}$

គេមាន $C_p^k = \dfrac{p!}{k!(p-k)!} = \dfrac{p}{k} \cdot \dfrac{(p-1)!}{(k-1)!(p-k)!} = \dfrac{p}{k} C_{p-1}^{k-1}$

ឬ $k\,C_p^k = p\,C_{p-1}^{k-1}$ នោះ $p \mid kC_p^k$

$\mathbf{p}$ ជាចំនួនបឋម ហើយ $\mathbf{k}$ ជាចំនួនគត់ដែល $1 \le k < p$ នោះ $\gcd(k,p) = 1$

ហេតុនេះតាម $p \mid kC_p^k$ គេទាញបាន $p \mid C_p^k$ ។

ដូចនេះ ស្រាយថា $C_p^k = \dfrac{p!}{k!(p-k)!}$ ចែកដាច់នឹង $\mathbf{p}$ ។

លំហាត់ទី៣ (Russia 2001)

គេឱ្យ $\mathbf{a}$ និង $\mathbf{b}$ ជាចំនួនគត់វិជ្ជមានខុសគ្នា ។

គេដឹងថា $\mathbf{ab(a+b)}$ ចែកដាច់នឹង $\mathbf{a^2+ab+b^2}$ ។

ចូរស្រាយថា $|\mathbf{a-b}| > \sqrt[3]{\mathbf{ab}}$?

ដំណោះស្រាយ

ស្រាយថា $|\mathbf{a-b}| > \sqrt[3]{\mathbf{ab}}$

តាង $\delta = \mathbf{GCD(a,b)}$ នាំឱ្យមានគូចំនួនគត់វិជ្ជមានបឋមរវាងគ្នា $\mathbf{(u,v)}$ ដែល

$\mathbf{a} = \delta\mathbf{u}$ និង $\mathbf{b} = \delta\mathbf{v}$

គេបាន $\dfrac{\mathbf{ab(a+b)}}{\mathbf{a^2+ab+b^2}} = \dfrac{\delta\mathbf{uv(u+v)}}{\mathbf{u^2+uv+v^2}}$ ជាចំនួនគត់វិជ្ជមាន ។

យើងមាន $\mathbf{GCD(u^2+uv+v^2,u) = GCD(v^2,u) = 1}$

ហើយ $\mathbf{GCD(u^2+uv+v^2,v) = GCD(u^2,v) = 1}$

និង $\mathbf{GCD(u^2+uv+v^2,u+v) = GCD(v^2,u+v) = 1}$

នោះប្រភាគ $\dfrac{\delta\mathbf{uv(u+v)}}{\mathbf{u^2+uv+v^2}}$ ជាចំនួនគត់លុះត្រាតែ $\mathbf{u^2+uv+v^2} \mid \delta$

នោះគេបាន $\delta \ge \mathbf{u^2+uv+v^2}$ ។ គ្រប់គូចំនួនគត់វិជ្ជមានបឋមរវាងគ្នា $\mathbf{(u,v)}$

គេមាន $|\mathbf{u-v}| \ge \mathbf{1}$ ហេតុនេះ $|\mathbf{a-b}|^3 = |\mathbf{u-v}|^3.\delta^3 \ge \delta^3$

តែ $\delta \ge \mathbf{u^2+uv+v^2}$ នោះ $|\mathbf{a-b}|^3 \ge \delta^2(\mathbf{u^2+uv+v^2}) > \delta^2\mathbf{uv}$

ដោយ $\mathbf{ab} = \delta^2\mathbf{uv}$ នោះ $|\mathbf{a-b}|^3 > \mathbf{ab}$ ដូចនេះ $|\mathbf{a-b}| > \sqrt[3]{\mathbf{ab}}$ ។

លំហាត់ទី៤ (Romania 2003)

គេឱ្យចំនួនបឋម $\mathbf{n_1 < n_2 < n_3 < .... < n_{31}}$ ដែល $\mathbf{n_1{}^4 + n_2{}^4 + ... + n_{31}{}^4}$ ចែកដាច់នឹង $\mathbf{30}$ នោះចូរស្រាយថាក្នុងចំណោមចំនួនទាំងនេះគេអាចរកចំនួនបឋមបីបន្តគ្នាបាន ។

ដំណោះស្រាយ

តាង $\mathbf{S = n_1{}^4 + n_2{}^4 + ... + n_{31}{}^4}$ ដែល $\mathbf{S}$ ចែកដាច់នឹង $\mathbf{30 = 2 \times 3 \times 5}$ ។

យើងដឹងថាគ្រប់ចំនួនបឋមទាំងអស់សុទ្ធតែជាចំនួនសេស លើកលែងតែចំនួនបឋម $\mathbf{2}$ ចេញ ហើយ $\mathbf{S}$ ជាផលបូកនៃចំនួនបឋមខុសគ្នាចំនួន $\mathbf{31}$ ហេតុនេះដើម្បីឱ្យ $\mathbf{30 | S}$ លុះណាតែក្នុងចំណោមចំនួនបឋមទាំងអស់នេះមានមួយស្មើនឹង $\mathbf{2}$ ។

យើងយក $\mathbf{n_1 = 2}$ ។

ជាបន្តទៀតយើងពិនិត្យឃើញថាគ្រប់ចំនួនបឋម $\mathbf{n_i}$ ដែល $\mathbf{1 \le i \le 31}$ ត្រូវមានមួយស្មើនឹង $\mathbf{3 = n_2}$ ព្រោះថាបើសិន $\mathbf{n_i}$ ចែកមិនដាច់នឹង $\mathbf{3}$ ទេនោះចំនួន $\mathbf{n_i}$ ត្រូវមានរាង $\mathbf{3k+1}$, $\mathbf{3k+2}$ គ្រប់ $\mathbf{1 \le i \le 31}$ និង $\mathbf{n_i{}^4 \equiv 1 \pmod 3}$

ហើយ $\mathbf{S = n_1{}^4 + n_2{}^4 + ... + n_{31}{}^4 \equiv 31 \equiv 1 \pmod 3}$ ។

ជាចុងក្រោយយើងនឹងស្រាយថាមាន $\mathbf{n_3 = 5}$ មួយទៀតក្នុងចំណោម $\mathbf{n_i}$ ដែល $\mathbf{1 \le i \le 31}$ ។ បើ $\mathbf{n_i}$ ដែល $\mathbf{1 \le i \le 31}$ សុទ្ធតែចែកមិនដាច់នឹង $\mathbf{5}$ នោះគេបាន $\mathbf{n_i{}^2 \equiv \pm 1 \pmod 5}$ នាំឱ្យ $\mathbf{n_i{}^4 \equiv 1 \pmod 5}$ ហើយ $\mathbf{S \equiv 31 \equiv 1 \pmod 5}$

ដូចនេះគេអាចរកបានចំនួនបឋម $\mathbf{2}$, $\mathbf{3}$, $\mathbf{5}$ បន្តគ្នាក្នុងចំណោមចំនួនបឋមទាំង $\mathbf{31}$ ។

លំហាត់ទី៥

ចូរកំណត់គ្រប់ត្រីធាតុ (x,y,z) ជាចំនួនគត់ដែល $3x+4y+5z=6$ ។

ដំណោះស្រាយ

គេមាន $3x+4y+5z=6$ នោះ $3x+4y=6-5z$

គេបាន $3x+4y\equiv 1 \pmod 5$ ព្រោះ $6-5z\equiv 1 \pmod 5$

នាំឱ្យមាន $t\in Z$ ដែល $3x+4y=1+5t$

គេទាញបាន $x=\dfrac{1+5t-4y}{3}=t-y+\dfrac{1+2t-y}{3}$

បើ $1+2t-y=0$ ឬ $y=1+2t$ នោះ $x=t-(1+2t)=-1-t$

ហើយតាមសមីការ $3x+4y+5z=6$ គេទាញបាន $z=\dfrac{6-3x-4y}{5}$

$$z=\frac{6-3(-1-t)-4(1+2t)}{5}=\frac{5-5t}{5}=1-t$$ ។

ដូចនេះ $x=-1-t$, $y=1+2t$, $z=1-t$ ។

លំហាត់ទី៦

គេឱ្យ $\mathbf{N=(11111)_n}$ ។ កំណត់ $\mathbf{n}$ ដើម្បីឱ្យ $\mathbf{N}$ ជាការេប្រាកដ ។

ដំណោះស្រាយ

គេមាន $\mathbf{N=(11111)_n=n^4+n^3+n^2+n+1}$

-បើ $\mathbf{n}$ ជាចំនួនគូនោះ $\mathbf{n^2+\frac{n}{2}}$ និង $\mathbf{n^2+\frac{n}{2}+1}$ ជាពីរចំនួនគត់បន្តគ្នា

គេមាន $\mathbf{(n^2+\frac{n}{2})^2=n^4+n^3+\frac{n^2}{4}<N}$

ហើយ $\mathbf{(n^2+\frac{n}{2}+1)^2=n^4+n^3+n^2+n+1+\frac{5n^2}{4}>N}$

នោះ $\mathbf{(n^2+\frac{n}{2})^2<N<(n^2+\frac{n}{2}+1)^2}$ នាំឱ្យ $\mathbf{N}$ មិនអាចជាការេប្រាកដ

ចំពោះគ្រប់ $\mathbf{n}$ ជាចំនួនគូ ។

-បើ $\mathbf{n}$ ជាចំនួនសេសនោះ $\mathbf{n^2+\frac{n-1}{2}}$ និង $\mathbf{n^2+\frac{n+1}{2}}$ ជាចំនួនគត់បន្តគ្នា ។

មាន $\mathbf{(n^2+\frac{n-1}{2})^2=n^4+n^3-\frac{n^2}{2}-n+\frac{1}{2}<N}$

$$\mathbf{(n^2+\frac{n+1}{2})^2=n^4+n^3+n^2+n+1+\frac{(n-3)(n+1)}{4}\geq N}$$

បើ $\mathbf{n>3}$ នោះ $\mathbf{(n^2+\frac{n-1}{2})^2<N<(n^2+\frac{n+1}{2})^2}$ នាំឱ្យ $\mathbf{N}$ មិនអាចជាការេប្រាកដ ។

