الحسابيات

I- قابلية القسمة في $\mathbb{Z}$

1) تعريف:

ليكن a و b من $\mathbb{Z}$. نقول إن b يقسم a إذا وجد عدد k من $\mathbb{Z}$ بحيث $a=kb$. ونكتب b/a.

ملاحظات:

* إذا كان b/a نقول كذلك إن b قاسم ل a مضاعف ل b.
* مجموعة مضاعفات b هي $\{...,-2b,-b,0,b,2b,...\}$ يعني $\{kb/k\in\mathbb{Z}\}$ ونرمز لها ب: $b\mathbb{Z}$
* $(\forall a\in\mathbb{Z})\ 1/a$ (لأن $a=1.a$)
* $(\forall a\in\mathbb{Z})\ -1/a$ (لأن $a=-1.(-a)$)
* $(\forall a\in\mathbb{Z})\ a/0$ (لأن $0=0.a$)
* $0/0$ (لأن مثلا $0=0\times 2$)
* $(\forall a\in\mathbb{Z}^*)\ 0\times a$.

* ليكن $a\in\mathbb{Z}^*$ و $b\in\mathbb{Z}$ بحيث b/a
لدينا b/a إذن يوجد $k\in\mathbb{Z}$ بحيث $a=kb$
إذن: $|a|=|k||b|$
ولدينا $a\neq 0$ إذن $k\neq 0$ إذن $|k|\in\mathbb{N}^*$
يعني $|k|\geq 1$
إذن $|b||k|\geq|b|$
يعني $|a|\geq|b|$
إذن: $\begin{cases}a\neq 0\\ b/a\end{cases}\Rightarrow|b|\leq|a|$

* $(\forall a\in\mathbb{Z})\ a/|a|$.
$(\forall a\in\mathbb{Z})\ |a|/a$.

2) خاصيات قابلية القسمة:

1- ليكن $a\in\mathbb{Z}$ لدينا: $a=1.a$ إذن a/a.
إذن $(\forall a\in\mathbb{Z})\ a/a$
نقول إن علاقة قابلية القسمة انعكاسية.

2- ليكن a و b و c من $\mathbb{Z}$ بحيث $\begin{cases}a/b\\ b/c\end{cases}$
لدينا a/b إذن يوجد k من $\mathbb{Z}$ بحيث $b=ka$
ولدينا b/c إذن يوجد k' من $\mathbb{Z}$ بحيث $c=k'b$
أي $c=k'ka$
إذن a/c
إذن $(\forall(a,b,c)\in\mathbb{Z}^3)\begin{cases}a/b\\ b/c\end{cases}\Rightarrow a/c$
نقول إن العلاقة $(/)$ متعدية.

3- ليكن a و b من $\mathbb{Z}$ بحيث $\begin{cases}a/b\\ b/a\end{cases}$ و
لدينا a/b إذن يوجد k من $\mathbb{Z}$ بحيث $b=ak$
و b/a إذن يوجد k' من $\mathbb{Z}$ بحيث $a=bk'$
يعني $a=kk'a$
* إذ كان $a=0$ فإن $b=0$ إذن $a=b$
* إذا كان $a\neq 0$ فإن $kk'=1$
إذن $k/1$ ونعلم أن قواسم 1 هي 1 و -1.
إذن $k=1$ أو $k=-1$
إذا كان $k=1$ فإن $k'=1$
إذا كان $k=-1$ فإن $k'=-1$
إذن $\begin{cases}k=1\\ k'=1\end{cases}$ أو $\begin{cases}k=-1\\ k'=-1\end{cases}$
إذن $a=b$ أو $a=-b$ إذن $|a|=|b|$

خاصية:

*) العلاقة $(/)$ انعكاسية. يعني $(\forall a\in\mathbb{Z})\ a/a$

*) العلاقة $(/)$ متعدية. يعني: $(\forall(a,b,c)\in\mathbb{Z}^3)\begin{cases}a/b\\ b/c\end{cases}\Rightarrow a/c$

*) $(\forall(a,b)\in\mathbb{Z}^2)\begin{cases}a/b\\ b/a\end{cases}\Rightarrow|a|=|b|$

*) $(\forall(a,b)\in\mathbb{N}^2)\begin{cases}a/b\\ b/a\end{cases}\Rightarrow a=b$

نقول في هذه الحالة إن العلاقة $(/)$ تخالفية.

3) القسمة الأقليدية في $\mathbb{Z}$

a) القسمة الأقليدية في $\mathbb{N}$

مبرهنة:

ليكن $a\in\mathbb{N}$ و $b\in\mathbb{N}^*$
يوجد زوج وحيد $(q,r)\in\mathbb{N}\times\mathbb{N}$ بحيث: $\begin{cases}a=q.b+r\\ 0\leq r\leq b\end{cases}$

برهان:

ليكن $a\in\mathbb{N}$ و $b\in\mathbb{N}^*$

1- Existence:

نعتبر المجموعة: $A=\{k\in\mathbb{N}/kb\leq a\}$
* لدينا $0\in A$ إذن $A\neq\varnothing$
* ليكن $k\in A$ لدينا: $kb\leq a$
ولدينا $b\in\mathbb{N}^*$ يعني $b\geq 1$ أي $kb\geq k$
إذن $k\leq a$
إذن $(\forall k\in A)\ k\leq a$
إذن A مكبورة ب a.
* ولدينا $A\subset\mathbb{N}$. إذن A تقبل الأكبر عنصر. نضع $q=MaxA$
و $r=a-bq$
* لنبين أن (q,r) يحقق الشرطين:
لدينا $r=a-bq$ إذن $a=b.q+r$
لنبين أن $0\leq r\leq b$
لدينا $q=MaxA$ إذن $q\in A$ ومنه $qb\leq a$
يعني $a-qb\geq 0$
إذن $0\leq r$
لدينا $q=MaxA$ إذن $(q+1)\notin A$
إذن $(q+1)b\rangle a$
يعني $a\langle bq+b$
أي $a-bq\langle b$ يعني $r\langle b$

ومنه $0 \le r \le b$

إذن يوجد زوج $(q,r) \in \mathbb{N}\times\mathbb{N}$ بحيث: $\begin{cases} a = bq + r \\ 0 \le r < b \end{cases}$

2) L'unicité:

نفترض أنه يوجد زوجان (q',r') و (q,r) من $\mathbb{N}\times\mathbb{N}$ بحيث $\begin{cases} a = bq + r \\ 0 \le r < b \end{cases}$ و $\begin{cases} a = bq' + r' \\ 0 \le r' < b \end{cases}$

لدينا: $bq + r = bq' + r'$

$b(q - q') = r' - r$

إذن: $|b|.|q - q'| = |r' - r|$

ولدينا $\begin{cases} 0 \le r < b \\ 0 \le r < b \end{cases}$ يعني $\begin{cases} -b < -r \le 0 \\ 0 \le r' < b \end{cases}$

إذن: $-b < r' - r < b$

يعني: $|r' - r| < b$

يعني: $|b||q - q'| < b$

يعني: $b|q - q'| < b$

يعني: $|q - q'| < 1$

ولدينا $|q - q'| \in \mathbb{N}$ إذن $|q - q'| = 0$

يعني $q = q'$

ومنه $|r - r'| = 0$ يعني $r' = r$

إذن $(q,r) = (q',r')$

وبالتالي يوجد زوج وحيد $(q,r) \in \mathbb{N}\times\mathbb{N}$ يحقق $\begin{cases} a = bq + r \\ 0 \le r < b \end{cases}$

b) القسمة الأقليدية في $\mathbb{Z}$:

مبرهنة:

ليكن $a \in \mathbb{Z}$ و $b \in \mathbb{N}^*$

يوجد زوج وحيد (q,r) من $(\mathbb{Z}\times\mathbb{N})$ بحيث: $\begin{cases} a = q.b + r \\ 0 \le r < b \end{cases}$

برهان:

ليكن $a \in \mathbb{Z}$ و $b \in \mathbb{N}^*$

1) Existence:

* إذا كان $a \in \mathbb{N}$ فإنه يوجد زوج وحيد يحقق الشرط.
* إذا كان $a \in \mathbb{Z}^{*-}$ فإن $-a \in \mathbb{N}^*$

إذن يوجد زوج وحيد (q',r') من $(\mathbb{N}\times\mathbb{N})$ بحيث:

$\begin{cases} -a = bq' + r' \\ 0 \le r' < b \end{cases}$

لدينا $a = b(-q') - r'$

إذا كان $r' = 0$ فإن $a = b(-q)$

نضع $q = -q'$ و $r = 0$

إذا كان $r' \neq 0$

فإن $a = b(-q') - r'$

$= b(-q') - b + b - r'$

$a = b(-q' - 1) + (b - r')$

نضع $\begin{cases} r = b - r' \\ q = -q' - 1 \end{cases}$ لدينا $a = bq + r$

ولدينا $0 < r < b$

يعني $0 < b - r' < b$ إذن $0 < r < b$

إذن $0 < r < b$

* وبالتالي يوجد زوج (q,r) بحيث: $\begin{cases} a = bq + r \\ 0 \le r < b \end{cases}$

2) L'unicité:

بنفس الطريقة السابقة نبين أن الزوج (q,r) وحيد.

II) الموافقة بتردد n:

1) تعريف:

ليكن $n \in \mathbb{N}$ و a و b من $\mathbb{Z}$

نقول إن a يوافق b بتردد n إذا وفقط إذا كان $n/a-b$ ونكتب $a \equiv b[n]$

ملاحظة:

$$a \equiv b[n] \Leftrightarrow n/a-b$$
$$\Leftrightarrow (\exists k \in \mathbb{Z}) a-b = nk$$
$$\Leftrightarrow a = nk + b$$

2) خاصيات:

1- ليكن $n \in \mathbb{N}$

*) $(\forall a \in \mathbb{Z})\ a \equiv a[n]$

إذن علاقة الموافقة انعكاسية.

*) ليكن a و b من $\mathbb{Z}$ بحيث $a \equiv b[n]$

إذن $n/a-b$ يعني يوجد k من $\mathbb{Z}$ بحيث: $a-b = nk$

إذن $b-a = n(-k)$

إذن $n/a-b$ ومنه $b \equiv a[n]$

إذن $a \equiv b[n] \Rightarrow b \equiv a[n]$: علاقة الموافقة تماثلي.

*) ليكن a و b من $\mathbb{Z}$ بحيث: $\begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases}$

لدينا $a \equiv b[n]$ إذن $a-b = kn$ (1) مع k من $\mathbb{Z}$.

و $b \equiv c[n]$ إذن $b-c = k'n$ (2) مع $k' \in \mathbb{Z}$.

من (1) + (2) نستنتج $a-c = (k+k')n$ إذن $n/a-c$ أي $a \equiv c[n]$

إذن: $\begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases} \Rightarrow a \equiv c[n]$

علاقة الموافقة متعدية.

خاصية (1):

علاقة الموفقة انعكاسية تماثلية ومتعدية.

نقول إن علاقة الموافقة علاقة تكافؤ.

$(\forall (a,b,c) \in \mathbb{Z}^3)$ $*a \equiv a[n]$

يعني: $*a \equiv b[n] \Rightarrow b \equiv a[n]$

$*\begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases} \Rightarrow a \equiv c[n]$

خاصية (2):

ليكن $n \in \mathbb{N}^*$

كل عدد a من $\mathbb{Z}$ يوافق بتردد n باقي قسمته على n يعني إذا كان r هو باقي قسمة a على n فإن $a \equiv r[n]$.

برهان:

لدينا $\begin{cases} a = nq + r \\ 0 \le r < n \end{cases}$

إذن $a-r=nq$

ومنه $n/a-r$ إذن $a\equiv r[n]$

خاصية (3):

ليكن $n\in\mathbb{N}^*$ و a و b من $\mathbb{Z}$.