ដូចនេះដើម្បីឱ្យ $\mathbf{N}$ ជាការេប្រាកដលុះត្រាតែ $\mathbf{n=3}$ គឺ $\mathbf{N=121=11^2}$ ។

លំហាត់ទី៧

ចូរស្រាយថា $\dfrac{12n+1}{30n+2}$ ជាប្រភាគសម្រួលមិនបានគ្រប់ចំនួនគត់រឺឡាទ្បិចមាន n ។

ដំណោះស្រាយ

របៀបទី១

តាង $a=12n+1$ និង $b=30n+2$

គេមាន $5a-2b=60n+5-60n-4=1$

តាមទ្រឹស្តីបទ **Bezout** គេទាញបាន a និង b ជាពីរចំនួនគត់បឋមរវាងគ្នា

ដូចនេះ $\dfrac{12n+1}{30n+2}$ ជាប្រភាគសម្រួលមិនបានគ្រប់ចំនួនគត់រឺឡាទ្បិចមាន n ។

របៀបទី២

តាមអាល់កូរីតអឺគ្លីតគេបាន :

$$\begin{aligned}\mathbf{GCD}(30n+2,12n+1)&=\mathbf{GCD}(12n+1,6n)\\&=\mathbf{GCD}(6n,1)=1\end{aligned}$$

គេទាញបាន $30n+2$ និង $12n+1$ ជាចំនួនបឋមរវាងគ្នា ។

ដូចនេះ $\dfrac{12n+1}{30n+2}$ ជាប្រភាគសម្រួលមិនបានគ្រប់ចំនួនគត់រឺឡាទ្បិចមាន n ។

លំហាត់ទី៨ (Russia 1995)

គេឱ្យ $\mathbf{m}$ និង $\mathbf{n}$ ជាចំនួនគត់វិជ្ជមានដែល :

$$\mathbf{LCM(m,n)+GCD(m,n)=m+n}$$

ចូរស្រាយថា $\mathbf{m|n}$ ឬ $\mathbf{n|m}$?

ដំណោះស្រាយ

តាង $\delta=\mathbf{GCD(m,n)}$ នាំឱ្យមានគូចំនួនគត់វិជ្ជមាន $\mathbf{(a,b)}$ ដែល $\mathbf{GCD(a,b)=1}$

ហើយ $\mathbf{m=a\delta}$ និង $\mathbf{n=b\delta}$

តាមរូបមន្ត $\mathbf{LCM(m,n)=\dfrac{mn}{GCD(m,n)}=\dfrac{ab\delta^2}{\delta}=ab\delta}$

សមីការ $\mathbf{LCM(m,n)+GCD(m,n)=m+n}$ ក្លាយជា

$$\mathbf{ab\delta+\delta=a\delta+b\delta}$$

$$\mathbf{ab+1=a+b}$$

$$\mathbf{ab-a-b+1=0}$$

$$\mathbf{a(b-1)-(b-1)=0}$$

$$\mathbf{(a-1)(b-1)=0}$$

គេទាញបាន $\mathbf{a=1}$ ឬ $\mathbf{b=1}$ ។

-បើ $\mathbf{a=1}$ គេបាន $\mathbf{m=\delta}$, $\mathbf{n=b\delta}$ នោះ $\mathbf{m|n}$

-បើ $\mathbf{b=1}$ គេបាន $\mathbf{m=a\delta}$, $\mathbf{n=\delta}$ នោះ $\mathbf{n|m}$

ដូចនេះ $\mathbf{m|n}$ ឬ $\mathbf{n|m}$ ។

លំហាត់ទី៩ (UK 1998)

គេឱ្យ x, y, z ជាចំនួនគត់វិជ្ជមានដែល $\frac{1}{x}-\frac{1}{y}=\frac{1}{z}$ ។

តាង h ជាតួចែករួមធំបំផុតនៃ x, y, z ។

ចូរស្រាយថា $hxyz$ និង $h(y-x)$ ជាការេប្រាកដ ។

ដំណោះស្រាយ

បើ h ជាតួចែករួមធំបំផុតនៃ x, y, z នាំឱ្យមានត្រីធាតុ (a, b, c) ដែល

$x = ah$, $y = bh$, $z = ch$ និង $GCD(a, b, c) = 1$ ។

តាង $\delta = GCD(a, b)$ នាំឱ្យមានគូ (m, n) ដែល $a = m\delta$, $b = n\delta$

ហើយ $GCD(a, b) = 1$ ។

គេមាន $\frac{1}{x}-\frac{1}{y}=\frac{1}{z}$ នោះ $\frac{1}{ah}-\frac{1}{bh}=\frac{1}{ch}$ ឬ $c(b-a) = ab$

ឬ $c(m\delta - n\delta) = mn\delta^2$

ឬ $c(m-n) = mn\delta$ ដោយ $GCD(m-n, n) = GCD(m, n) = 1$

និង $GCD(m-n, m) = GCD(m, n) = 1$

នោះ $\delta \mid c$ តែ $GCD(a, b, c) = 1$ នោះ $\delta = 1$ ហើយ $GCD(a, b) = 1$

គេបាន $GCD(b-a, ab) = 1$ ។ តាម $c(b-a) = ab$ គេទាញបាន

$c = ab$ និង $b - a = 1$ ។

ដូចនេះ $hxyz = h^4abc = h^4c^2 = (ch)^2$ និង $h(y-x) = h^2(b-a) = h^2$

លំហាត់ទី១០ (HMMT 2005)

ចំនួន **27000001** មានបួនកត្តាបឋមប្រាកដ ។

ចូរគណនាផលបូកកត្តាបឋមនោះ ?

ដំណោះស្រាយ

តាមសមភាព $\mathbf{a^3 + 1 = (a+1)(a^2 - a + 1) = (a+1)[(a+1)^2 - 3a]}$

បើយើងយក $\mathbf{a = 300}$ គេបាន :

$$\mathbf{27000001 = 301(301^2 - 30^2)}$$
$$\mathbf{= 301 \times 331 \times 271}$$
$$\mathbf{= 7 \times 43 \times 271 \times 331}$$

ដូចនេះ $\mathbf{7 + 43 + 271 + 331 = 652}$ ។

លំហាត់ទី១១ (HMMT 2005)

ចូរកំណត់គ្រប់ចំនួនគត់វិជ្ជមាន $\mathbf{n}$ ដើម្បីឱ្យ $\mathbf{n!+5}$ ជាគូបប្រាកដ ។

ដំណោះស្រាយ

កំណត់ $\mathbf{n}$

ចំពោះ $\mathbf{n \geq 7}$ គេបាន $\mathbf{n!+5 \equiv 5 \pmod 7}$

ចំពោះគ្រប់ចំនួនគត់វិជ្ជមាន $\mathbf{k}$ គេមាន $\mathbf{k^3 \equiv 0, \pm 1 \pmod 7}$

ដូចនេះបើ $\mathbf{n \geq 7}$ ចំនួន $\mathbf{n!+5}$ មិនអាចជាគូបប្រាកដ ។

ចំពោះ $\mathbf{n = 1\ ,\ 2\ ,\ 3, 4\ , 5, 6}$ មានតែករណី $\mathbf{n = 5}$ ដែល $\mathbf{n!+6 = 125 = 5^3}$

ដូចនេះ $\mathbf{n = 5}$ ។

លំហាត់ទី១២

បើ $\mathbf{a \equiv r \pmod n}$ នោះបង្ហាញថា $\mathbf{a^n \equiv r^n \pmod{n^2}}$

តើចម្រាស់សំណើនេះពិតឬទេ ?

ដំណោះស្រាយ

បើ $\mathbf{a \equiv r \pmod n}$ នាំឱ្យមាន $\mathbf{q \geq 0}$ ជាចំនួនគត់ដែល $\mathbf{a = nq + r}$

តាមរូបមន្តទ្វេធាញូតុនគេមាន :

$$\mathbf{a^n = (nq + r)^n = \sum_{p=0}^{n} C_n^p (nq)^{n-p} r^p}$$

$$\mathbf{a^n = \sum_{p=0}^{n-1} C_n^p (nq)^{n-p} + r^n}$$

ដោយគ្រប់ $\mathbf{0 \leq p \leq n-1}$ គេមាន $\mathbf{n \,|\, (nq)^{n-p}}$ និង $\mathbf{n \,|\, C_n^p}$

នោះ $\mathbf{n^2 \,|\, \sum_{p=0}^{n-1} C_n^p (nq)^{n-p}}$

ដូចនេះ $\mathbf{a^n \equiv r^n \pmod{n^2}}$ ។

ចម្រាស់នៃសំណើនេះមិនពិតទេ ។

ជាឧទាហរណ៍ $\mathbf{3^4 \equiv 1 \pmod{4^2}}$ ប៉ុន្តែ $\mathbf{3 \neq 1 \pmod 4}$ ។

លំហាត់ទី១៣

គេតាង $S_n(k)=1^k+2^k+3^k+....+n^k$

និង $S_n(1)=1+2+3+....+n$ ដែល k ជាចំនួនគត់វិជ្ជមានសេស ។

ចូរស្រាយថា $S_n(k)$ ចែកដាច់នឹង $S_n(1)$ ។

ដំណោះស្រាយ

គេមានគ្រប់ k ជាចំនួនសេស $a+b\,|\,a^k+b^k$ ដែល $a\,,b$ ជាចំនួនគត់វិជ្ជមាន

-ករណី $n=2m+1$ ជាចំនួនសេសនោះគេបាន

$$S_{2m+1}(k)=1^k+2^k+3^k+.....+(2m)^k+(2m+1)^k$$
$$=[1^k+(2m+1)^k]+[2^k+(2m)^k]+....$$

ដោយ $(m+1)\,|\,1^k+(2m+1)^k\ ,\ (m+1)\,|\,2^k+(2m)^k,...$

នោះគេទាញបាន $(m+1)\,|\,S_{2m+1}(k)$

ម្យ៉ាងទៀតគេអាចសរសេរ :

$$S_{2m+1}(k)=1^k+2^k+3^k+.....+(2m)^k+(2m+1)^k$$
$$=[1^k+(2m)^k]+[2^k+(2m-1)^k]+....$$

ដោយ $2m+1\,|\,1^k+(2m)^k\ ,\ 2m+1\,|\,2^k+(2m-1)^k,...$

នោះគេទាញបាន $(2m+1)\,|\,S_{2m+1}(k)$ ដោយ $\mathrm{GCD}(m+1\,,2m+1)=1$

នោះ $(m+1)(2m+1)\,|\,S_{2m+1}(k)$ ឬ $S_{2m+1}(1)\,|\,S_{2m+1}(k)$

-ករណី $n=2m$ គូ (ដោះស្រាយខាងលើដែរ) ។

លំហាត់ទី១៤ (IMO 1986)

គេតាង $\mathbf{d}$ ជាចំនួនគត់វិជ្ជមានខុសពី $\mathbf{2, 5}$ ឬ $\mathbf{13}$ ។

ចូរបង្ហាញថាគេអាចរកតម្លៃខុសគ្នា $\mathbf{a,b}$ មួយនៅក្នុងសំណុំ $\mathbf{\{2,5,13,d\}}$

ដែល $\mathbf{ab-1}$ មិនមែនជាការេប្រាកដ ។

ដំណោះស្រាយ

ការបង្ហាញ

បើ $\mathbf{a,b}$ ជាតម្លៃខុសគ្នានៃ $\mathbf{\{2,5,13,d\}}$ នោះគេបាន :

$$\mathbf{ab-1\in\{9,25,\ 64\ ,\ 2d-1,\ 5d-1,\ 13d-1\ \}}$$

ដើម្បីបង្ហាញថាមានតម្លៃ $\mathbf{a,b}$ ដែល $\mathbf{ab-1}$ មិនមែនជាការេប្រាកដនោះយើងត្រូវ

ឧបមាថា $\mathbf{2d-1\ ,\ 5d-1,\ 13d-1}$ សុទ្ធតែជាការេប្រាកដជាករណីមិនអាចមាន។

បើ $\mathbf{2d-1\ ,\ 5d-1,\ 13d-1}$ ជាការេប្រាកដនោះមានចំនួនគត់ $\mathbf{a\ ,b\ ,c}$ ដែល

$\mathbf{2d-1=a^2\ ,\ 5d-1=b^2\ ,\ 13d-1=c^2}$ ។

តាមសមីការ $\mathbf{2d-1=a^2}$ បញ្ជាក់ថា $\mathbf{a}$ គឺជាចំនួនសេស ។ យក $\mathbf{a=2x+1}$

គេបាន $\mathbf{d=\dfrac{(2x+1)^2+1}{2}=2x(x+1)+1}$ នោះ $\mathbf{d\equiv 1\ (mod\,4)}$

ម្យ៉ាងទៀតដោយ $\mathbf{d=2x(x+1)+1}$ ជាចំនួនសេសនោះតាមសមីការ :

$\mathbf{5d-1=b^2}$ និង $\mathbf{13d-1=c^2}$ គេបាន $\mathbf{b}$ និង $\mathbf{c}$ សុទ្ធតែជាចំនួនគូ ។

តាង $\mathbf{b=2y\ ,\ c=2z}$ គេបាន $\mathbf{(13d-1)-(5d-1)=c^2-b^2=4(z^2-y^2)}$

គេទាញ $\mathbf{d=\dfrac{1}{2}(z^2-y^2)}$ នោះអាចមាន $\mathbf{z}$ និង $\mathbf{y}$ ដែល $\mathbf{d\equiv 0\ (mod\,4)}$

ដោយ $d \equiv 1$ នោះមានន័យថាការឧបមាខាងលើមិនពិត ។

ដូចនេះគ្មានតម្លៃ d ដែលធ្វើឱ្យ $2d-1$, $5d-1$, $13d-1$ សុទ្ធតែជាការេប្រាកដបានទេ ។

សរុបមកគេអាចរកតម្លៃខុសគ្នា a,b មួយនៅក្នុងសំណុំ $\{2,5,13,d\}$ ដែល $ab-1$ មិនមែនជាការេប្រាកដ ។

លំហាត់ទី១៥ (IMO 1998)

ចូរកំណត់គ្រប់គូនៃចំនួនគត់វិជ្ជមាន (x,y) ដោយដឹងថា x^2y+x+y ចែកដាច់នឹង xy^2+y+7 ។

ដំណោះស្រាយ

កំណត់គ្រប់គូនៃចំនួនគត់វិជ្ជមាន (x,y)

តាង $a=x^2y+x+y$ និង $b=xy^2+y+7$

បើ a ចែកដាច់នឹង b នោះគេបានដូចគ្នា $ay-bx$ ចែកដាច់នឹង b ។

គេមាន $ay-bx=y(x^2y+x+y)-x(xy^2+y+7)=y^2-7x$

ដោយ $x\ge 1$ នោះ $xy^2\ge y^2$

នាំឱ្យ $y^2-7x\le xy^2-7x<xy^2+y+7=b$ ។

ដូចនេះ y^2-7x ចែកដាច់នឹង b លុះត្រាតែ $y^2-7x\le 0$ ។

ក. ករណីទី១ : $y^2-7x=0$ នោះ $y^2=7x$

ដោយ y ជាចំនួនគត់វិជ្ជមាននោះលុះត្រាតែ $x=7k^2$ ហើយ $y=7k$ គ្រប់ចំនួនគត់វិជ្ជមាន k ។

ខ.ករណីទី២ $y^2-7x<0$ នោះ $7x-y^2>0$

ដោយពិនិត្យឃើញថា $7x-y^2<7x$ ហេតុនេះដើម្បីឱ្យ $7x-y^2$ ចែកដាច់នឹង $b=xy^2+y+7$ លុះត្រាតែ $7x>7x-y^2\ge xy^2+y+7$

ហេតុនេះគេត្រូវឱ្យ $y^2<7$ នោះ $y=1$ ឬ $y=2$ ។

-ចំពោះ $y=1$ គេបាន $7x-y^2=7x-1$ ហើយ $b=x+8$

គេមាន $7x-1=7(x+8)-57$ ចែកដាច់នឹង $b=x+8$ លុះត្រាតែ

b ជាតួចែកនៃ 57 ។ ដោយ $b=x+8>8$ នោះ $b=19$ ឬ $b=57$

គេទាញបាន $x=11$ ឬ $x=49$ ។

ដូចនេះគេបាន $x=11$, $y=1$ ឬ $x=49$, $y=1$ ។

-ចំពោះ $y=2$ គេបាន $7x-y^2=7x-4$ ហើយ $b=4x+9$

ដោយ $GCD(4x+9;4)=1$ នោះ $7x-4$ ចែកដាច់នឹង $4x+9$

សមមូល $4(7x-4)$ ចែកដាច់នឹង $4x+9$ ។

គេមាន $4(7x-4)=7(4x+9)-79$ ។

ដោយ 79 ជាចំនួនបឋមនោះដើម្បីឱ្យ$4(7x-4)$ ចែកដាច់នឹង $4x+9$

លុះត្រាតែ $4x+9=79$ នោះ $x=\dfrac{35}{2}$ មិនមែនជាចំនួនគត់ ។

ដូចនេះក្នុងករណី $y=2$ គ្មានចម្លើយ ។

សរុបមកគេបានគូចម្លើយ :

$(x,y)\in\{\ (11,1),(49,1),(7k^2,7k)\ \},k=1,2,...$

លំហាត់ទី១៦

ចូរបង្ហាញថាចំពោះគ្រប់ចំនួនគត់វិជ្ជមាន n ចំនួន $3^n + n^3$ ចែកដាច់នឹង 7 លុះត្រាតែ $3^n n^3 + 1$ ចែកដាច់នឹង 7 ។

ដំណោះស្រាយ

-សន្មតថា $3^n + n^3$ ចែកដាច់នឹង 7 នោះ n ត្រូវចែកមិនដាច់នឹង 7

តាមទ្រឹស្តីបទ Euler គេបាន $n^6 \equiv 1 \pmod 7$ ។

ចំនួន $3^n + n^3$ ចែកដាច់នឹង 7 នោះគេបានដូចគ្នា $n^3(3^n + n^3)$ ចែកដាច់នឹង 7 ។

គេមាន $n^3(3^n + n^3) = (n^3 3^n + 1) + (n^6 - 1)$

ដោយ $n^6 \equiv 1 \pmod 7$ នោះគេទាញបាន $n^3 3^n + 1$ ចែកដាច់នឹង7

-សន្មតថា $n^3 3^n + 1$ ចែកដាច់នឹង 7 នោះ n ត្រូវចែកមិនដាច់នឹង 7

តាមទ្រឹស្តីបទ Euler គេបាន $n^6 \equiv 1 \pmod 7$ ។

ចំនួន $n^3 3^n + 1$ ចែកដាច់នឹង 7 នោះ $n^3(n^3 3^n + 1)$ ចែកដាច់នឹង 7 ។

គេមាន $n^3(n^3 3^n + 1) = (n^6 - 1)3^n + n^3 + 3^n$

ដោយ $n^6 \equiv 1 \pmod 7$ នោះគេទាញបាន $n^3 + 3^n$ ចែកដាច់នឹង7

ដូចនេះ ចំនួន $3^n + n^3$ ចែកដាច់នឹង 7 លុះត្រាតែ $3^n n^3 + 1$ ចែកដាច់នឹង 7 ។

លំហាត់ទី១៧

ចូរកំនត់គ្រប់គូតម្លៃគត់វិជ្ជមាន (a , b) បើគេដឹងថាចំនួន

$$\frac{a^2}{2ab^2-b^3+1}$$ **ជាចំនួនគត់វិជ្ជមានដែរ ។**

ដំណោះស្រាយ

កំនត់គ្រប់គូតម្លៃគត់វិជ្ជមាន (a , b) ៖

យក $\frac{a^2}{2ab^2-b^3+1}=k$ ដែល $k\in IN^*$

គេបាន $a^2-2kb^2a+k(b^3-1)=0 \quad (1)$

ឌីសគ្រីមីណង់នៃសមីការ $\Delta=4k^2b^4-4k(b^3-1)$

$$\Delta=(2kb^2-b)^2+4k-b^2$$

សមីការ (1) មានចម្លើយក្នុង IN^* លុះត្រាតែ Δ ជាការេប្រាកដ

មានន័យថា $\Delta=(2kb^2-b)^2+4k-b^2=d^2$

ដែល d ជាចំនួនគត់។

-បើ $4k-b^2=0$ ឬ $k=\frac{b^2}{4}$

យើងទទួលបាន $a=2b^2k-\frac{b}{2}=\frac{b^3-b}{2}$ ឬ $a=\frac{b}{2}$

ដោយ a , b ជាចំនួនគត់វិជ្ជមាន ហេតុនេះគេត្រូវឲ្យ ៖

$b=2p \quad , \forall p\in IN$

គេទាញ $a = 2(2p)^2 \dfrac{(2p)^2}{4} - p = 8p^4 - p$

ហើយ $a = \dfrac{2p}{2} = p$ ។

ដូចនេះ

$(a\,,b\,) = (\,8p^4 - p\,,\,2p\,)\,;\,(\,p\,,2p\,)\,,\forall p \in IN^*$

-បើ $4k - b^2 > 0$

គេបាន $(2b^2k - b)^2 + 4k - b^2 = d^2 \geq (2b^2k - b + 1)^2\,,\ \forall k \in IN^*$