ليكن r باقي قسمة a على n و r' باقي قسمة b على n.

لدينا: $a\equiv b[n]\Leftrightarrow r=r'$

برهان:

لدينا: $\begin{cases}a=nq+r\\0\leq r<n\end{cases}$ و $\begin{cases}b=nq'+r'\\0\leq r'<n\end{cases}$

* نفترض أن $r=r'$

نعلم أن $\begin{cases}a\equiv r[n]\\b\equiv r'[n]\end{cases}$ و $\begin{cases}a\equiv r[n]\\b\equiv r[n]\end{cases}$

و $r=r'$ إذن $a\equiv b[n]$

* نفترض أن $a\equiv b[n]$ ولنبين أن $r=r'$

لدينا $\begin{cases}a\equiv r[n]\\b\equiv r[n]\\r=r'\end{cases}$ إذن $r\equiv r'[n]$

أي $r-r'=k.n$ مع $k\in\mathbb{Z}$

إذن $|r-r'|=|k|n$

ولدينا $\begin{cases}0\leq r<n\\0\leq r'<n\end{cases}$

إذن $-n<r-r'<n$

أي $|r-r'|<n$

يعني $|k|n<n$

إذن $|k|<1$

ولدينا $|k|\in\mathbb{N}$ إذن $k=0$

ومنه $r-r'=0$ إذن $r=r'$

خاصية (4):

ليكن $n\in\mathbb{N}$

1) $(\forall(a,b,c,d)\in\mathbb{Z}^4)\begin{cases}a\equiv b[n]\\c\equiv d[n]\end{cases}\Rightarrow\begin{cases}a+c\equiv b+d[n]\\a.c\equiv b.d[n]\end{cases}$

2) ليكن $b_n...b_2,b_1$ و $a_n...a_2a_1$ من $\mathbb{Z}$

$$(\forall i\in\{1,2,...,n\})\,a_i\equiv b_i[n]\Rightarrow\begin{cases}\sum_{i=1}^{n}a_i\equiv\sum_{i=1}^{n}b_i[n]\\\prod_{i=1}^{n}a_i\equiv\prod_{i=1}^{n}b_i[n]\end{cases}$$

3) $(\forall(a,b,c)\in\mathbb{Z}^3)\,a\equiv b[n]\Rightarrow\begin{cases}a+c\equiv b+c[n]\\a.c\equiv b.c[n]\end{cases}$

4) $(\forall(a,b)\in\mathbb{Z}^2)(\forall n'\in\mathbb{N}):a\equiv b[n]\Rightarrow a^{n'}\equiv b^{n'}[n]$

برهان: لنبرهن على (1)

نفترض أن $\begin{cases}a\equiv b[n]\\c\equiv d[n]\end{cases}$

* لدينا $a\equiv b[n]$ يعني $a-b=kn(1)$ $(k\in\mathbb{Z})$

و $c\equiv d[n]$ إذن $c-d=k'n(2)$ $(k'\in\mathbb{Z})$

من خلال (1) + (2) نجد:

$(a+c)-(b+d)=(k+k')n$

إذن $a+c\equiv b+d[n]$

* لدينا من (1): $c(a-b)=ckn$

ومن (2): $b(c-d)=bk'n$

وبجمع الطرفين: $ac-bd=n(ck+bk')$

إذن: $n/ac-bd$ ومنه $ac\equiv bd[n]$

ملاحظة: ليكن $n\in\mathbb{N}$ و a من $\mathbb{Z}$.

$(\forall k\in\mathbb{Z})\;\;a\equiv a+nk[n]$

تمرين تطبيقي:

1) لنبين أن: $(\forall n\in\mathbb{N})\;\;7/3^{2n}-2^n$

ملاحظة: $n/a\Leftrightarrow a\equiv 0[n]$

لدينا:

$3^2\equiv 9[7]$

$\equiv 9-7[7]$

$\equiv 2[7]$

إذن $3^2\equiv 2[7]$

إذن $3^{2n}\equiv 2^n[7]$

إذن $(\forall n\in\mathbb{N}):\;\;7/3^{2n}-2^n$

2) لنبين أن $17/3.5^{2n-1}+2^{3n-2}$ لكل n من $\mathbb{N}^*$

لدينا:

$5^{2n-1}=5^{2(n-1)+1}$

$=5^{2(n-1)}\times 5$

ولدينا :

$5^2\equiv 25[17]$

$\equiv 8[17]$

$5^2\equiv 2^3[17]$

إذن: $5^{2(n+1)}\equiv 2^{3(n-1)}[17]$

يعني: $5.5^{2(n-1)}\equiv 2^{3(n-1)}\times 5[17]$

يعني: $5^{2n-1}\equiv 2^{3(n-1)}\times 5[17]$

يعني: $3.5^{2n-1}\equiv 2^{3(n-1)}\times 15[17]$

يعني: $3.5^{2n-1}+2^{3n-2}\equiv 2^{3n-3}\times 15+2^{3n-2}[17]$

يعني: $3.5^{2n-1}+2^{3n-2}\equiv 2^{3n-3}(15+2)[17]$

يعني: $\equiv 2^{3n-3}(17)[17]$

إذن: $3.5^{2n-1}+2^{3n-2}\equiv 0[17]$

إذن $17/3.5^{2n-1}+2^{3n-2}$ $(\forall n\in\mathbb{N}^*)$

3) مجموعة أصناف تكافؤ:

a) تعريف:

ليكن $a\in\mathbb{N}$ وليكن $x\in\mathbb{Z}$

نسمي صنف تكافؤ x المجموعة التي نرمز لها ب $\bar{x}$ أو $\dot{x}$ والمعرفة بما يلي:

$$\bar{x}=\{y\in\mathbb{Z}/y\equiv x[n]\}$$

ونرمز لمجموعة هذه الأصناف ب: $\mathbb{Z}/n\mathbb{Z}$

$$\overline{x}=\{y\in\mathbb{Z}/\ y\equiv x[3]\}$$
$$=\{y\in\mathbb{Z}/\ y=x+3k/k\in\mathbb{Z}\}$$
إذن $\overline{x}=\{y\in\mathbb{Z}/\ y=x+3k/k\in\mathbb{Z}\}$
$$\overline{0}=\{3k/k\in\mathbb{Z}\}$$
$$=\{...,-9,-6,-3,0,3,6,9,...\}$$
$$\overline{1}=\{1+3k/k\in\mathbb{Z}\}$$
$$=\{...,-8,-5,-2,1,4,7,10,...\}$$
$$\overline{2}=\{2+3k/k\in\mathbb{Z}\}$$
$$=\{...,-7,-4,-1,2,5,8,11,...\}$$
$$\overline{3}=\{3+3k/k\in\mathbb{Z}\}$$
$$=\{...,-6,-3,0,3,6,9,...\}=\overline{0}$$

b) خاصيات:

1- ليكن $x\in\mathbb{Z}$ و $n\in\mathbb{N}$

$$\overline{x}=\{y\in\mathbb{Z}/\ y\equiv x[n]\}$$
$$y\in\overline{x}\Leftrightarrow y\equiv x[n]\Leftrightarrow y=x+nk/k\in\mathbb{Z}$$
إذن: $\overline{x}=\{x+nk/k\in\mathbb{Z}\}$

2- ليكن $n\in\mathbb{N}$ و x و y من $\mathbb{Z}$

لنبين أن: $\overline{x}=\overline{y}\Leftrightarrow x\equiv y[n]$

* $\Leftarrow$) نفترض أن $x\equiv y[n]$ ولنبين أن $\overline{x}=\overline{y}$

$$z\in\overline{x}\Leftrightarrow z\equiv x[n]$$
$$\Leftrightarrow z\equiv y[n]\ \ (x\equiv y[n])$$
$$\Leftrightarrow z\in\overline{y}$$
إذن $\overline{x}=\overline{y}$

* $\Rightarrow$) نفترض أن $\overline{x}=\overline{y}$ ولنبين أن $x\equiv y[n]$

لدينا $\overline{x}=\overline{y}$ إذن يوجد z من $\mathbb{Z}$ بحيث $z\in\overline{x}$ و $z\in\overline{y}$

إذن $\begin{cases}z\equiv x[n]\\ z\equiv y[n]\end{cases}$ إذن $x\equiv y[n]$

3- ليكن $n\in\mathbb{N}$ و x و y من $\mathbb{Z}$ بحيث $x\not\equiv y[n]$

لنبين أن: $\overline{x}\cap\overline{y}=\varnothing$

- نفترض أن $\overline{x}\cap\overline{y}\neq\varnothing$

إذن يوجد $z\in\overline{x}\cap\overline{y}$ إذن $\begin{cases}z\equiv x[n]\\ z\equiv y[n]\end{cases}$ إذن $x\equiv y[n]$

وهذا غير صحيح. إذن $\overline{x}\cap\overline{y}=\varnothing$

خاصية:

ليكن $n\in\mathbb{N}$ و x و y من $\mathbb{Z}$

1) $\overline{x}=\{x+nk/k\in\mathbb{Z}\}$

2) $\overline{x}=\overline{y}\Leftrightarrow x\equiv y[n]$

3) $\overline{x}\cap\overline{y}=\varnothing\Leftrightarrow x\not\equiv y[n]$

هذا يعني أن صنفي تكافؤ منطبقان أو منفصلان.

4- تحديد $\mathbb{Z}/n\mathbb{Z}$ مع $n\in\mathbb{N}^*$

لنبين أن $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},...,\overline{(n-1)}\}$

* لدينا:

$$\{\overline{0},\overline{1},\overline{2},...,\overline{(n-1)}\}\subset\mathbb{Z}/n\mathbb{Z}$$

* لنبين أن $\mathbb{Z}/n\mathbb{Z}\subset\{\overline{0},\overline{1},\overline{2},...,\overline{(n-1)}\}$

ليكن $\overline{x}\in\mathbb{Z}/n\mathbb{Z}$

نعتبر قسمة x على n. ليكن r هو باقي قسمة a على n

أي: $\begin{cases}x=nq+r\\ 0\leq r<n\end{cases}$

نعلم أن $x\equiv r[n]$ إذن $\overline{x}=\overline{r}$

ولدينا: $r\in\{0,1,2,...,n-1\}$

إذن $\overline{r}\in\{\overline{0},\overline{1},\overline{2},...,\overline{(n-1)}\}$

ومنه $\mathbb{Z}/n\mathbb{Z}\subset\{\overline{0},\overline{1},\overline{2},...,\overline{(n-1)}\}$

بالتالي: $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},...,\overline{(n-1)}\}$

* لنحدد $card\ \mathbb{Z}/n\mathbb{Z}$

ليكن r و r' من $\{0,1,2,...,n-1\}$ بحيث $r\neq r'$

لنبين أن $\overline{r'}\neq\overline{r}$

نفترض أن $\overline{r'}=\overline{r}$

يعني: $r\equiv r'[n]$

يعني: $|r-r'|=|k|n$ أي $r-r'=kn/k\in\mathbb{Z}$

ولدينا $\begin{cases}0\leq r<n\\ 0\leq r'<n\end{cases}$ إذن $|r-r'|<n$

يعني: $|k|n<n$

يعني $|k|<1$

ولدينا $|k|\in\mathbb{N}$ إذن $k=0$

ومنه $r=r'$ وهذا تناقض.