ឬ $4k(b^2 - 1) + (b-1)^2 \leq 0$ គេទាញបាន $b = 1$

ក្នុងករណីសមីការ (1) ក្លាយជា $a^2 - 2k\,a = 0$ នាំឲ្យ $a = 2k$

ដូចនេះ $(\,a\,,b\,) = (\,2k\,,\,1\,)$ ចំពោះគ្រប់ $k \in IN^*$ ។

-បើ $4k - b^2 < 0$

គេបាន $(2b^2k - b)^2 + 4k - b^2 = d^2 < (2b^2k - b - 1)^2$

សមមូល $(2b^2k - b)^2 + 4k - b^2 - (2b^2k - b - 1)^2 < 0$

ឬ $b^2(4k-3) + 2b(b-1) + (4k-1) < 0$ (មិនពិតក្នុង IN^*)

សរុបមកគេបានគូចម្លើយបីមានរាងដូចខាងក្រោម ៖

$(\,a\,,b\,) = (\,2k\,,\,1\,)\,;\,(\,k\,,2k\,)\,;(8k^4 - k\,,2k\,)$

ដែល $k \in IN^*$ ។

លំហាត់ទី១៨

ចូរកំនត់គ្រប់គូតម្លៃគត់ $m , n \geq 3$ បើគេដឹងថាចំពោះគ្រប់

ចំនួនគត់វិជ្ជមាន a គេមាន $\dfrac{a^m + a - 1}{a^n + a^2 - 1}$ ជាចំនួនគត់ ។

ដំណោះស្រាយ

កំនត់គ្រប់គូតម្លៃគត់វិជ្ជមាន (m, n) ៖

ដើម្បីឲ្យ $\dfrac{a^m + a - 1}{a^n + a^2 - 1}$ ជាចំនួនគត់លុះត្រាតែ $a^n + a^2 - 1$

ជាកត្តារួមនៃ $a^m + a - 1$ ហើយ $m > n$ ។

យើងយក $m = n + k \ , \ k \in IN^*$

$$a^m + a - 1 = a^{n+k} + a - 1$$

$$= a^k (a^n + a^2 - 1) + (1 - a)(a^{k+1} + a^k - 1)$$

តាមទំនាក់ទំនងនេះដើម្បីឲ្យ $a^n + a^2 - 1$ ជាកត្តារួមនៃ $a^m + a - 1$

លុះត្រាតែ $n = k + 1$ និង $k = 2$ ។

ដូចនេះ $(m , n) = (5 , 3)$ ។

លំហាត់ទី១៩

ចូរបង្ហាញថា $P_n = n(n+1)(n+2)....(n+k)$

ចែកដាច់នឹង $(k+1)!$ ចំពោះគ្រប់ $n \in IN^*$ និង $k \in IN^*$ ។

ដំណោះស្រាយ

ការបង្ហាញ

គេមាន $P_n = n(n+1)(n+2)....(n+k)$

ចំពោះ $n = 1 :\ P_1 = 1\times 2\times 3....\times(k+1) = (k+1)!$ ចែកដាច់នឹង

$(k+1)!$ ពិត ។

ឧបមាថាវាពិតចំពោះ $n = p$ គឺ P_p ចែកដាច់នឹង $(k+1)!$

គេបាន $P_p = p(p+1)(p+2)...(p+k) = (k+1)!q\ ,q \in IN^*$

យើងនឹងស្រាយថាវាពិតចំពោះ $n = p+1$ គឺ P_{p+1} ចែកដាច់នឹង $(k+1)!$

គេមាន $P_{p+1} = (p+1)(p+2)(p+3)...(p+1+k)$

$P_{p+1} - P_p = (p+1)(p+2)...(p+k)[(p+1+k)-p]$

$P_{p+1} = P_p + (k+1)(p+1)(p+2)...(p+k)$

ដោយ $C(p+k,k) = \dfrac{(p+k)!}{k!p!} = \dfrac{(p+1)(p+2)...(p+k)}{k!}$

គេបាន $P_{p+1} = (k+1)!q + (k+1)!C(p+k,p)$ ពិត

ដូចនេះ $P_n = n(n+1)(n+2)...(n+k)$ ចែកដាច់នឹង $(k+1)!$ ។

លំហាត់ទី២០ (IMO 1997)

គេឱ្យពីចំនួនគត់វិជ្ជមាន $\mathbf{a}$ និង $\mathbf{b}$ ។ ពេលដែល $\mathbf{a^2+b^2}$ ចែកនឹង $\mathbf{a+b}$ នោះគេបានផលចែក $\mathbf{q}$ និងសំណល់ $\mathbf{r}$ ។

ចូរកំណត់គ្រប់គូ $\mathbf{(a\,,b)}$ ដោយដឹងថា $\mathbf{q^2+r=1977}$ ។

ដំណោះស្រាយ

កំណត់គ្រប់គូ $\mathbf{(a\,,b)}$

តាមវិធីចែកបែបអឺគ្លីតគេអាចសរសេរ $\mathbf{a^2+b^2=(a+b)q+r}$ **(*)**

ដែល $\mathbf{0\le r\le a+b-1}$ ។

គេមាន $\mathbf{r\le a+b-1}$ នោះ $\mathbf{q^2+r\le q^2+a+b-1}$

ឬ $\mathbf{q^2+a+b-1\ge 1977}$

ឬ $\mathbf{q^2+a+b\ge 1978}$ **(**)**

គេមាន $\mathbf{r\ge 0}$ នោះ $\mathbf{a^2+b^2=(a+b)q+r\ge(a+b)q}$

តាមវិសមភាព $\mathbf{a^2+b^2\ge\dfrac{(a+b)^2}{2}}$

គេបាន $\mathbf{(a+b)q\ge\dfrac{(a+b)^2}{2}}$ ឬ $\mathbf{a+b\le 2q}$

តាមវិសមភាព **(**)** គេអាចសរសេរ $\mathbf{q^2+2q\ge 1978}$

ឬ $\mathbf{(q+1)^2\ge 1979=44^2+43}$

គេទាញ $\mathbf{q+1\ge 45}$ ឬ $\mathbf{q\ge 44}$

ម្យ៉ាងទៀត $q^2 \le q^2 + r = 1977 = 44^2 + 43$

គេទាញបាន $q \le 44$ ។

ពីលទ្ធផលខាងលើនេះគេទាញបាន :

$q = 44$ ហើយ $r = 1977 - 44^2 = 41$

សមីការ (*) អាចសរសេរ $a^2 + b^2 = 44(a+b) + 41$

ឬ $(a-22)^2 + (b-22)^2 = 1009$

តាង $u = |a-22|$ និង $v = |b-22|$ ដែល $u , v \in IN$

គេបានសមីការ $u^2 + v^2 = 1009$ ។

យើងដឹងថាគ្រប់ការេនៃចំនួនគត់មានលេខចុងក្រោយ $\{0,1,4,9,5,6\}$

ហេតុនេះផលបូកការេនៃពីចំនួនគត់ដែលមានលេខចុងក្រោយស្មើ 9 លុះត្រាតែ

លេខចុងក្រោយនៃការេចំនួននីមួយស្មើរៀងគ្នា 4 និង 5 ឬ 5 និង 4

ឬ 0 និង 9 ឬ 9 និង 0 ។

ពីសមីការ $u^2 + v^2 = 1009 = 31^2 + 48$ គេទាញបាន $0 \le u \le 31$

ឧបមាថា $u \ge v$ នោះ $2u^2 \ge u^2 + v^2 = 1009$

គេទាញ $u^2 \ge \dfrac{1009}{2} = 22^2 + \dfrac{41}{2}$ ឬ $u \ge 23$

ហេតុនេះ $23 \le u \le 31$ ។

ដោយ u^2 ត្រូវមានលេខចុងក្រោយ $\{0 , 4 , 5 , 9\}$

នោះគេអាចជ្រើសរើសតម្លៃ $\mathbf{u}$ ជាដំបូងដូចខាងក្រោម :

$\mathbf{u} \in \{30, 28, 25, 23, 27\}$

ដោយ $\mathbf{u}^2 + \mathbf{v}^2 = 1009$ នោះ $\mathbf{v}^2 = \sqrt{1009 - \mathbf{u}^2}$