إذن $\overline{r'}\neq\overline{r}$

بالتالي: $Card\ \mathbb{Z}/n\mathbb{Z}=n$

خاصية:

ليكن $n\in\mathbb{N}^*$

(*) $Card\ \mathbb{Z}/n\mathbb{Z}=n$

(*) $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},...,\overline{(n-1)}\}$

c) الجمع والضرب في $\mathbb{Z}/n\mathbb{Z}$:

ليكن X و Y من $\mathbb{Z}/n\mathbb{Z}$

نفترض أن: $X=\overline{x}=\overline{x'}$

و: $Y=\overline{y}=\overline{y'}$

إذن $\begin{cases}x\equiv x'[n]\\ y\equiv y'[n]\end{cases}$

إذن $\begin{cases}x+y\equiv x'+y'[n]\\ xy\equiv x'y'[n]\end{cases}$

إذن $\begin{matrix}\overline{x+y}=\overline{x'+y'}\\ \overline{xy}=\overline{x'y'}\end{matrix}$

نضع إذن $\begin{cases}x+y=\overline{x+y}\\ xy=\overline{xy}\end{cases}$

يعني: $\begin{cases}\overline{x}+\overline{y}=\overline{x+y}\\ \overline{x}.\overline{y}=\overline{xy}\end{cases}$

تعريف:

تعريف الجمع والضرب في $\mathbb{Z}/n\mathbb{Z}$ بما يلي:

$$\overline{x}+\overline{y}=\overline{x+y}$$
$$\overline{x}.\overline{y}=\overline{xy}$$

مثال:

ضع جدول الجمع والضرب في $\mathbb{Z}/6\mathbb{Z}$

– لدينا: $\mathbb{Z}/6\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}$

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

تمرين تطبيقي:

*) حل في $\mathbb{Z}$ المعادلة: $4x\equiv 2[6]$

لدينا في $\mathbb{Z}/6\mathbb{Z}$:

$$4x\equiv 2[6]\Leftrightarrow \overline{4x}=\overline{2}$$
$$\Leftrightarrow \overline{4}.\overline{x}=\overline{2}$$
$$\Leftrightarrow \begin{cases}\overline{x}=\overline{2}\\ \overline{x}=\overline{5}\end{cases}$$ (من خلال الجدول)
$$\Leftrightarrow x\equiv 2[6] \text{ أو } x\equiv 5[6]$$
$$\Leftrightarrow x=2+6k \text{ أو } x=5+6k\ (k\in\mathbb{Z})$$

إذن: $S=\{2+6k,5+6k/k\in\mathbb{Z}\}$

*) حل في $\mathbb{Z}$ المعادلة:

$$3x\equiv 1[5]$$

لدينا في $\mathbb{Z}/5\mathbb{Z}$

$$3x\equiv 1[5]\Leftrightarrow \overline{3x}=\overline{1}$$
$$\Leftrightarrow \overline{3}.\overline{x}=\overline{1}$$

لدينا: $\mathbb{Z}/5\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$

بالتعويض نستنتج أن:

$\overline{x}=\overline{2}$

يعني $x\equiv 2[5]$

يعني $x=2+5k$

إذن $S=\{2+5k/k\in\mathbb{Z}\}$

خاصيات:

*) الجمع والضرب وتباديليان في $\mathbb{Z}/n\mathbb{Z}$

*) الضرب توزيعي بالنسبة للجمع في $\mathbb{Z}/n\mathbb{Z}$

*) $\overline{0}$ هو العنصر المحايد بالنسبة للجمع.

*) $\overline{1}$ هو العنصر المحايد بالنسبة للضرب.

*) $\overline{x}$ يقبل مقابل $\overline{-x}$ ونرمز له ب $-\overline{x}$.

نلخص هذه الخاصيات بقولنا $\left(\mathbb{Z}/n\mathbb{Z},+,\times\right)$ حلقة تبادلية وواحدية.

برهان:

– لنبين أن $(+)$ تجميعي.

لدينا:

$$\overline{x}+(\overline{y}+\overline{z})=\overline{x}+\overline{(y+z)}$$
$$=\overline{x+(y+z)}=\overline{(x+y)+z}$$
$$=\overline{(x+y)}+\overline{z}$$

إذن $\overline{x}+(\overline{y}+\overline{z})=(\overline{x}+\overline{y})+\overline{z}$

ملاحظة:

$(\forall(x,y)\in\mathbb{Z}^2)\ \overline{x}.\overline{y}=\overline{0}\Rightarrow \overline{x}=\overline{0}$ أو $\overline{y}=\overline{0}$

مثل مضاد:

في $\mathbb{Z}/6\mathbb{Z}$: لدينا $\overline{3}.\overline{4}=\overline{0}$

و $\overline{4}\neq\overline{0}$ و $\overline{3}\neq\overline{0}$

III– القاسم المشترك الأكبر.

1) تعريف:

ليكن a و b من $\mathbb{Z}^*$

نعتبر المجموعة $A=\{d\in\mathbb{N}^*/d/a \text{ و } d/b\}$

*) لدينا $A\neq\varnothing$ (لأن $1\in A$)

*) لدينا: $(\forall d\in A)\ d/a$

إذن $d\le|a|$

إذن A مكبورة ب $|a|$

*) ولدينا $A\subset\mathbb{N}$

إذن A تقبل أكبر عنصر.

نضع $\delta=\max A$

δ يسمى القاسم المشترك الأكبر ل a و b

ونكتب $\delta=a\wedge b$.

تعريف:

ليكن a و b من $\mathbb{Z}^*$

نسمي القاسم المشترك الأكبر ل a و b أكبر قاسم موجب قطعا مشترك بين a و b. نرمز له ب $a\wedge b$ أو $a\triangle b$ أو $\gcd\{a,b\}$

مثال:

لنحدد $36\wedge 48$

القواسم الموجبة ل 48 هي: 1, 2, 3, 4, 6, 8, 12, 16, 24, 48.

القواسم الموجبة ل 36 هي: 1, 2, 3, 4, 6, 9, 12, 18, 36.

إذن القواسم المشتركة: 1, 2, 3, 4, 6, 12. إذن $36\wedge 48=12$

ملاحظة:

*) $a\wedge b=b\wedge a$

*) إذا كان $b\neq 0$ نضع $0\wedge b=|b|$

*) $0\wedge 0$ غير معرف.

*) إذا كان a/b فإن $a\wedge b=|a|$

*) $a\wedge b=d$ يعني $\begin{cases}d/a\\d/b\end{cases}$ وإذا كان $\begin{cases}d'/a\\d'/b\end{cases}$ فإن $d'\leq d$

2) خاصيات:

1- ليكن a و b من $\mathbb{Z}^*$

ليكن $d=a\wedge b$

لنبين أنه يوجد (u,v) من $\mathbb{Z}\times\mathbb{Z}$ بحيث $d=au+bv$

* نعتبر المجموعة: $A=\{au+bv/u,v\in\mathbb{Z}\}$

- لدينا $A\neq 0$ لأن $n=a^2+b^2\in A$

- لدينا A مصغورة ب 1.

- ولدينا $A\subset\mathbb{N}$

إذن لدينا p صاغر ل A

و $p\in A$ إذن يوجد (u,v) من $\mathbb{Z}^2$ بحيث $p=au+bv$

* لنبين أن $d=p$

- لدينا $\begin{cases}d/a\\d/b\end{cases}$ إذن $\begin{cases}d/au\\d/bv\end{cases}$ إذن $d/au+bv$ يعني d/p

إذن $|d|\leq|p|$ يعني $d\leq p$ (1)

- لنبين أن p/a

نعتبر القسمة الأقليدية ل a على p يعني $\begin{cases}a=pq+r\\0\leq r\langle p\end{cases}$

لنبين أن $r=0$: نفترض أن $r\neq 0$ إذن $0\langle r\langle p$

لدينا:
$$\begin{aligned}r&=a-pq\\&=a-(au+bv)q\\&=a(1-uq)+b(-Vq)\end{aligned}$$

لدينا $\begin{cases}r=aU+bV\\r\in\mathbb{N}^*\end{cases}$ إذن $r\in A$ ولدينا $r\langle p$ و $p=\sin A$

هذا تناقض. إذن $r=0$.

ومنه p/a

وبنفس الطريقة نبين أن p/b

إذن p قاسم مشترك ل a و b و $a\wedge b=d$

إذن $p\leq d$ (2)

من (1) و (2) نستنتج أن: $p=d$

إذن: $d=au+bv$

خاصية (1):

ليكن a و b من $\mathbb{Z}^*$

إذا كان $a\wedge b=d$ فإنه يوجد زوج (u,v) من $\mathbb{Z}^2$ بحيث:

$$d=au+bv$$

ملاحظة:

ليكن a و b من $\mathbb{Z}^*$ وليكن $d=a\wedge b$

* العدد d هو أصغر عدد طبيعي غير منعدم يكتب على شكل $d=au+bv$.

* الزوج (u,v) ليس وحيدا.

2- ليكن a و b من $\mathbb{Z}^*$ و $d=a\wedge b$

لنبين أن: $\begin{cases}d'/a\\d'/b\end{cases}\Leftrightarrow d'/d$

*) $\Leftarrow$) نفترض أن d'/d

ولدينا $\begin{cases}d/a\\d/b\end{cases}$ إذن: $\begin{cases}d'/a\\d'/b\end{cases}$

*) $\Rightarrow$) نفترض أن $\begin{cases}d'/a\\d'/b\end{cases}$

لدينا $d=a\wedge b$ إذن $d=au+bv$ مع $(u,v)\in\mathbb{Z}^2$

لدينا $\begin{cases}d'/a\\d'/b\end{cases}$ أن $\begin{cases}d'/au\\d'/bv\end{cases}$ إذن $d'/au+bv$ يعني d'/d

خاصية (2):

ليكن a و b من $\mathbb{Z}^*$ و $d=a\wedge b$

لدينا: $\begin{cases}d'/a\\d'/b\end{cases}\Leftrightarrow d'/d$

وهذا يعني أن القواسم المشتركة ل a و b هي بالضبط قواسم d

$$\begin{cases}d'/a\\d'/b\end{cases}\Leftrightarrow d'/a\wedge b$$

ملاحظة:

ليكن a و b من $\mathbb{Z}^*$

*) لدينا: $|a|\wedge|b|=a\wedge|b|=|a|\wedge b=a\wedge b$

برهان:

لنبين أن: $|a|\wedge|b|=a\wedge b$

نضع $d=a\wedge b$ و $d'=|a|\wedge|b|$

- لدينا $d=a\wedge b$ إذن $\begin{cases}d/a\\d/b\end{cases}$

ولدينا: $\begin{cases}a/|a|\\b/|b|\end{cases}$ إذن $\begin{cases}d/|a|\\d/|b|\end{cases}$ يعني $d/|a|\wedge|b|$

يعني d/d' (1)

- لدينا $d'=|a|\wedge|b|$ إذن $\begin{cases}d'/|a|\\d'/|b|\end{cases}$ ولدينا $\begin{cases}|a|/a\\|b|/b\end{cases}$

إذن $\begin{cases}d'/a\\d'/b\end{cases}$ يعني $d'/a\wedge b$ يعني d'/d (2)

من (1) و (2) نستنتج أن $|d|=|d'|$

إذن: $a\wedge b=|a|\wedge|b|$

*) إذن يلغي البحث عن طرق تحديد القاسم المشترك الأكبر لعددين موجبين.