-បើ $\mathbf{u} = 30$ នោះ $\mathbf{v} = \sqrt{1009 - 900} = \sqrt{109}$ មិនយក

-បើ $\mathbf{u} = 28$ នោះ $\mathbf{v} = \sqrt{1009 - 784} = 15$ យក

-បើ $\mathbf{u} = 25$ នោះ $\mathbf{v} = \sqrt{1009 - 6225} = \sqrt{384}$ មិនយក

-បើ $\mathbf{u} = 23$ នោះ $\mathbf{v} = \sqrt{1009 - 529} = \sqrt{480}$ មិនយក

-បើ $\mathbf{u} = 27$ នោះ $\mathbf{v} = \sqrt{1009 - 729} = \sqrt{280}$ មិនយក

ដោយ $\mathbf{u}^2 + \mathbf{v}^2 = 1009$ ជាសមីការឆ្លុះហេតុនេះបើ $(\mathbf{a}, \mathbf{b})$ ជាចម្លើយ

របស់សមីការនោះ $(\mathbf{b}, \mathbf{a})$ ក៏ជាចម្លើយរបស់សមីការដែរ ។

គេទាញបានចម្លើយ $\mathbf{u} = 28$, $\mathbf{v} = 15$ ឬ $\mathbf{u} = 15$, $\mathbf{v} = 28$

-ករណី $\mathbf{u} = 28$, $\mathbf{v} = 15$ គេបាន $\begin{cases} |\mathbf{a} - 22| = 28 \\ |\mathbf{b} - 22| = 15 \end{cases}$

គេទាញបាន $\mathbf{a} = 50, \mathbf{b} = 37$ ឬ $\mathbf{a} = 50$, $\mathbf{b} = 7$ ។

-ករណី $\mathbf{u} = 15$, $\mathbf{v} = 28$ គេបាន $\begin{cases} |\mathbf{a} - 22| = 15 \\ |\mathbf{b} - 22| = 28 \end{cases}$

$\mathbf{a} = 37, \mathbf{b} = 50$ ឬ $\mathbf{a} = 7$, $\mathbf{b} = 50$ ។

ដូចនេះ $(\mathbf{a}, \mathbf{b}) = \{(50, 37); (37, 50); (7, 50); (50, 7)\}$ ។

លំហាត់ទី២១ (IMO 1960)

គេឱ្យ $\mathbf{N}$ ជាចំនួនមានលេខបីខ្ទង់ ។ គេដឹងថា $\mathbf{N}$ ចែកដាច់នឹង $\mathbf{11}$ ហើយ $\mathbf{N}$ ចែកនឹង $\mathbf{11}$ បានផលចែកស្មើនឹងផលបូកការេនៃលេខខ្ទង់របស់ $\mathbf{N}$ ។ ចូរកំណត់លេខទាំងបីខ្ទង់របស់ $\mathbf{N}$?

ដំណោះស្រាយ

កំណត់លេខទាំងបីខ្ទង់របស់ $\mathbf{N}$

តាង $\mathbf{N = abc = 100a + 10b + c}$ $\mathbf{(1)}$

គេបាន $\mathbf{\dfrac{N}{11} = a^2 + b^2 + c^2}$ ឬ $\mathbf{N = 11(a^2 + b^2 + c^2)}$ $\mathbf{(2)}$

តាម $\mathbf{(1)}$ គេអាចសរសេរ $\mathbf{N = 11(9a + b) + a - b + c}$

ដើម្បីឱ្យ $\mathbf{N}$ ចែកដាច់នឹង $\mathbf{11}$ លុះត្រាតែ $\mathbf{a - b + c}$ ចែកដាច់នឹង $\mathbf{11}$

ដោយ $\mathbf{1 \le a \le 9}$ និង $\mathbf{0 \le b \le 9}$, $\mathbf{0 \le c \le 9}$

គេបាន $\mathbf{-8 \le a - b + c \le 18}$ ហេតុនេះ $\mathbf{a - b + c = 0}$

ឬ $\mathbf{a - b + c = 11}$ ។

-ករណី $\mathbf{a - b + c = 0}$ ឬ $\mathbf{b = a + c}$

គេបាន $\mathbf{N = 11(9a + b) = 11(a^2 + b^2 + c^2)}$

ឬ $\mathbf{9a + a + c = a^2 + (a + c)^2 + c^2}$

ឬ $\mathbf{2a^2 + 2(c - 5)a + 2c^2 - c = 0}$ $\mathbf{(E_1)}$

ឌីសគ្រមីណង់សមីការ (E_1) គឺ $\Delta'_1=(c-5)^2-2(2c^2-c)$

ឬ $\Delta'_1=-3c^2-8c+25$ ។

សមីការ (E_1) មានឫសក្នុងសំណុំ $\mathbb{N}$ លុះត្រាតែ $\Delta'_1\geq 0$ និង Δ'_1

ជាការេប្រាកដ ។ ដោយ $\Delta'_1<0$ ចំពោះ $c\geq 2$ នោះ $c=0$, $c=1$

ដោយ Δ'_1 ជាការេប្រាកដតែក្នុងករណី $c=0$ មួយគត់

ហេតុនេះសមីការ (E_1) ក្លាយជា $2a^2-10a=0$ គេទាញបាន $a=5$

ហើយ $b=a+c=5+0=5$ ។

ដូចនេះ $a=5$, $b=5$, $c=0$ ហើយ $N=550$ ។

-ករណី $a-b+c=11$ ឬ $b=(a+c)-11$

គេបាន $N=11(9a+b+1)=11(a^2+b^2+c^2)$

$$9a+a+c-11+1=a^2+(a+c-11)^2+c^2$$

ឬ $2a^2+2(c-32)a+2c^2-23c+131=0$ (E_2)

ឌីសគ្រីមីណង់នៃសមីការ (E_2) គឺ :

$$\Delta'_2=(c-32)^2-2(2c^2-23c+131)$$

$$=-3c^2+14c-6$$

សមីការ (E_2) មានឫសក្នុងសំណុំ $\mathbb{N}$ លុះត្រាតែ $\Delta'_2\geq 0$ និង Δ'_1

ជាការេប្រាកដ ។

ដោយ $\Delta'_2<0$ ចំពោះគ្រប់ $c\geq 5$ នោះ $c=\{1,2,3,4\}$

ដោយ Δ'_2 ជាការេប្រាកដតែក្នុងករណី $\mathbf{c=3}$ មួយគត់

ហេតុនេះសមីការ $\mathbf{(E_1)}$ ក្លាយជា $\mathbf{2a^2-26a+80=0}$ គេទាញបាន

$\mathbf{a=5\ ;\ a=8}$ ។

- ចំពោះ $\mathbf{a=5\ ,\ c=3}$

នោះ $\mathbf{b=a+c-11=8-11=-3<0}$ មិនយក ។

-ចំពោះ $\mathbf{a=8\ ,\ c=3}$ នោះ $\mathbf{b=8+3-11=0}$ ។

ដូចនេះ $\mathbf{a=8\ ,\ b=0\ ,\ c=3}$ ហើយ $\mathbf{N=803}$ ។

លំហាត់ទី២២ (IMO 1978)

គេឱ្យចំនួនគត់វិជ្ជមាន $\mathbf{m}$ និង $\mathbf{n}$ ដែល $\mathbf{1 \le m < n}$ ។

ចូរកំណត់តម្លៃតូចបំផុតនៃ $\mathbf{m+n}$ ដើម្បីឱ្យចំនួន $\mathbf{1978^m}$ និង $\mathbf{1978^n}$

មានលេខបីខ្ទង់ចុងក្រោយបំផុតដូចគ្នា ?

ដំណោះស្រាយ

កំណត់តម្លៃតូចបំផុតនៃ $\mathbf{m+n}$

ដើម្បីឱ្យចំនួន $\mathbf{1978^m}$ និង $\mathbf{1978^n}$ មានលេខបីខ្ទង់ចុងក្រោយបំផុតដូចគ្នា

លុះត្រាតែផលសង $\mathbf{d = 1978^n - 1978^m}$ ចែកដាច់នឹង $\mathbf{1000}$ ។

គេមាន $\mathbf{d = 1978^m(1978^{n-m} - 1)}$ ចំពោះគ្រប់ $\mathbf{1 \le m < n}$ ។

ដោយ $\mathbf{1000 = 8 \times 125}$ ហើយ $\mathbf{1978 = 989 \times 2}$ នោះដើម្បីឱ្យ

$\mathbf{d = 1978^m(1978^{n-m} - 1)}$ ចែកដាច់នឹង $\mathbf{1000}$ លុះត្រាតែ

$\mathbf{1978^m}$ ចែកដាច់នឹង $\mathbf{8}$ និង $\mathbf{1978^{n-m} - 1}$ ចែកដាច់នឹង $\mathbf{125}$ ។

ចំនួន $\mathbf{1978^m = 989^m \times 2^m}$ ចែកដាច់នឹង $\mathbf{8}$ លុះត្រាតែ $\mathbf{m \ge 3}$

ហើយដោយ $\mathbf{1 \le m < n}$ នោះគេទាញបាន $\mathbf{n > m \ge 3}$ ។

គេមាន $\mathbf{1978 = 15 \times 125 + 103 = 125q_1 + 103}$ ដែល $\mathbf{q_1 = 15}$

ហើយ $\mathbf{1978^2 = (125q_1 + 103)^2 = 125q_2 + 103^2}$

តែដោយ $\mathbf{103^2 = 84 \times 125 + 109}$

នោះ $\mathbf{1978^2 = (q_2 + 84) \times 125 + 109}$

ឬ $1978^2 = 125q_3 + 109$ ដែល $q_3 = (q_2 + 4) \in IN*$

លើកជាការេ $1978^4 = (125q_3 + 109)^2$

$$= 125q_4 + 109^2$$

$$= 125(q_4 + 95) + 6$$

$$= 125q_5 + 6 \ ; \ q_5 = (q_4 + 95) \in IN*$$

ហេតុនេះគ្រប់ $p \in IN*$ គេបាន :

$$1978^{4p} = (125q_5 + 6)^p = 125q_6 + 6^p$$

ដោយ $6^p = (1+5)^p = \sum_{k=0}^{p} C(p,k).5^k$

$$= 1 + 5p + \frac{25p(p-1)}{2} + 125\sum_{k=3}^{p} C(p,k)5^{k-3}$$

គេបាន $1978^{4p} = 125q_7 + 1 + 5p + \dfrac{25p(p-1)}{2}$

ដែល $q_7 = q_6 + \sum_{k=3}^{p} C(o,k)5^{k-3}$ (ជាចំនួនគត់វិជ្ជមាន)