5) خوارزمية اقليدس:

خاصية (1):

ليكن a و b من $\mathbb{N}^*$

إذا كان r هو باقي قيمة a على b يعني: $\begin{cases}a=bq+r\\0\leq r\langle b\end{cases}$

فإن $a\wedge b=b\wedge r$

برهان:

لدينا $\begin{cases} a=bq+r \\ 0\le r<b \end{cases}$ لنبين أن $a\wedge b=b\wedge r$

نضع: $d=a\wedge b$ و $d'=b\wedge r$. لنبين أن $d=d'$

- لدينا: $\begin{cases} d'/a \\ d'/r \end{cases}$ إذن $\begin{cases} d'/bq \\ d'/r \end{cases}$ إذن $d'/bq+r$

يعني d'/a

إذن $\begin{cases} d'/a \\ d'/b \end{cases}$ يعني $d'/a\wedge b$ يعني d'/d (1)

- لدينا $\begin{cases} d/a \\ d/b \end{cases}$ إذن $\begin{cases} d/a \\ d/bq \end{cases}$ إذن $d/a-bq$ يعني

d/r إذن $\begin{cases} d/b \\ d/r \end{cases}$ يعني: $d/b\wedge r$ يعني

d/d' (2)

من (1) و (2) نستنتج أن $|d|=|d'|$

وبما أن d و d' وجبان قطعا فإن $d=d'$

يعني $a\wedge b=b\wedge r$

ملاحظة:

في البرهان م نستعمل كون $0\le r<b$. إذن بصفة عامة:

إذا كان $a=bq+r$ فإن $a\wedge b=b\wedge r$

مثال:

لنحدد $416\wedge 76$

لدينا

416	76
36	5

إذن $416=76\times 5+36$

إذن $416\wedge 76=76\wedge 36$

ولدينا: $76=2\times 36+4$

إذن $76\wedge 36=36\wedge 4$

ولدينا $36=9\times 4+0$

إذن: $4/36$ ومنه: $36\wedge 4=|4|=4$

بالتالي: $76\wedge 36=4$

أي: $416\wedge 76=4$

نلخص هذا في الجدول التالي:

416	76	36	4
	5	2	9
36	4	0	

تعميم:

ليكن b من $\mathbb{N}^*$ بحيث $a>b$

* نقوم بقسمة a على b: $a=bq_1+r_1$, $0\le r_1<b$

- إذا كان $r_1=0$ فإن b/a إذن $a\wedge b=b$
- إذا كان $r_1\neq 0$ فإن $a\wedge b=b\wedge r_1$

نقوم بقسمة b على r_1: $b=r_1q_2+r_2$ ، $0\le r_2<r_1$

- إذا كان $r_2=0$ فإن r_1/b إذن $b\wedge r_1=r_1$
- إذا كان $r_2\neq 0$ فإن $b\wedge r_1=r_1\wedge r_2$

وهكذا نتائج القسمات المتتالية حتى نحصل على باقي منعدم (ومن الضروري الحصول على باقي منعدم لأن هذه البواقي موجبة وتناقصية قطعا).

نفترض أن r_{n+1} أول باقي منعدم.

يعني: $r_{n+1}=0$ و $r_n\neq 0$

$a=bq_1+r_1$	$0\le r_1<b$	$a\wedge b=b\wedge r_1$
$b=r_1q_2+r_2$	$0\le r_2<r_1$	$b\wedge r_1=r_1\wedge r_2$
$r_{n+1}=r_nq_{n+1}+r_{n+1}$	لدينا $r_{n+1}=0$	إذن r_n/r_{n-1}

ومنه $r_{n-1}\wedge r_n=r_n$

إذن $a\wedge b=r_n$ وهو آخر باقي غير منعدم.

خاصية:

ليكن b و a من $\mathbb{N}^*$

القاسم المشترك الأكبر هو آخر باقي غير منعدم في القسمات المتتالية (خوارزمية أقليدس).

ملاحظة:

نلخص هذه النتائج في الجدول:

a	b	r_1	r_2	...	...	...
	q_1	q_2	q_3			
r_1	r_2	r_3	−	−	r_n	0

مثال:

لنحدد: $792\wedge 36$

لدينا:

792	36	16	4
	21	2	4
16	4	0	

إذن: $792\wedge 36=4$

4) الأعداد الأولية فيما بينها:

a) تعريف:

ليكن b و a من $\mathbb{Z}^*$

نقول إن a و b أوليان فيما بينهما إذا وفقط إذا كان $a\wedge b=1$

مثال: $9\wedge 4=1$

إذن 9 و 4 أوليان فيما بينهما.

b) خاصيات:

مبرهنة (1): (مبرهنة Bezout)

ليكن b و a من $\mathbb{Z}^*$

$$a\wedge b=1\Leftrightarrow (\exists (u,v)\in\mathbb{Z}^2):1=au+bv$$

برهان:

$\Rightarrow$) نفترض أن $a\wedge b=1$ من خلال خاصية سابقة نستنتج أن:

$(\exists (u,v)\in\mathbb{Z}^2):1=au+bv$

$\Leftarrow$) نفترض أن $(\exists (u,v)\in\mathbb{Z}^2):1=au+bv$ لنبين أن $a\wedge b=1$

نضع $a\wedge b=d$ ولنبين أن: $d=1$

لدينا: $\begin{cases} d/a \\ d/b \end{cases}$ إذن $\begin{cases} d/au \\ d/bv \end{cases}$ إذن $d/au+bv$ أو $d=-1$

يعني $d/1$

إذن $d=1$ أو $d=-1$

ولدينا $d>0$ إذن $d=1$ يعني $a\wedge b=1$.

مثال:

ليكن $n\in\mathbb{Z}$ مع $n\neq 0$ و $n\neq -1$. لنحدد: $(n+1)\wedge n$

لدينا: $1(n+1)-1(n)=1$

إذن $(n+1)\wedge(n)=1$

مبرهنة (2)

ليكن c عنصرا من $\mathbb{Z}^*$
لدينا $ac \wedge bc = |c|(a \wedge b)$.

برهان:

نضع $d' = a \wedge b$ و $a \neq bc$

لنبين أن $d = |c|d'$

لدينا $\begin{cases} d'/a \\ d'/b \end{cases}$ ولدينا $|c|/c$ يعني $\begin{cases} |c|d'/ac \\ |c|d'/bc \end{cases}$

$|c|d'/ac \wedge bc$

يعني $|c|d'/d$ (1)

لدينا: $d' = a \wedge b$ إذن: $(\exists (u,v) \in \mathbb{Z}^2): \quad d' = au + bv$

إذن $|c|d' = |c|au + |c|bv$

ولدينا: $d = ac \wedge bc$

إذن $\begin{cases} d/ac \\ d/bc \end{cases}$ إذن $\begin{cases} d/a|c| \\ d/b|c| \end{cases}$ إذن $\begin{cases} d/a|c|u \\ d/b|c|v \end{cases}$

إذن $d/a|c|u + b|c|v$

يعني: $d/d'|c|$ (2)

من (1) و (2) نستنتج أن: $d = |c|d'$ (لأنهما عددان موجبان)

مبرهنة (3):

ليكن a و b عنصرين من $\mathbb{Z}^*$ و $d \in \mathbb{N}^*$

$$a \wedge b = d \Leftrightarrow \begin{cases} d/a \text{ et } d/b \\ \frac{a}{d} \wedge \frac{b}{d} = 1 \end{cases}$$

برهان:

$\Leftarrow$) نفترض أن $\begin{cases} d/a \\ d/b \end{cases}$ و $\frac{a}{d} \wedge \frac{b}{d} = 1$ ولنبين $a \wedge b = d$

لدينا: $a \wedge b = d.\frac{a}{d} \wedge d.\frac{b}{d} = |d|\left(\frac{a}{d} \wedge \frac{b}{d}\right)$

$= d.1 = d$

إذن: $a \wedge b = d$

$\Rightarrow$) نفترض أن $a \wedge b = d$ لنبين أن $\begin{cases} d/a \\ d/b \end{cases}$ و $\frac{a}{d} \wedge \frac{b}{d} = 1$

- لدينا $a \wedge b = d$ إذن $\begin{cases} d/a \\ d/b \end{cases}$
- لدينا $a \wedge b = d$ إذن $(\exists (u,v) \in \mathbb{Z}^2): \quad d = au + bv$

يعني: $d = d.\frac{a}{d}u + d\frac{b}{d}v$

يعني: $d = d\left(\frac{a}{d}u + \frac{b}{d}v\right)$

يعني: $1 = \frac{a}{d}u + \frac{b}{d}v$

وحسب (Bezout) نستنتج أن $\frac{a}{d} \wedge \frac{b}{d} = 1$

ملاحظة:

ليكن a و b عنصرين من $\mathbb{Z}^*$ و $d = a \wedge b$

نضع: $\begin{cases} a = da' \\ b = db' \end{cases}$ لدينا $\begin{cases} a' = \frac{a}{d} \\ b' = \frac{b}{d} \end{cases}$ إذن $a' \wedge b' = \frac{a}{d} \wedge \frac{b}{d} = 1$

إذن إذا كان $\begin{cases} d = a \wedge b \\ a = da' \\ b = db' \end{cases}$ فإن $a' \wedge b' = 1$

مبرهنة (4):

ليكن a و b و c عناصر من $\mathbb{Z}^*$

لدينا: $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Rightarrow a \wedge bc = 1$

برهان:

لدينا $a \wedge b = 1$ إذن: $(\exists (u,v) \in \mathbb{Z}^2): (1) \quad 1 = au + bv$

و $a \wedge c = 1$ إذن: $(\exists (u',v') \in \mathbb{Z}^2): (2) \quad 1 = au' + cv'$

من (1) . (2) نستنتج أن:

$1 = a^2uu' + acuv' + bau'v + bcvv'$

يعني $1 = a(auu' + cuv' + bu'v) + bc(vv')$

$1 = aU + bcV$

وحسب (Bezout) نستنتج أن:

$a \wedge bc = 1$

ملاحظة:

الاستلزام العكسي صحيح.

استنتاج:

1- ليكن a و b_1 و b_2 ... و b_n عناصر من $\mathbb{Z}^*$

$(\forall i \in \{1,2,...,n\}) a_1b_i = 1 \Rightarrow a \wedge \prod_{i=1}^{n} b_i = 1$

2- ليكن a و b عنصرين من $\mathbb{Z}^*$

$(\forall (m,n) \in \mathbb{N}^2) \quad a \wedge b = 1 \Rightarrow a^n \wedge b^n = 1$

مبرهنة (5): (مبرهنة Gauss)

ليكن a و b و c عناصر من $\mathbb{Z}^*$

لدينا: $\begin{cases} a/c \\ b/c \\ a \wedge b = 1 \end{cases} \Rightarrow ab/c$

ملاحظة:

إذا كان $a \wedge b \neq 1$ فإن الاستلزام خاطئ:

مثلا: $\begin{cases} 6/12 \\ 4/12 \end{cases}$ لكن 6.4×12

برهان:

لدينا a/c إذن $\exists k \in \mathbb{Z} \quad c = ak$

و b/c يعني b/ak

ولدينا $a \wedge b = 1$ إذن حسب (Gauss) نستنتج أن b/k

إذن $k = bk'$

ومنه $c = abk'$

إذن ab/c

ملاحظة:

$$\begin{cases} a_1/b \\ a_2/b \\ a_n/b \end{cases} \Rightarrow a_1.a_2...a_n/b$$

أولية فيما بينها مثنى مثنى

مبرهنة (7):

ليكن a و b من $\mathbb{Z}^*$ و $n \in \mathbb{N}^*$

$$\begin{cases} ax \equiv ay[n] \\ a \wedge n = 1 \end{cases} \Rightarrow x \equiv y[n]$$

ملاحظة:

إذا كان $a \wedge n \neq 1$ فإن الاستلزام خاطئ.

مثل: $3.2 \equiv 3.4[6]$ لكن $2 \neq 4[6]$

برهان:

لدينا $ax \equiv ay[n]$ يعني $n/ax-ay$

يعني $n/a(x-y)$

ولدينا $a \wedge n = 1$ إذن حسب (Gauss) نستنتج أن: $n/x-y$

يعني $x \equiv y[n]$

إذن: $\begin{cases} ax \equiv ay[n] \\ a \wedge n = 1 \end{cases} \Rightarrow x \equiv y[n]$

5) حل المعادلة $ax+by=c$ في $\mathbb{N}$.

a) أمثلة:

مثال 1: لنحل في $\mathbb{Z}^2$ المعادلة $(1)\ 3x-4y=1$.

* لدينا $3 \wedge 4 = 1$ إذن حسب Bezout: يوجد زوج (u,v) من $\mathbb{Z}$.

بحيث: $3u+4v=1$

يعني: $3u-4(-v)=1$

إذن $(u,-v)$ حل للمعادلة (1)

وبالتالي المعادلة (1) تقبل حلا على الأقل.

* لنبحث عن حل خاص للمعادلة (1).

نلاحظ أن $(-1,-1)$ حل للمعادلة (1).

* لنحدد جميع الحلول:

ليكن (x,y) حل للمعادلة (1).

لدينا $3(-1)-4(-1)=1$ (2)

ولدينا $(-1,-1)$ حل إذن: $3(-1)-4(-1)=1$ (3)

من $(3)-(2)$ نستنتج أن: $3(x+1)-4(y+1)=0$

يعني $3(x+1)=4(y+1)$

إذن $3/4(y+1)$

ولدينا $3 \wedge 4 = 1$ إذن حسب (Gauss) لدينا: $3/y+1$.

يعني $y+1=3k$ يعني: $y=3k-1$

وبالتعويض في (2) نحصل على:

$3x-4(3k-1)=1$

يعني $3x=12k-3$

يعني $x=4k-1$

إذن: $(k \in \mathbb{Z})$ $\begin{cases} y=3k-1 \\ x=4k-1 \end{cases}$

عكسا

نلاحظ أنه تم حساب x انطلاقا من المعادلة (2) إذن x و y يحققان المعادلة (1)

وبالتالي: $S=\{(4k-1;3k-1)/k \in \mathbb{Z}\}$

مثال 2:

لنحل في $\mathbb{Z}^2$ المعادلة: $(E): 67x+57y=2$

* لنحدد $67 \wedge 57$

67	57	10	7	3	1
	1	5	1	2	3
10	7	3	1	0	

إذن $67 \wedge 57 = 1$

وحسب Bezout فإنه يوجد (u,v) بحيث $67u+57v=1$

يعني $67(2u)+57(2v)=2$

إذن الزوج $(2u,2v)$ حل للمعادلة (E).

إذن (E) تقبل حلا على الأقل.

* لنبحث عن حل خاص للمعادلة (E).

خوارزمية أقليدس تمكننا من البحث عن حل خاص إذا لم يكن هناك حل واضح.

لدينا: $(1)\ 67=1\times57+10$

$(2)\ 57=5\times10+7$

$(3)\ 10=1\times7+3$

$(4)\ 7=2\times3+1$

نضع $a=67$ و $b=57$

من (1) نحصل على: $10=a-b$

من (2) نحصل على: $7=5(a-b)+7$ أي $7=6b-5a$

من (3) نحصل على: $a-b=(6b-5a)+3$ أي $3=6a-7b$

من (4) نحصل على: $6b-5a=2(6a-7b)+1$ أي $-17a+20b=1$

يعني: $67(-17)+57(20)=1$

يعني: $67(-34)+57(40)=2$

إذن $(-34,40)$ حل للمعادلة (E).

* لنحدد جميع حلول المعادلة (E).

ليكن (x,y) حل للمعادلة.

إذن $(1)\ 67x+57y=2$

ولدينا $(-34,40)$ حل إذن:

$(2)\ 67(-34)+57(40)=2$

من $(1)-(2)$ نستنتج أن:

$67(x+34)+57(y-40)=0$

يعني $67(x+34)=-57(y-40)$

إذن $57/67(x+34)$

وبما أن $57 \wedge 67 = 1$ فإن $57/x+34$

أي $x+34=57k$

إذن $x=57k-34$

وبالتعويض في (1) نجد:

$57y=-67\times57k+2280$

ومنه $y=-67k+40$

إذن: $\begin{cases} x = 57k + 34 \\ y = -67k + 40 \end{cases} (k \in \mathbb{Z})$

عكسيا:

(x, y) يحققان (E) لأنه تم تحديد y انطلاقا من (E)

* وبالتالي: $S = \{(57k + 34; -67k + 40) / k \in \mathbb{Z}\}$

b) تعميم:

نعتبر المعادلة (E) $ax + by = c$ مع $a \neq 0$ و $b \neq 0$

- نضع $d = a \wedge b$

1- إذا كان $d \times c$

نفترض أن المعادلة تقبل حلا (x, y).

إذن $ax + by = c$

ولدينا $\begin{cases} d/a \\ d/b \end{cases}$ إذن $\begin{cases} d/ax \\ d/by \end{cases}$ إذن $d/ax + by$ يعني d/c

وهذا تناقض. إذن المعادلة ليس لها حل.

2- إذا كان d/c :

نضع: $\begin{cases} a = da' \\ b = db' \\ c = dc' \end{cases}$ مع $a' \wedge b' = 1$

إذن (E) تصبح: $a'dx + b'dy = c'd$

أي $(E')\ a'x + b'y = c'$

* لدينا $a' \wedge b' = 1$

إذن يوجد (u, v) بحيث $a'u + b'v = 1$

يعني: $a'(c'u) + b'(c'v) = c'$

إذن $(c'u, c'v)$ حل للمعادلة (E').

إذن (E) لها حل.

* لنبحث عن حل خاص:

باستعمال خوارزمية أقليدس إذا لم يكن هناك حل واضح.

نفترض أن (x_0, y_0) حل خاص للمعادلة.

يعني (1) $a'x_0 + b'y_0 = c'$

* ليكن (x, y) حل للمعادلة يعني: (2) $a'x + b'y = c'$

من (1) و (2) نجد: $a'(x - x_0) + b'(y - y_0) = 0$

يعني: $a'(x - x_0) = -b(y - y_0)$

إذن $b'/a'(x - x_0)$

ولدينا $a' \wedge b' = 1$ إذن $b'/(x - x_0)$ يعني $x = b'k + x_0$

وبالتعويض في (E') نجد

$a'(b'k + x_0) + b'y = c'$

يعني: $b'y = c' - a'x - a'b'k$

ولدينا من (1): $a'x_0 = c' - b'y_0$

إذن $b'y = c' - c' + b'y_0 - a'b'k$

إذن $y = -a'k + y_0$

عكسيا: (x, y) يحقق (E) لأنه تم حساب y انطلاقا من (E)

وبالتالي: $S = \{(b'k + x_0, -a'k + y_0) / k \in \mathbb{Z}\}$

IV) القاسم المشترك الأكبر لعدة أعداد:

1- تعريف:

ليكن $a_1, a_2 ... a_n$ أعداد غير منعدمة

نسمي القاسم المشترك الأكبر لهذه الأعداد أكبر قاسم مشترك موجب قطعا لهذه الأعداد. ونرمز له ب $a_1 \wedge a_2 \wedge ... \wedge a_n$

2- خاصيات:

خاصية (1):

ليكن $a_1, a_2 ... a_n$ من $\mathbb{Z}^*$

$$d = a_1 \wedge a_2 \wedge ... \wedge a_n \Rightarrow \exists (u_1, u_2, ..., u_3) \in \mathbb{Z}^n / d = \sum_{i=1}^{n} a_i u_i$$

خاصية (2):

ليكن: $d = a_1 \wedge a_2 \wedge ... \wedge a_n$

قواسم d هي بالضبط القواسم المشتركة للأعداد a_i

يعني: $\begin{cases} d'/a_1 \\ d'/a_2 \\ d'/a_n \end{cases} \Leftrightarrow d'/a_1 \wedge a_2 \wedge ... \wedge a_n = d$

خاصية (3):

ليكن a, b, c من $\mathbb{Z}^*$

لدينا: $a \wedge b \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c)$

هذا يعني أنه عنك حساب القاسم المشترك الأكبر لعدة أعداد يمكن تعويض كل اثنين بالقاسم المشترك الأكبر لهما.

3) الأعداد الأولية فيما بينها:

a) تعريف:

نقول إن الأعداد $a_1 ... a_n$ من $\mathbb{Z}^*$ أولية فيما بينها إذا وفقط إذا كان $a_1 \wedge a_2 \wedge ... \wedge a_n = 1$

لاحظة:

لا يجب الخلط بين أعداد أولية فيما بينها وأعداد أولية فيما بينها مثنى مثنى.

مثلا: الأعداد $9, 12, 16, 4, 30$ أولية فيما بينها.

لكنها ليست أولية فيما بينها مثنى مثنى.

b) خاصيات:

خاصية (1):

ليكن $a_1, a_2 ... a_n$ من $\mathbb{Z}^*$

$$a_1 \wedge a_2 \wedge ... \wedge a_n = 1 \Leftrightarrow \exists (u_1, u_2, ..., u_n) \in \mathbb{Z}^n / 1 = \sum_{i=1}^{n} a_i u_i$$

خاصية (2):

ليكن $a_1, a_2 ... a_n$ من $\mathbb{Z}^*$ و $d > 0$

لدينا: $d = a_1 \wedge a_2 \wedge ... \wedge a_n \Leftrightarrow \begin{cases} d/a_1 \ et \ d/a_2 ... d/a_n \\ \frac{a_1}{d} \wedge \frac{a_2}{d} \wedge ... \wedge \frac{a_n}{d} = 1 \end{cases}$

V) المضاعف المشترك الأصغر:

1) تعريف:

ليكن a, b من $\mathbb{Z}^*$

ونعتبر المجموعة $E = \{m \in \mathbb{N}^* / \ a/m \ et \ b/m\}$

- لدينا $E \neq \varnothing$ (لأن $|ab| \in E$).
- E مصغورة ب 0.
- $E \subset \mathbb{N}$

إذن E تقبل الأصغر عنصر نضع: $q = \min E$

q يسمى المضاعف المشترك الأصغر ل a و b. ونكتب $q = a \vee b$

1) تعريف:

ليكن b و a من $\mathbb{Z}^*$

نسمي المضاعف المشترك الأصغر للعددين a و b أصغر مضاعف موجب مشترك بين a و b. ونرمز له ب $a\vee b$.

* ملاحظة:

$m=a\vee b$ يعني: $\begin{cases}a/m\\ b/m\end{cases}$

وإذا كان m' مضاعف مشترك ل a و b فإن $m\leq m'$

$b\vee a=a\vee b$

$a\vee a=|a|$

إذا كان a/b فإن $a\vee b=|b|$

2) خاصيات:

خاصية (1):

ليكن a و b من $\mathbb{Z}^*$ و $m=a\vee b$

مضاعفات m هي بالضبط المضاعفات المشتركة ل a و b.

يعني: $\begin{cases}a/m'\\ b/m'\end{cases}\Leftrightarrow m=a\vee b/m'$

برهان:

$\Leftarrow$) نفترض أن m/m'

ولدينا $\begin{cases}a/m\\ b/m\end{cases}$ إذن $\begin{cases}a/m'\\ b/m'\end{cases}$

$\Rightarrow$) نفترض أن: a/m' و b/m' لنبين أن m/m'

نعتبر قسمة m' على m. يعني: $\begin{cases}m'=mq+r\\ 0\leq r<m\end{cases}$

لنبين أن $r=0$

نفترض العكس. يعني $r\neq 0$

إذن $0<r<m$

لدينا: $r=m'-mq$

ولدينا $\begin{cases}a/m\\ a/m'\end{cases}$ إذن $a/m'-mq$ يعني a/r

وبنفس الطريقة نجد b/r

إذن r مضاعف مشترك ل a و b.

وجدنا أن r مضاعف مشترك ل a و b ويحقق $0<r<m$ وهذا تناقض لأن $a\vee b=m$

إذن $r=0$ ومنه m/m'.