គេទាញ $1978^{4p} - 1 = 125q_7 + \dfrac{5p(5p-3)}{2}$

ដើម្បីឱ្យ$1978^{n-m} - 1$ ចែកដាច់នឹង 125 លុះត្រាតែ និងគ្រាន់តែឱ្យ

$n - m = 4p \ , p \in IN*$ និង $\dfrac{5p(5p-3)}{2}$ ចែកដាច់នឹង 125

ដើម្បីឱ្យ $\frac{5p(5p-3)}{2}$ ចែកដាច់នឹង 125 លុះត្រាតែ p ជាពហុគុណនៃ 25

ពោលគឺ $p = 25k\ ,\ \forall k \in IN^*$

ហើយដោយ $n - m = 4p$ នោះ $n - m = 100k$ និង $m \geq 3$

គេមាន $m + n = (n - m) + 2m \geq 100k + 6$ គ្រប់ $k \in IN^*$

ដូចនេះតម្លៃអប្បបរមានៃ $m + n$ គឺ 106 ដែលត្រូវនឹង $k = 1$ ។

លំហាត់ទី២៣ (IMO 1962)

ចូរកំណត់ចំនួនគត់ធម្មជាតិតូចបំផុត $\mathbf{n}$ ដោយដឹងថា ក្នុងប្រព័ន្ធដេស៊ីម៉ាល់ $\mathbf{n}$ មានលេខ $\mathbf{6}$ ជាលេខចុងក្រោយបំផុត ។ បើគេលុបលេខ $\mathbf{6}$ ចុងក្រោយនោះចោលហើយយកទៅសរសេរពីខាងមុខនៃលេខដែលនៅសល់នោះគេបានចំនួនមួយទៀតស្មើនឹង $\mathbf{4}$ នៃចំនួនដើម $\mathbf{n}$ ។

ដំណោះស្រាយ

កំណត់ចំនួនគត់ធម្មជាតិតូចបំផុត $\mathbf{n}$

សន្មតថា $\mathbf{n}$ ជាចំនួនមានលេខ $\mathbf{k+1}$ ខ្ទង់នោះគេបាន :

$\mathbf{n = \overline{a_k a_{k-1} \ldots a_1 6} = 10.N + 6}$ ដែល $\mathbf{N = \overline{a_k a_{k-1} \ldots a_2 a_1}}$

យក $\mathbf{p = \overline{6 a_k a_{k-1} \ldots a_1} = 6 \times 10^k + N}$ ។

តាមលក្ខខណ្ឌនៃសម្មតិកម្មគេបាន $\mathbf{p = 4 \times n}$

គេទាញ $\mathbf{6 \times 10^k + N = 4(10.N + 6)}$

គេទាញបាន $\mathbf{N = 2 \times \dfrac{10^k - 4}{13}}$ ។ តម្លៃ $\mathbf{k}$ ដំបូងដែលធ្វើឱ្យ $\mathbf{10^k - 4}$ ចែកដាច់នឹង $\mathbf{13}$ គឺ $\mathbf{k = 5}$ ហើយ $\mathbf{N = 2 \times \dfrac{10^5 - 4}{13} = 15384}$

ដូចនេះ $\mathbf{n = 10N + 6 = 153846}$ ។

លំហាត់ទី២៤

ចូរកំណត់គ្រប់គូចំនួនគត់ធម្មជាតិ (a,b) បើគេដឹងថា :

a^2+b^2 ចែកនឹង $a+b$ បានផលចែក 40 និងសំណល់ 53 ។

ដំណោះស្រាយ

កំណត់គ្រប់គូចំនួនគត់ធម្មជាតិ (a,b)

តាមវិធីចែកបែបអឺគ្លីតគេបាន :

$$a^2+b^2=40(a+b)+53$$
$$a^2+b^2-40a-40b=53$$
$$(a-20)^2+(b-20)^2=853$$

តាង $u=|a-20|\,;\ v=|b-20|$ ដែល $u,v\in\mathbb{N}^*$

គេបានសមីការ $u^2+v^2=853$ ។

យើងដឹងថាគ្រប់ការេនៃចំនួនគត់មានលេខចុងក្រោយ $\{0,1,4,9,5,6\}$

ហេតុនេះផលបូកការេនៃពីចំនួនគត់ដែលមានលេខចុងក្រោយស្មើ 3 លុះត្រាតែ

លេខចុងក្រោយនៃការេចំនួននីមួយស្មើរៀងគ្នា 4 និង 9 ឬ 9 និង 4 ។

ឧបមាថា $u\ge v$ នោះ $2u^2\ge u^2+v^2=853$

ឬ $u\ge\sqrt{\dfrac{853}{2}}>20$ ហើយ $u^2<u^2+v^2=853$ ឬ $u\le 29$

ហេតុនេះ $21\le u\le 29$ ហើយ u^2 ត្រូវមានលេខចុងក្រោយ 4 ឬ 9

នោះគេបាន $\mathbf{u=22}$ ឬ $\mathbf{u=23}$ ឬ $\mathbf{u=27}$ ឬ $\mathbf{u=28}$ ។

តាមសមីការ $\mathbf{u^2+v^2=853}$ គេទាញ $\mathbf{v=\sqrt{853-u^2}}$

-បើ $\mathbf{u=22}$ នោះ $\mathbf{v=\sqrt{853-484}=\sqrt{369}}$ មិនយក

-បើ $\mathbf{u=23}$ នោះ $\mathbf{v=\sqrt{853-529}=\sqrt{324}=18}$

-បើ $\mathbf{u=27}$ នោះ $\mathbf{v=\sqrt{853-729}=\sqrt{124}}$ មិនយក

-បើ $\mathbf{u=28}$ នោះ $\mathbf{v=\sqrt{853-784}=\sqrt{69}}$ មិនយក

ដោយសមីការ $\mathbf{u^2+v^2=853}$ មានលក្ខណះឆ្លុះនោះគេទាញបានគូចម្លើយ

$\mathbf{u=23\ ,\ v=18}$ ឬ $\mathbf{u=18\ ,\ v=23}$

ដោយ $\mathbf{u=|a-20|\ ;\ v=|b-20|}$ នោះគេទាញបានគូចម្លើយ

$\mathbf{(a,b)=(38,43)\ ;\ (43,38)}$ ។

លំហាត់ទី២៥ **(Singapore National Mathematical Olympiad 2009)**

ចូរកំណត់គ្រប់ចំនួនគត់វិជ្ជមាន $\mathbf{m}$ និង $\mathbf{n}$ ដែលផ្ទៀងផ្ទាត់សមីការ

$\mathbf{3.2^m + 1 = n^2}$ ។

ដំណោះស្រាយ

កំណត់ចំនួនគត់វិជ្ជមាន $\mathbf{m}$ និង $\mathbf{n}$:

សមីការ $\mathbf{3.2^m + 1 = n^2}$ សមមូល $\mathbf{2^m = \frac{(n+1)(n-1)}{3}}$ **(*)**

សមីការនេះមានចម្លើយក្នុង $\mathbf{IN^*}$ លុះត្រាតែ $\mathbf{\frac{n+1}{3}}$ ឬ $\mathbf{\frac{n-1}{3}}$ ជាចំនួនគត់ ។

-ករណី $\mathbf{\frac{n-1}{3}}$ ជាចំនួនគត់ :

ដោយអង្គទីមួយនៃសមីការ **(*)** ជាកត្តាស្វ័យគុណនៃ **2** និង

$\mathbf{\frac{n-1}{3} < n+1}$ នោះគេត្រូវ ឱ្យ $\mathbf{n+1 = \frac{n-1}{3}.2^k}$

ឬ $\mathbf{n = \frac{2^k+3}{2^k-3} = 1 + \frac{6}{2^k-3}}$ ដែល $\mathbf{k \in IN}$

ដើម្បីឱ្យ $\mathbf{n \in IN^*}$ លុះត្រាតែ $\mathbf{\frac{6}{2^k-3} \in IN}$ នោះគេទាញបាន $\mathbf{k = 2}$

ហើយ $\mathbf{n = 7}$

ហើយតាម **(*)** គេបាន $\mathbf{2^m = \frac{8 \times 6}{3} = 2^4 \Rightarrow m = 4}$ ។

-ករណី $\frac{n+1}{3}$ ជាចំនួនគត់ :

ដោយអង្គទីមួយនៃសមីការ (*) ជាកត្តាស្វ័យគុណនៃ 2 និង

$n-1>\frac{n+1}{3}$ គ្រប់ $n\geq 2$

នោះគេត្រូវឱ្យ $n-1=\frac{n+1}{3}.2^k$ ឬ $n=-\frac{2^k+3}{2^k-3}$ ដែល $k\in IN$

ដើម្បីឱ្យ $n\in IN^*$ លុះត្រាតែ $-\frac{2^k+3}{2^k-3}\in IN^*$ នោះគេទាញបាន

$k=0$, $k=1$ ហើយ $n=2$, $n=5$ ។

. ចំពោះ $n=2$ តាម (*) គេបាន $2^m=1\Rightarrow m=0$

មិនយកព្រោះ $m\in IN^*$ ។

. ចំពោះ $n=5$ តាម (*) គេបាន $2^m=2^3\Rightarrow m=3$ ។

ដូចនេះ $m=3$, $n=5$ ឬ $m=4$, $n=7$ ។

លំហាត់ទី២៦ **(IMO 1967)**

គេឱ្យ $\mathbf{k}$, $\mathbf{m}$, $\mathbf{n}$ ជាចំនួនគត់ធម្មជាតិដោយដឹងថា $\mathbf{m+k+1}$ ជាចំនួនបឋមធំជាង $\mathbf{n+1}$ ។ គេយក $\mathbf{c_s = s(s+1)}$ ។