ملاحظة:

$|a|\vee|b|=|a|\vee b=a\vee|b|=a\vee b$

خاصية (2):

ليكن a و b من $\mathbb{Z}^*$

لدينا: $(a\wedge b).(a\vee b)=|ab|$

برهان:

نضع $\begin{cases}d=a\wedge b\\ m=a\vee b\end{cases}$

نضع $\begin{cases}a=\alpha d\\ b=\beta d\end{cases}$ مع $\alpha\wedge\beta=1$

ونضع $\begin{cases}m=\gamma a\\ m=\varphi b\end{cases}$

ولدينا: $\gamma a=\varphi b$ يعني: $\gamma\alpha d=\varphi\beta d$

يعني: $\gamma\alpha=\varphi\beta$

إذن $\alpha/\varphi\beta$

ولدينا $\alpha\wedge\beta=1$ إذن α/φ يعني: $\varphi=dk$

إذن: $m=\varphi b$

يعني: $m=\alpha k\beta d$ إذن $\alpha\beta d/m$ (1)

* لنبين أن $m/\alpha\beta d$:

لدينا: $\alpha\beta d=\alpha b$ و $\alpha\beta d=\beta a$ إذن $\begin{cases}b/\alpha\beta d\\ a/\alpha\beta d\end{cases}$ إذن

$a\vee b/\alpha\beta d$

يعني: $m/\alpha\beta d$ (2)

من (1) و (2) نستنتج أن:

$|m|=|\alpha\beta d|$

يعني: $m=|\alpha\beta d|$

يعني: $dm=|\alpha\beta d^2|$

يعني: $dm=|ab|$

ومنه: $(a\wedge b).(a\vee b)=|ab|$

خاصية (3):

ليكن a و b و c من $\mathbb{Z}^*$

لدينا: $ac\vee bc=|c|(a\vee b)$

برهان:

نعلم أن: $(ac\wedge bc)(ac\vee bc)=|ac.bc|$

يعني: $|c|(a\wedge b).(ac\vee bc)=|ab|.|c|^2$

يعني: $(a\wedge b).(ac\vee bc)=(a\wedge b)(a\vee b)|c|$

يعني: $(ac\vee bc)=|c|.(a\vee b)$

تمرين:

ليكن a و b من $\mathbb{Z}^*$ و $m>0$

$$m=a\vee b\Leftrightarrow\begin{cases}a/m\ \ et\ \ b/m\\ \dfrac{m}{a}\wedge\dfrac{m}{b}=1\end{cases}$$

3) المضاعف المشترك الأصغر لعدة أعداد:

تعريف:

ليكن $a_1, a_2 ... a_n$ من $\mathbb{Z}^*$

المضاعف المشترك الأصغر لهذه الأعداد هو أصغر مضاعف موجب مشترك بين هذه الأعداد.

خاصية:

ليكن $a_1, a_2 ... a_n$ من $\mathbb{Z}^*$ و $m=a_1\vee a_2\vee ...\vee a_n$

مضاعفات m هي بالضبط المضاعفات المشتركة للأعداد a_i.

VI) الأعداد الأولية:

1) تعاريف:

تعريف (1):

ليكن a من $\mathbb{Z}^*$.

نسمي قاسم فعلي ل a كل قاسم d ل a يخالف $-1,1,-a,a$

يعني $d\notin\{a,-a,1,-1\}$.

تعريف (2):

ليكن $p\in\mathbb{Z}^*-\{-1,1\}$

نقول إن p أولي إذا وفقط إذا كان لا يقبل أي قاسم فعلي يعني إذا كان يقبل 4 قواسم بالضبط هي $-p;p;-1;1$

أمثلة:

*) $-1,1,0$ ليست أولية.

*) 4 ليس أولي لأن 2 قاسم فعلي ل 4.

*) 2, 3, 5, 7 أعداد أولية.

2) خاصية (1):

خاصية (1):

ليكن $a\in\mathbb{Z}^*-\{-1,1\}$ غير أولي.

أصغر قاسم فعلي موجب ل a يكون أوليا.

برهان:

لتكن A مجموعة القواسم الفعلية الموجبة ل a.

- لدينا $A\neq 0$ (لأن a ليس أولي وبالتالي يقبل قاسم فعلي موجب)
- لدينا A مصغورة ب 0.
- $A\subset\mathbb{N}$

إذن A تقبل الأصغر عنصر. نضع $p=\min A$

- لنبين أن p أولي:

لدينا p قاسم فعلي ل a إذن $p\neq 0$ و $p\notin\{-1,1\}$ لأن $a\neq 0$

لنبين أن p لا يقبل قاسما فعليا.

نفترض أن p يقبل قاسما فعليا p'

لدينا $\begin{cases}|p'|/p\\ p/a\end{cases}$ إذن $|p'|/a$

- لدينا $|p'|/p$ إذن $|p'|\leq|p|$

يعني: $|p'|\leq p$

ولدينا $\begin{cases}p'\neq p\\ p'\neq -p\end{cases}$ إذن $|p'|<p$

ولدينا p/a إذن $|p|\leq|a|$ أي $p\leq|a|$

إذن $|p'|<|a|$

إذن $|p'|\neq|a|$

ولدينا $|p'|\neq 1$

إذن $|p'|$ قاسم فعلي ل a

ولدينا $|p'|<p$

وجدنا قاسما فعليا موجبا ل a ويحقق $|p'|<p$

وهذا تناقض لأن p أصغر قاسم فعلي موجب.

ومنه p لا يقبل قاسما فعليا.

وبالتالي p أولي.

ملاحظة:

كل عدد $a\in\mathbb{Z}^*-\{-1,1\}$ غير أولي يقبل قاسم فعلي أولي موجب.

خاصية (2):

مجموعة الأعداد الأولية غير منتهية.

برهان:

لتكن P مجموعة الأعداد الأولية الموجبة.

لنبين أن P غير مكبورة.

نفترض العكس. يعني P مكبورة.

- لدينا $P\neq\varnothing$ (لأن $2\in P$).
- $P\subset\mathbb{N}$

إذن P تقبل الأكبر عنصر. نضع: $q=\max P$

- نضع $p=q!+1$

لنبين أن p أولي:

نفترض العكس. يعني p يقبل قاسما فعليا أولي موجب p_0.

لدينا $P=\{2,3,5,7,...,q\}$

ولدينا p_0 أولي موجب إذن $p_0\in P$

إذن p_0 هو أحد عوامل $q!$ إذن $p_0/q!$

ولدينا p_0/p

إذن $p_0/p-q!$

يعني $p_0/1$

يعني $p_0=1$ أو $p_0=-1$

وهذا تناقض لأن p_0 أولي.

إذن p أولي.

- وجدنا إذن p أولي و $p>q$ وهذا تناقض لأن q هو أكبر عدد أولي.

بالتالي P غير مكبورة.

ومنه P غير منتهية.

3) طريقة عملية لتحديد الأعداد الأولية:

ملاحظة:

إذا كان p عدد أولي فإن $-p$ أولي. وبالتالي يكفي البحث عن طرق لتحدد الأعداد الأولية الموجبة.

خاصية:

ليكن $n\in\mathbb{N}^*-\{1\}$

إذا كان n غير أولي فإنه يوجد عدد أولي p بحيث $\begin{cases}p/n\\ p^2\leq n\end{cases}$

برهان

نفترض أن n غير أولي.

لدينا $n\in\mathbb{N}^*-\{1\}$

ليكن p أصغر قاسم فعلي موجل ل n.

من خلال الخاصية (1) لدينا p أولي.

إذن p أولي و p/n

لنبين أن $p^2\leq n$

لدينا: p/n يعني $n=kp$

لنبين أن k قاسم فعلي ل n

لدينا $k\neq 0$ و $k>0$

- نفترض أن $k=1$ إذن $n=p$ وهذا تناقض لأن: n غير أولي و p أولي.

إذن $k\neq 1$

- نفترض أن $k=n$ إذن $p=1$ وهذا تناقض لأن p أولي.

إذن $k\neq n$

- ولدينا $k>0$ إذن $k\neq -1$ و $k\neq n$

إذن k قاسم فعلي موجب ل n.

- وبما أن p هو اصغر قاسم فعلي موجب ل n.

فإن: $p\leq k$

يعني: $p^2\leq kp$

يعني $p^2\leq n$

- إذن يوجد p أولي بحيث: $\begin{cases}p/n\\ p^2\leq n\end{cases}$

ملاحظة:

1- ليكن $n\in\mathbb{N}^*-\{1\}$

إذا أردنا أن نتحقق هل n أولي، نتبع ما يلي:

+ نعتبر الأعداد الأولية p التي تحقق $p^2\leq n$

- إذا كان أحد هذه الأعداد يقسم n فإن n غير أولي لأنه يقبل قاسما فعليا.

- إذا كانت جميع هذه الأعداد لا تقسم n فإن n أولي.

مثال:

- لنحدد جميع الأعداد الأولية أصغر من 100.

بالنسبة للأعداد الأصغر من 100، الأعداد الأولية p التي يمكن أن تحقق $p^2\leq n$ هي 2, 3, 5, 7.

إذن الأعداد الأولية الأصغر من 100 هي الأعداد التي لا تقبل القسمة على 2, 3, 5, 7 إضافة إلى الأعداد 2, 3, 5, 7.

- إذن هذه الأعداد هي:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

2- ليكن $n\in\mathbb{N}^*-\{1\}$.

لكي نتحقق هل n أولي يمكن اتباع الخوارزمية التالية.

نقوم بقسمة n على الأعداد الأولية p انطلاقا من 2 على التوالي، ونقف عند إحدى الحالات:

- إذا أصبح الخارج q أصغر من p قطعا، والباقي غير منعدم فيكون في هذه الحالة العدد n أولي.

- إذا حصلنا على باقي منعدم. فيكون n غير أولي.

برهان:

*) إذا حصلنا على باقي منعدم فإن n يقبل قاسما فعليا.

إذن n غير أولي.

*) نفتر أن حصلنا على $q<p$ قبل $r=0$

لدينا $n=qp+r$ $0\leq r<p$

لدينا: $q<p\Rightarrow q+1\leq p$

$\Rightarrow pq+p\leq p^2$

ولدينا $r<p$

إذن $pq+r<p+pq\leq p^2$

إذن $pq+r\leq p^2$ يعني $n\leq p^2$

إذن أجرينا قسمات n على p ولم نحصل على باقي منعدم حتى أصبح $p^2\geq n$ هذا يعني أن n لا يقبل على أي عدد أولي p يحقق $p^2\leq n$. إذن n أولي.

مثال:

لنتحقق هل 179 أولي:

p	2	3	5	7	11	13	17
q	89	59	35	25	16	13	10
r	1	2	4	4	3	10	9

إذن 179 أولي.

4) الأعداد الأولية وقابلية القسمة:

خاصية (1):

ليكن $a\in\mathbb{Z}^*$ و p أولي.

$p\wedge a=1\Leftrightarrow p\times a$

برهان:

$\Rightarrow$) نفترض أن $p\wedge a$. ولنبين أن $p\times a$

- نفترض p/a

إذن $p\wedge a=|p|$ إذن $|p|=1$

يعني $p=1$ أو $p=-1$

وهذا تناقض لأن p أولي.

إذن $p\times a$

$\Leftarrow$) نفترض أن $p\times a$ لنبين أن $p\wedge a=1$

نضع $d=p\wedge a$

إذن $\begin{cases}d/p\\d/a\end{cases}$ ونعلم أن قواسم p هي: $-1,1,-p,p$

ولدينا $\begin{cases}p\times a\\-p\times a\end{cases}$ إذن $d\neq p$ و $d\neq -p$

ولدينا $d\neq -1$ لأن $d>0$

إذن $d=1$ ومنه $p\wedge a=1$

خاصية (2):

ليكن p و q أوليين:

$p\wedge q=1\Leftrightarrow |p|\neq|q|$

برهان:

$p\wedge q=1\Leftrightarrow p\times q$

$\Leftrightarrow p\notin\{1,-1,q,-q\}$

$\Leftrightarrow p\notin\{q,-q\}$

$\Leftrightarrow p\neq q$ و $p\neq -q$

$\Leftrightarrow |p|\neq|q|$

خاصية (3):

ليكن $a_1,a_2,...,a_n$ من $\mathbb{Z}$ و p أولي.