ចូរស្រាយថាផលគុណ :

$$(c_{m+1}-c_k)(c_{m+2}-c_k)(c_{m+3}-c_k)...(c_{m+n}-c_k)$$

ចែកដាច់នឹងផលគុណ $c_1.c_2.c_3...c_n$ ។

ដំណោះស្រាយ

ស្រាយថាផលគុណ :

$$(c_{m+1}-c_k)(c_{m+2}-c_k)(c_{m+3}-c_k)...(c_{m+n}-c_k)$$

ចែកដាច់នឹងផលគុណ $c_1.c_2.c_3...c_n$

តាង $P_n = \prod_{i=1}^{n}\left(c_{m+i}-c_k\right)$ និង $Q_n = \prod_{i=1}^{n}\left(c_i\right)$

គេមាន $c_x - c_y = (x-y)(x+y+1)$

គេបាន $P_n = \prod_{i=1}^{n}(m+i-k)(m+i+k+1)$

$$= \prod_{i=1}^{n}(m+i-k) \times \prod_{i=1}^{n}(m+i+k+1)$$

ឬ $P_n=\frac{(m+n-k)!}{(m-k)!}\times\frac{(m+n+k+1)!}{(m+k+1)!}$

ហើយ $Q_n=\prod_{i=1}^{n}\left[i(i+1)\right]=n!(n+1)!$

គេបាន $\frac{P_n}{Q_n}=\frac{(m+n-k)!(m+n+k+1)!}{n!(n+1)!(m-k)!(m+k+1)!}$

គេមាន $C_{m+n-k}^{n}=\frac{(m+n-k)!}{n!(m-k)!}$

និង $C_{m+n+k+1}^{n+1}=\frac{(m+n+k+1)!}{(n+1)!(m+k)!}$

នោះ $\frac{P_n}{Q_n}=\frac{1}{m+k+1}.C_{m+n-k}^{n}.C_{m+n+k+1}^{n+1}$

គេមាន C_{m+n-k}^{n} ជាចំនួនគត់

ហើយ $\frac{1}{m+k+1}C_{m+n+k+1}^{n+1}=\frac{(m+n+k+1)!}{(n+1)!(m+k)!(m+k+1)}$

$$=\frac{(m+n+k+1)!}{(n+1)!(m+k+1)!}$$

តាមសម្មតិកម្ម $m+k+1$ ជាចំនួនបឋមធំជាង $n+1$ នោះវាគ្មានកត្តារួមជាមួយនឹង $(n+1)!$ ហើយ$(m+n+k+1)!$ ចែកដាច់នឹង $(n+k+1)!$

តាមទ្រឹស្តីបទ Gauss គេបាន $C_{m+n+k+1}^{n+1}$ ចែកដាច់នឹង $m+k+1$

ដូចនេះ $(c_{m+1}-c_k)(c_{m+2}-c_k)(c_{m+3}-c_k)...(c_{m+n}-c_k)$

ចែកដាច់នឹងផលគុណ $c_1.c_2.c_3...c_n$ ។

លំហាត់ទី២៧ (IMO 2005)

គេឱ្យស្វ៊ីត $a_1, a_2, a_3, ...$ កំណត់ដោយ $a_n = 2^n + 3^n + 6^n - 1$

ចំពោះគ្រប់ចំនួនគត់វិជ្ជមាន n ។

ចូរកំណត់គ្រប់ចំនួនគត់វិជ្ជមានដែលបឋមទៅនឹងគ្រប់តួនៃស្វ៊ីត ។

ដំណោះស្រាយ

ចំនួនគត់វិជ្ជមានដែលបឋមទៅនឹងគ្រប់តួនៃស្វ៊ីតនេះមានតែមួយគត់គឺ 1 ។

យើងនឹងបង្ហាញថាគ្រប់ចំនួនបឋម p ចែកដាច់ a_n ចំពោះគ្រប់ចំនួនវិជ្ជមាន n ។

សម្គាល់ឃើញថាចំពោះ $p = 2$ និង $p = 3$ ចែកដាច់

$a_2 = 2^2 + 3^2 + 6^2 - 1 = 48$ ។

យើងឧបមាថា $p \geq 5$ ។ តាមទ្រឹស្តីបទ Fermat យើងមាន

$2^{p-1} \equiv 1 \pmod{p}$

$3^{p-1} \equiv 1 \pmod{p}$

$6^{p-1} \equiv 1 \pmod{p}$

នោះ $3.2^{p-1} + 2.3^{p-1} + 6^{p-1} \equiv 3 + 2 + 1 \equiv 6 \equiv 0 \pmod{6}$

ឬ $6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1) \equiv 0 \pmod{p}$

នោះ $6a_{p-2}$ ចែកដាច់នឹង p ។

ពីព្រោះតែ p បឋមទៅនឹង 6 នោះ a_{p-2} ចែកដាច់នឹង p ។

លំហាត់ទី២៨ (IMO Shortlist 2003)

ចូរកំណត់ចំនួនគត់វិជ្ជមាន k តូចជាងគេ ដោយដឹងថាមានចំនួនគត់

$x_1, x_2, x_3, ..., x_k$ ដែល $x_1^3 + x_2^3 + ... + x_k^3 = 2002^{2002}$ ។

ដំណោះស្រាយ

ចំនួនគត់វិជ្ជមាន k ដែលតូចជាងគេគឺ $k = 4$ ។

ជាដំបូងយើងនឹងបង្ហាញថា 2002^{2002} មិនអាចជាផលបូកនៃគូបបីចំនួន ។

គេមាន $2002 \equiv 4 \pmod 9$ នោះ $2002 \equiv 4^3 \equiv 1 \pmod 9$

គេបាន $2002^{2002} = (2002^3)^{67}.2004 \equiv 4 \pmod 9$

ម្យ៉ាងទៀត $x^3 \equiv 0, \pm 1 \pmod 9$ ចំពោះគ្រប់ចំនួនគត់ x

ហេតុនេះ $x_1^3 + x_2^3 + x_3^3$ ចែកនឹង 9 មិនអាចឱ្យសំណល់ស្មើ 4 បានទេ។

ដូចនេះ 2002^{2002} មិនអាចសរសេរជាផលបូកគូបប្រាកដនៃបីចំនួនគត់បានទេ។

យើងនឹងបង្ហាញថា 2002^{2002} អាចសរសេរជាផលបូកនៃគូបប្រាកដនៃបួនចំនួន

បាន ។ គេមាន $2002 = 1000 + 1000 + 1 + 1 = 10^3 + 10^3 + 1 + 1$

ដោយ $2002^{2002} = 2002^{2001} \times 2002$

$$= (2002^{667})^3(10^3 + 10^3 + 1 + 1)$$

$$= (2002^{667}.10)^3 + (2002^{667}.10)^3 + (2002^{667})^3 + (2002^{667})^3$$

ដូចនេះ $k = 4$ ។

លំហាត់ទី២៩

គេឱ្យចំនួនគត់វិជ្ជមាន $\mathbf{n}$ ។ យក $\mathbf{p(n)}$ ជាផលគុណនៃតួលេខមិនសូន្យនៃ $\mathbf{n}$ ។

(បើ $\mathbf{n}$ មានលេខតែមួយ នោះ $\mathbf{p(n)}$ ស្មើនឹងលេខនោះ)

គេយក $\mathbf{S = p(1) + p(2) + ... + p(999)}$ ។

តើកត្តាបឋមធំជាងគេនៃ $\mathbf{S}$ ស្មើប៉ុន្មាន ?

ដំណោះស្រាយ

កត្តាបឋមធំជាងគេនៃ $\mathbf{S}$

តាមបំរាប់ $\mathbf{p(n)}$ ជាផលគុណនៃតួលេខមិនសូន្យនៃ $\mathbf{n}$

បើ $\mathbf{n = \overline{abc}}$ នោះ $\mathbf{p(n) = p(\overline{abc}) = p(a)p(b)p(c)}$

ហើយ $\mathbf{p(n) = n}$ ចំពោះ $\mathbf{1 \le n \le 9}$ និង $\mathbf{p(0) = 1}$ ។

យក $\mathbf{T = p(0) + p(1) + ... + p(999)}$ នោះ $\mathbf{S = T - p(0) = T - 1}$

តាង $\mathbf{k = p(0) + p(1) + p(2) + ... + p(9) = 1 + 1 + 2 + ... + 9 = 46}$

គេបាន $\mathbf{T = \sum_{n=0}^{999} p(n) = \sum_{0\le a,b,c\le 9} p(\overline{abc}) = [\sum_{0\le a\le 9} p(a)]^3 = k^3}$

ហេតុនេះ $\mathbf{S = T - 1 = 46^3 - 1 = (46-1)(46^2 + 46 + 1) = 3^3 \times 5 \times 7 \times 103}$

ដូចនេះ $\mathbf{103}$ ជាកត្តាបឋមធំជាងគេរបស់ $\mathbf{S}$ ។

លំហាត់ទី៣០ (IMO 1976)

គេឱ្យស្វ៊ីត (u_n) កំណត់ដោយ :

$u_0 = 2\ ,\ u_1 = \frac{5}{2}, u_{n+1} = u_n({u_{n-1}}^2 - 2) - u_1$ ចំពោះ $n = 1, 2, ...$

ចូរបង្ហាញថាចំពោះគ្រប់ចំនួនគត់វិជ្ជមាន n គេមាន $[\,u_n] = 2^{\frac{2^n-(-1)^n}{3}}$

(ដែល $[x]$ តាងជាចំនួនគត់វិជ្ជមានតូចជាង x)

ដំណោះស្រាយ

បង្ហាញថា $[\,u_n] = 2^{\frac{2^n-(-1)^n}{3}}$

ជាដំបូងយើងគណនាតួ $u_2, u_3, u_4\ ,\ u_5$ គេបានលំនាំដូចខាងក្រោម :