$p/a_1a_2...a_n\Rightarrow(\exists i\in\{1,2,...,n\})\ p/a_i$

برهان:

نفترض أن $p/a_1a_2...a_n$. لنبين أن: p/a_i $\exists i\in\{1,2,...,n\}$

* إذا كان أحد الأعداد a_i منعدم.

مثلا $a_{i_0}=0$ فإن p/a_{i_0}

* إذا كانت جميع الأعداد a_i تخالف 0.

نفترض أن: $p\times a_i$: $(\forall i\in\{1,2,...,n\})$

يعني $p\wedge a_i=1$

إذن $P\wedge\prod_{i=1}^{n}a_i=1$ يعني $p\times\prod_{i=1}^{n}a_i$

وهذا تناقض.

إذن p/a_i : $(\exists i\in\{1,2,...,n\})$.

ملاحظة:

1- ليكن $a\in\mathbb{Z}$ و p أولي و $n\in\mathbb{N}$.

(*) $p/a^n\Rightarrow p/a$

(*) $p/ab\Rightarrow p/a$ أو p/b

2- ليكن p أولي موجب.

(*) $(\forall 1\leq k<p)$: $p\wedge k=1$

(*) $(\forall k\in\mathbb{Z}/1\leq|k|<p)$: $p\wedge k=1$

خاصية (4):

ليكن $p,p_1,p_2,...,p_n$ أعداد أولية.

$p/p_1p_2...p_n\Rightarrow(\exists i\in\{1,2,...,n\})|p|=|p_i|$

برهان:

لدينا: $p/p_1p_2...p_n$

إذن يوجد i بحيث p/p_i

ونعلم أن قواسم p_i هي: $-1,1,-p_i,p_i$

ولدينا $p\neq 1$ و $p_i\neq 1$ إذن $p_i=p$ أو $-p_i=p$

يعني $|p|=|p_i|$

ملاحظة:

*) $p/p_1^{\alpha_1}.p_2^{\alpha_2}....p_n^{\alpha_n}\Rightarrow(\exists i\in\{1,2,...,n\})|p|=|p_i|$

*) إذا كانت الأعداد p و p_i موجبة

فإن: $p/p_1^{\alpha_1}.p_2^{\alpha_2}....p_n^{\alpha_n}\Rightarrow(\exists i\in\{1,2,...,n\})\ p=p_i$

تطبيق:

ليكن p عدد أولي موجب.

1) بين أن p/C_p^k لكل $1\le k\le p-1$

2) بين أن $(\forall a\in\mathbb{N})\ (a+1)^p\equiv a^p+1[p]$

3) a) بين أن: $(\forall n\in\mathbb{N})\ n^p\equiv n[p]$

b) استنتج أن: $n^{p-1}\equiv 1[p]$ لكل n من $\mathbb{N}$ بحيث $n\wedge p=1$

4) a) بين أن $(\forall a\in\mathbb{Z})\ a^p\equiv a[p]$

b) بين أن $a^{p-1}\equiv 1[p]$ لكل a من $\mathbb{Z}$ بحيث $a\wedge p=1$

1) لنبين أن p/C_p^k لكل $1\le k\le p-1$

ليكن $1\le k\le p-1$. لنبين أن p/C_p^k

لدينا:

$$C_p^k=\frac{p!}{k!(p-k)!}=\frac{1.2....(p-k)(p-k+1)...p}{k!(1.2....(p-k))}$$

$$=\frac{(p-k+1)....p}{k!}$$

إذن $k!C_p^k=(p-k+1)...p$

إذن $p/k!C_p^k$

ولدينا: $\forall i\in\{1,2,...,k\}\quad 1\le i\langle p$

إذن $p\times i$

إذن $p\wedge i=1$

إذن $p\wedge k!=1$ إذن حسب Gauss:

لدينا p/C_p^k $(\forall 1\le k\le p-1)$

2) ليكن $a\in\mathbb{N}$. لنبين أن: $(a+1)^p\equiv a^p+1[p]$

لدينا:

$$(a+1)^p-(a^p+1)=\sum_{k=0}^{p}a^k.1^{p-k}-(a^p+1)$$

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

$$=1+a^p+\sum_{k=1}^{p-1}C_p^ka^k-(a^p+1)$$

$$=\sum_{k=1}^{p-1}C_p^ka^k$$

ولدينا p/C_p^k $1\le k\le p-1$

إذن $p/C_p^ka^k$

إذن $p/\sum_{k=1}^{p-1}C_p^ka^k$

يعني: $p/(a+1)^p-(a^p+1)$

بالتالي: $(a+1)^p\equiv a^p+1[p]$

3) a) ليكن $n\in\mathbb{N}$ لنبين أن $n^p\equiv n[p]$

نعلم أن:

ليكن $n\in\mathbb{N}^*$ $(a+1)^p\equiv a^p+1[p]$ $(\forall a\in\mathbb{N})$

إذن $1^p\equiv 1[p]$

$2^p\equiv 1^p+1[p]$

$3^p\equiv 2^p+1[p]$

$n^p\equiv(n-1)^p+1[p]$

بجمع أطراف المتساويات طرف طرف نستنتج أن:

$n^p\equiv 1+\underbrace{1+...1}_{n\text{ مرة}}[p]$

يعني: $n^p\equiv n[p]$

ونلاحظ أن الخاصية تبقى صحيحة من أجل $n=0$

إذن: $(\forall n\in\mathbb{N})\quad n^p\equiv n[p]$

b) ليكن $n\in\mathbb{N}$ بحيث $n\wedge p=1$. لنبين أن: $n^{p-1}\equiv 1[p]$

لدينا مما سبق: $n^p\equiv n[p]$

يعني p/n^p-n

يعني $p/n(n^{p-1}-1)$

وبما أن $n\wedge p=1$

فإن $p/n^{p-1}-1$

يعني $n^{p-1}\equiv 1[p]$ لكل n بحيث $n\wedge p=1$

4) a) ليكن $a\in\mathbb{Z}$. لنبين أن $a^p\equiv a[p]$

← إذا كان $a\ge 0$

فإنه من خلال ما سبق: $a^p\equiv a[p]$

← إذا كان $a\le -1$

فإن $-a\ge 1$ إذن $(-a)^p\equiv -a[p]$

– إذا كان $p\neq 2$ فإن p فردي.

إذن: $(-a)^p=-a^p$

إذن $-a^p\equiv -a[p]$

إذن $a^p\equiv a[p]$

– إذا كان $p=2$ فإن: $(-a)^2\equiv -a[2]$

يعني: $a^2\equiv -a[2]$

ولدينا $-a\equiv a[2]$

إذن $a^2\equiv a[2]$

إذن:

$(\forall a\in\mathbb{Z})\quad a^p\equiv a[p]$

b) ليكن $a\in\mathbb{Z}$ بحيث $a\wedge p=1$. لنبين أن $a^{p-1}\equiv 1[p]$

لدينا: $a^p\equiv a[p]$

يعني p/a^p-a

أي $p/a^{p-1}-1$

وبما أن $a\wedge p=1$ فإن $p/a^{p-1}-1$

إذن $a^{p-1}\equiv 1[p]$

مبرهنة Fermat:

ليكن p أولي موجب.

*) $\forall a\in\mathbb{Z}\quad a^p\equiv a[p]$

*) $a\wedge p=1/\mathbb{Z}$ من a لكل $a^{p-1}\equiv 1[p]$

5) تفكيك عدد إلى عداد عوامل أولية:

a) مبرهنة:

كل عدد a من $\mathbb{Z}^*-\{-1,1\}$ يكتب بطريقة وحيدة على شكل

$$a=\varepsilon p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$$

حيث:

*) الأعداد p_i أولية موجبة ومختلفة مثنى مثنى.

*) الأعداد α_i طبيعية غير منعدمة.

*) $\varepsilon=1$ إذا كان $a\rangle 0$

*) $\varepsilon=-1$ إذا كان $a\langle 0$

b) تطبيقات:

← قابلية القسمة:

خاصية:

ليكن b عدد من $\mathbb{N}^*-\{1\}$

ليكن: $a=p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$ تفكيك a إلى جداد عوامل أولية.

b/a إذا وفقط إذا كان b يكتب على شكل:

$$b=p_1^{\beta_1}p_2^{\beta_2}...p_r^{\beta_r}$$

حيث: $\beta_i\in\{0,1,2,...,\alpha_i\}=E_i$

كل ترتيبة $(\beta_1,\beta_2,...,\beta_r)$ من $E_1\times E_2\times...\times E_r$ تعطينا قاسم موجب ل a هو: $b=p_1^{\beta_1}p_2^{\beta_2}...p_r^{\beta_r}$

إذن عدد القواسم الموجبة ل a هو عدد الترتيبات $(\beta_1,\beta_2,...,\beta_r)$

ونعلم أن عدد هذه الترتيبات هو: $card(E_1\times E_2\times...\times E_r)$

$$=(cardE_1)(cardE_2)\times...(cardE_r)$$
$$=(1+\alpha_1)(1+\alpha_2)...(1+\alpha_r)$$

خاصية:

ليكن a من $\mathbb{N}^*-\{1\}$ و $a=p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$ تفكيك a إلى جداد عوامل أولية.

عدد القواسم الموجبة ل a هو: $\alpha=\prod_{i=1}^{r}(1+\alpha_i)$

مثال:

لنحدد القواسم الموجبة للعدد 54:

لنفكك 54:

54	2
27	3
9	3
3	3
1	

إذن $54=2\times 3^3$

– عدد القواسم الموجبة ل 54 هو:

$$\alpha=(1+1)(1+3)=8$$

وهذه القواسم هي الأعداد التي تكتب على شكل:

$d=2^{\beta_1}.3^{\beta_2}$ حيث $\beta_1\in\{0,1\}$

و $\beta_2\in\{0,1,2,3\}$

إذن هذه القواسم هي:

$2^0.3^0=1$; $2^0.3^1=3$; $2^0.3^2=9$

$2^0.3^3=27$; $2^1.3^0=2$; $2^1.3^1=6$

$2^1.3^2=18$; $2^1.3^3=54$.

← القاسم المشترك الأكبر والمضاعف المشترك الأصغر:

ليكن $p_r,...,p_2,p_1$ الأعداد الأولية التي تظهر في تفكيك a و b

نضع: $a=p_1^{\alpha_1}.p_2^{\alpha_2}...p_r^{\alpha_r}$ حيث $0\le\alpha_i$

و $b=p_1^{\beta_1}.p_2^{\beta_2}....p_r^{\beta_r}$ و $0\le\beta_i$

حيث $\alpha_1=0$ إذا كان p_i لا يظهر في تفكيك a.

و $\beta_i=0$ إذا كان p_i لا يظهر في تفكيك b.

نضع $d=p_1^{\gamma_1}.p_2^{\gamma_2}...p_r^{\gamma_r}$ حيث: $\gamma_i=\inf(\alpha_i,\beta_i)$

لنبين أن $d=a\wedge b$

* لدينا: $\forall i\in\{1,2,...,r\}\quad \gamma_i\le\alpha_i$

و $\gamma_i\le\beta_i$

إذن $\begin{cases}d/a\\ d/b\end{cases}$ إذن لا قاسم مشترك ل a و b

* ليكن d' قاسم مشترك ل a و b. لنبين أن $d'\le d$

لدينا: $\begin{cases}d'/a\\ d'/b\end{cases}$ إذن d' يكتب على شكل: $d'=p_1^{\lambda_1}.p_2^{\lambda_2}....p_r^{\lambda_r}$

حيث $0\le\lambda_i\le\alpha_i$

$0\le\lambda_i\le\beta_i$

إذن $0\le\lambda_i\le\inf(\alpha_i,\beta_i)$

إذن $0\le\lambda_i\le\gamma_i$

إذن d'/d

إذن $d=a\wedge b$

⇐ بنفس الطريقة نجد المضاعف المشترك الأصغر.