$u_0 = 2 = 2^0 + \frac{1}{2^0}\ \ ,\ \ u_1 = \frac{5}{2} = 2^1 + \frac{1}{2^1}$

$u_2 = \frac{5}{2} = 2^1 + \frac{1}{2^1}\ ,\ \ u_3 = 2^3 + \frac{1}{2^3}$

$u_4 = 2^5 + \frac{1}{2^5}\ \ ,\ \ u_5 = 2^{11} + \frac{1}{2^{11}}$

យើងសង្កេតឃើញថាកន្សោម u_n មានរាងទូទៅ $u_n = 2^{V_n} + \frac{1}{2^{V_n}}$

ដែល (V_n) ជាស្វ៊ីតកំណត់ដោយ $(V_n): 0, 1, 1, 3, 5, 11, ...$

តាងស្វ៊ីត (w_n) ដែល $w_n = V_n + V_{n+1}$ គ្រប់ $n \geq 0$

គេបាន : $(W_n): 1 , 2 , 4,8,16,....$ នាំឱ្យ (W_n) ជាស្វ៊ីតធរណីមាត្រ

មានតួ $W_0 = 1$ និង រេសុង $q = 2$ ។

គេបាន $W_n = 2^n$ នោះ $V_{n+1} + V_n = 2^n$

គុណអង្គទាំងពីរនឹង $(-1)^{n+1}$ គេបាន :

$$(-1)^{n+1}V_{n+1} - (-1)^n V_n = (-1)^{n+1}2^n$$

គេបាន $\sum_{k=0}^{n-1}\left[(-1)^{k+1}V_{k+1} - (-1)^k V_k\right] = \sum_{k=0}^{n-1}\left[(-1)^{k+1}2^k\right]$

$$(-1)^n V_n - V_0 = \frac{(-1)^n 2^n - 1}{3}$$

ដោយ $V_0 = 0$ នោះ $V_n = \frac{(-1)^n 2^n - 1}{(-1)^n .3} = \frac{2^n - (-1)^n}{3}$

ដូចនេះ $[\, u_n] = 2^{\frac{2^n - (-1)^n}{3}} + 2^{-\frac{2^n - (-1)^n}{3}}$

ដោយ $2^n \equiv (-1)^n \pmod{3}$ នោះ $3 | 2^n - (-1)^n$

ហើយ $2^{-\frac{2^n - (-1)^n}{3}} < 1$ ដូចនេះ $[\, u_n] = 2^{\frac{2^n - (-1)^n}{3}}$ ។

លំហាត់ទី៣១ (IMO 2010)

ចូរកំណត់គ្រប់អនុគមន៍ $\mathbf{f : IR \to IR}$ ដោយដឹងថាសមភាព

$\mathbf{f(\lfloor x \rfloor y) = f(x) \lfloor f(y) \rfloor}$ ពិតជានិច្ចគ្រប់ $\mathbf{x, y \in IR}$ ។

($\lfloor \mathbf{a} \rfloor$ តាងឱ្យផ្នែកគត់នៃ $\mathbf{a}$) ។

ដំណោះស្រាយ

កំណត់គ្រប់អនុគមន៍ $\mathbf{f : IR \to IR}$

គ្រប់ $\mathbf{x, y \in IR}$ គេមានសមភាព

យក $\mathbf{x = 0}$ និង $\mathbf{y = 0}$ គេបាន $\mathbf{f(0) = f(0) \lfloor f(0) \rfloor}$

គេទាញ $\mathbf{f(0)(1 - \lfloor f(0) \rfloor) = 0}$ នោះ $\mathbf{f(0) = 0}$ ឬ $\mathbf{\lfloor f(0) \rfloor = 1}$

-ករណី $\mathbf{\lfloor f(0) \rfloor = 1}$

យក $\mathbf{y = 0}$ ជំនួសក្នុង **(*)** គេបាន $\mathbf{f(0) = f(x) \lfloor f(0) \rfloor}$

ឬ $\mathbf{f(x) = f(0)}$ នាំឱ្យ $\mathbf{f(x)}$ ជាអនុគមន៍ថេរ

តាង $\mathbf{f(x) = c}$ ជំនួសក្នុងសមីការ **(*)** គេបាន $\mathbf{c = c \lfloor c \rfloor}$

នោះ $\mathbf{c = 0}$, $\mathbf{\lfloor c \rfloor = 1}$ ។

ដូចនេះ $\mathbf{f(x) = 0}$ ឬ $\mathbf{f(x) = c}$ ដែល $\mathbf{c \in [1, 2)}$ (ព្រោះ $\mathbf{\lfloor c \rfloor = 1}$)

-ករណី $f(0)=0$

យក $x=y=1$ ជំនួសក្នុង (*) គេបាន $f(1)=f(1)\lfloor f(1)\rfloor$

នោះ $f(1)=0$ ឬ $\lfloor f(1)\rfloor=1$

ក. ចំពោះ $f(1)=0$ នោះយើងយក $x=1$ ជំនួសក្នុង (*) គេបាន

$f(y)=f(1)\lfloor f(y)\rfloor=0 \ \forall y\in IR$ ។

ខ. ចំពោះ $\lfloor f(1)\rfloor=1$ នោះយើងយក $y=1$ គេបាន $f(\lfloor x\rfloor)=f(x)$ (**)

យក $x=2$, $y=\frac{1}{2}$ ក្នុង (*) គេបាន $f(1)=f(2)\left\lfloor f(\frac{1}{2})\right\rfloor$

តែតាម (**) គេបាន $f(\frac{1}{2})=f(0)=0$ ហេតុនេះគេទាញបាន $f(1)=0$

មិនពិតព្រោះ $\lfloor f(1)\rfloor=1$ ។

សរុបមកគេបានចម្លើយ $f(x)=0 \ ,\forall x\in IR$

ឬ $f(x)=c$, $\forall x\in IR$ ដែល $1\le c<2$ ។

លំហាត់ទី៣២

គេដឹងថា $\mathbf{1002004008016032}$ មានកត្តាបឋម $p > 250000$

ចូរកំណត់កត្តាបឋមនោះ ។

ដំណោះស្រាយ

កំណត់កត្តាបឋម

ដោយជ្រើសរើស $a = 1000$, $b = 2$ គេបាន :

$$\begin{aligned}
1002004008016032 &= a^5 + a^4b + a^3b^2 + a^2b^3 + ab^4 + b^5 \\
&= \frac{a^6 - b^6}{a - b} \\
&= (a+b)(a^2+ab+b^2)(a^2-ab+b^2) \\
&= (1002)(1002004)(998004) \\
&= 4^2.1002.250501.k
\end{aligned}$$

ដែល $k < 250000$ នោះ $p = 250501$ ។

លំហាត់ទី៣៣ (IMO 1984)

ចូរកំណត់គូមួយនៃចំនួនគត់វិជ្ជមាន a,b ដោយដឹងថា :

$(i):\ \ ab(a+b)$ មិនចែកដាច់នឹង 7

$(ii):\ (a+b)^7-a^7-b^7$ ចែកដាច់នឹង 7^7 ។

ដំណោះស្រាយ

កំណត់គូមួយនៃចំនួនគត់វិជ្ជមាន a,b :

តាមរូបមន្តទ្វេធាញូតុនគេបាន :

$$(a+b)^7-a^7-b^7=7ab(a+b)(a^2+ab+b^2)^2$$

តាមបម្រាប់គេមាន $(i):\ \ ab(a+b)$ មិនចែកដាច់នឹង 7

ដូចនេះដើម្បីឱ្យ $(ii):\ (a+b)^7-a^7-b^7$ ចែកដាច់នឹង 7^7

លុះត្រាតែ a^2+ab+b^2 ចែកដាច់នឹង 7^3 ។

គេមាន $(a+b)^2>a^2+ab+b^2\geq 7^3$ នោះ $a+b\geq 19$

ដោយធ្វើការសាកល្បងជំនួស $a=1\ ,\ b=18$ នោះគេបាន :

$$a^2+ab+b^2=1^2+1\times 18+18^2=343=7^3$$

ដូចនេះគូ $a=1\ ,\ b=18$ ជាចម្លើយ ។

ម្យ៉ាងទៀតតាមទ្រឹស្តីបទអឺលែ :

បើ $GCD(a,n)=1$ នោះ $a^{\phi(n)}\equiv 1\ (\bmod n)$ ។

គេមាន $a^3-b^3=(a-b)(a^2+ab+b^2)$

ហេតុនេះដើម្បីឱ្យ a^2+ab+b^2 ចែកដាច់នឹង 7^3 លុះត្រាតែ

$a^3\equiv b^3\ (\bmod 7^3)$ និង $a-b$ ចែកមិនដាច់នឹង 7 ។

គេមាន $\phi(7^3)=7^3-7^2=6\times 7^2=3\times 98$ ។

បើ c ជាចំនួនគត់វិជ្ជមានចែកមិនដាច់នឹង 7 នោះគេបាន

$(c^{98})^3\equiv 1\ (\bmod 7^3)$ ។

ដូចនេះដើម្បីឱ្យ $a^3\equiv 1\ (\bmod\ 7^3)$ លុះត្រាតែ $a=c^{98}$

ឧទាហរណ៍ :

-បើគេយក $c=2$ នោះ $2^{98}\equiv 18\ (\bmod 7^3)$

ហេតុនេះ $\left(2^{98}\right)^3\equiv 18^3\equiv 1\quad(\bmod\ 7^3)$

ដូចនេះ $a=18$, $b=1$ ជាចម្លើយមួយ ។

-បើគេយក $c=3$ នោះ $3^{98}\equiv 324\ (\bmod 7^3)$

ហេតុនេះ $\left(3^{98}\right)^3\equiv 324^3\equiv 1\ (\bmod 7^3)$

ដូចនេះ $a=324$, $b=1$ ជាចម្លើយផ្សេងមួយទៀត ។

ឯកសារយោង

1. គណិតវិទ្យាថ្នាក់ទី១២ កំរិតខ្ពស់ (បោះពុម្ពលើកទី១ ឆ្នាំ២០១០)

2.គណិតវិទ្យាអូឡាំពិច (ភាគ១ នព្វន្ត) របស់លោក **លឹម សុវណ្ណវិចិត្រ**

3. **104 NUMBER THEORY PROBLEMS**
(Tutu Andreescu , Dorin Andrica , Zuming FenG)

4. **The theory of numbers an Introduction**
(Anthony A.Gioia)

5. **250 Problems in elementary number theory**
(Waclaw Sierpinski)

6. **Introduction to number theory**
(James E.Shokley)