خاصية:

ليكن a و b من $\mathbb{N}^*-\{1\}$

نضع $a=p_1^{\alpha_1}.p_2^{\alpha_2}...p_r^{\alpha_r}$

و $b=p_1^{\beta_1}.p_2^{\beta_2}...p_r^{\beta_r}$

حيث p_i هي الأعداد الأولية التي تظهر في تفكيك a أو b

$\alpha_i=0$ إذا كان p_i لا يظهر في تفكيك a

$\beta_i=0$ إذا كان p_i لا يظهر في تفكيك b

لدينا: $a\wedge b=\prod_{i=1}^{r}P_i^{\inf(\alpha_i,\beta_i)}$

و $a\vee b=\prod_{i=1}^{r}P_i^{\sup(\alpha_i,\beta_i)}$

ملاحظة:

*) القاسم المشترك الأكبر ل a و b هو جداء العوامل الأولية المشتركة مرفوعة إلى أصغر أس.

*) $a\vee b$ هو جداء العوامل الأولية المشتركة وغير المشتركة مرفوعة إلى أكبر أس.

مثال:

لنحدد: $632\wedge 76$ و $632\vee 76$

632	2
316	2
158	2
79	79
1	

إذن $632=2^3.79$

76	2
38	2
19	19
1	

إذن $76=2^2.19$

لدينا: $632\wedge 76=2^2=4$

$76 \vee 632 = 2^3.19.79 = 12008$

VII) نظمات العد:

1- أمثلة:

مثال 1: نعتبر العدد $n = 526$

*) لدينا:

$$n = 526 = 500 + 20 + 6$$
$$= 510^2 + 210^1 + 6$$

إذن العدد n يكتب باستعمال العشرة أرقام 0, 1, 2, ..., 9 وقوى 10.

نقول إن الكتابة $n = 256$ تمثيل عشري للعدد n أو تمثيل n في نظمة العد العشري، أو تمثيل العدد n في نظمة العد ذات الأساس 10.

*) ويمكن كتابة n باستعمال 3 أرقام فقط 0, 1, 2 وقوى 3:

$$n = 526 = 486 + 40$$
$$= 2.3^5 + 27 + 13$$
$$= 2.3^5 + 3^3 + 9 + 4$$
$$= 2.3^5 + 3^3 + 3^2 + 3 + 1$$

إذن $n = 2.3^5 + 0.3^4 + 1.3^3 + 1.3^2 + 1.3 + 1$

ونكتب: $n = \overline{201111}_{(3)}$

وهذه الكتابة تسمى تمثيل n في نظمة العد ذات الأساس 3.

مثال 2: نعتبر العدد $n = 200$

- لنكتب تمثيل n في نظمة العد ذات الأساس 3.

$$n = 200 = 162 + 38$$
$$= 2.3^4 + 27 + 11$$
$$= 2.3^4 + 3^3 + 3^2 + 2$$
$$= 2.3^4 + 1.3^3 + 1.3^2 + 0.3 + 2$$

إذن: $n = \overline{21102}_{(3)}$

2- تعميل عدد طبيعي في نظمة العد ذات الأساس b

مبرهنة:

ليكن $b \in \mathbb{N}^* - \{1\}$

كل عدد n من $\mathbb{N}^*$ يكتب بطريقة وحيدة على شكل:

$$n = \alpha_p b^p + \alpha_{p-1} b^{p-1} + \alpha_{p-2} b^{p-2} + ... + \alpha_1 b^1 + \alpha_0$$

حيث:

$$\begin{cases} \alpha_i \in \mathbb{N} \\ 0 \le \alpha_i < b \end{cases} \quad \forall i \in \{0, 1, 2, ..., p\} \quad \text{و} \quad \alpha_p \neq 0$$

و $b^p \le n < b^{p+1}$

ونكتب: $n = \overline{\alpha_p \alpha_{p-1} ... \alpha_1 \alpha_0}_{(b)}$

وتسمى هذه الكتابة تمثيل العدد n في نظمة العد ذات الأساس 5.

ملاحظة:

هناك عدة نظمات العد أهمها:

- نظمة العد العشري وهي النظمة المتداولة.
- نظمة العد الثنائي والأرقام المستعملة هي 0, 1.
- نظمة العد ذات الأساس 8. والأرقام المستعملة هي: 0, 1, ..., 7
- نظمة العد ذات الأساس 12. والأرقام المستعملة 0, 1, ..., 9, α, β.

3- طريقة عملية لتمثيل عدد n في تتمةعدأساسها b.

ليكن $b \in \mathbb{N}^* - \{1\}$ و $n \in \mathbb{N}^*$

+) نقسم n على b: $n = b.q_0 + r_0$ مع $0 \le r_0 < b$

*) إذا كان $q_0 \neq 0$: نقسم q_0 على b:

$$q_0 = bq_1 + r_1 \qquad 0 \le r_1 < b$$

*) إذا كان $q_1 \neq 0$: نقسم q_1 على b:

$$q_1 = bq_2 + r_2 \qquad 0 \le r_2 < b$$

وهكذا نتابع القسمات حتى نحصل على خارج منعدم.

ومن الضروري أن نحصل على خارج منعدم، لأن:

- لدينا: $q_0 < q_0 b < q_0 b + r_0 = n \Rightarrow 1 < b$

إذن $q_0 < n$

- $q_1 < q_1 b < q_1 b + r_1 = q_0 \Rightarrow 1 < b$

إذن $q_1 < q_0$

إذن $0 < ... < q_2 < q_1 < q_0 < n$

هذه الخوارج تناقصية قطعا. وبالتالي ضروري أن نحصل على خارج منعدم.

- نفترض أن q_p هو أول خارج منعدم.

يعني: $\forall i \in \{0, ..., (p-1)\} \quad q_i \neq 0$

$$n = q_0 b + r_0 \qquad (b^0) \qquad 0 \le r_0 < b$$
$$q_0 = q_1 b + r_1 \qquad (b^1) \qquad 0 \le r_1 < b$$
$$q_1 = q_2 b + r_2 \qquad (b^2) \qquad 0 \le r_2 < b$$
$$q_{p-1} = b.q_p + r_p \qquad (b^p)$$

بضرب الأسطر في $b^p, ..., b^2, b^1, b^0$ على التوالي نحصل على وبجمع أطراف المتساويات نحصل على:

$$n = r_0 + r_1 b^1 + r_2 b^2 + ... + r_p b^p + q_p b^{p+1} \qquad (q_p = 0)$$

$q_p = 0$

إذن: $n = r_p b^p + r_{p-1} b^{p-1} + ... + r_1 b + r_0$

حيث $0 \le r_i < b$

و $r_p = q_{p-i} \neq 0$

إذن $n = \overline{r_p r_{p-1} ... r_0}_{(b)}$

خاصية:

ليكن $b \in \mathbb{N}^* - \{1\}$ و $n \in \mathbb{N}^*$

نقوم بالقسمات المتتالية للخوارج على b بدءا من n.

وإذا كانت $r_p, ..., r_1, r_0$ هي بواقي هذه القسمات حيث r_p هو باقي أول قسمة نحصل فيها على خارج منعدم

فإن: $n = \overline{r_p r_{p-1} ... r_0}_{(b)}$

ونلخص هذه القسمات في الجدول التالي:

n	b
q_0	b
q_1	b
q_2	b
$0=q_p$	

مثال:

نعتبر الدد $n = 798$

لنمثل n في نظمة العد ذات الأساس 7.

798	7
114	7
16	7
2	7
0	

إذن: $799=\overline{2220}_{(7)}$

4) تغيير الأساسية:

*) إذا أردنا المرور من التمثيل العشري إلى نظمة عد أساسها b نتبع الخوارزمية السابقة.

*) إذا أردنا المرور من التمثيل في نظمة عد أساسها b إلى نظمة العد العشري، نستعمل: $n=\overline{d_p\alpha_{p-1}....d_0}_{(b)}$

$$=\alpha_p b^p+\alpha_{p-1}b^{p-1}...+\alpha_1 b+\alpha_0$$

مثال:

$$n=\overline{3450}_{(6)}=3.6^3+4.6^2+5.6+0$$
$$=822$$

*) إذا أردنا المرور من التمثيل في نظمة عد أساسها b إلى نظمة عد أساسها b'، نمر من b إلى التمثيل العشري ومن التمثيل العشري إلى b'.

5) مقارنة عددين:

خاصية:

نعتبر العددين: $x=\overline{\alpha_p\alpha_{p-1}...\alpha_0}_{(b)}$

$y=\overline{\beta_q\beta_{q-1}...\beta_0}_{(b)}$

إذا كان $p\rangle q$ يعني عدد أرقام x أكبر قطعا من عدد أرقام y. فإن $x\rangle y$.

خاصية 2:

نعتبر العددين:

$x=\overline{\alpha_p...\alpha_0}_{(b)}$

$y=\overline{\beta_p...\beta_0}_{(b)}$

(x و y لهما نفس عدد الأرقام)

نفترض أن $\alpha_i\neq\beta_i...,\alpha_{p-1}=\beta_{p-1},\alpha_p=\beta_p$

- إذا كان $\alpha_i\rangle\beta_i$ فإن $x\rangle y$
- إذا كان $\alpha_i\langle\beta_i$ فإن $x\langle y$

6) الجمع والضرب في نظمة عد أساسها b.

عمليتا الجمع والضرب في نظمة عد أساسها b تتم بنفس الطريقة في نظمة العد العشري.

هناك فرق فقط في الاحتفاظ، حيث عند حساب $\alpha_i\beta_i$ أو $\alpha_i+\beta_i$ إذا حصلنا على رقم $\gamma\langle b$ نكتب γ. وإذا حصلنا على $\gamma\geq b$ نقوم بقسمة γ على b مع $0\leq r\langle b$: نكتب r ونحتفظ ب q.

مثال:

*) $\overline{3675}_{(8)}+\overline{2764}_{(8)}=\overline{6661}_{(8)}$

*) $\overline{5624}_{(7)}\times\overline{56}_{(7)}=\overline{50313}_{(7)}+\overline{41356}_{(7)}=\overline{464203}_{(7)}$

7) مضاعف القسمة على 2, 3, 4, 5, 9, 11, 25.

نعتبر العدد $x=\overline{\alpha_p\alpha_{p-1}...\alpha_0}_{(10)}$

لدينا: $x=\alpha_p10^p+\alpha_{p-1}10^{p-1}+...+\alpha_1 10+\alpha_0$

*) لنبين أن: $2/x\Leftrightarrow 2/\alpha_0$

لدينا: $10\equiv 0[2]$ إذن $\forall i\in\{1,...,p\}\ \ 10^i\equiv 0[2]$

يعني $\alpha_i 10^i\equiv 0[2]$

إذن: $\sum_{i=1}^{p}\alpha_i 10^i\equiv 0[2]$

يعني: $\sum_{i=1}^{p}-\alpha_i 10^i+\alpha_0\equiv\alpha_0[2]$

يعني: $x\equiv\alpha_0[2]$

إذن:

$$2/x\Leftrightarrow x\equiv 0[2]$$
$$\Leftrightarrow\alpha_0\equiv 0[2]\ \left(x\equiv\alpha_0[2]\right)$$
$$\Leftrightarrow 2/\alpha_0$$

وبالتالي: $2/x\Leftrightarrow 2/\alpha_0$

*) لنبين أن:

$$3/x\Leftrightarrow 3\Big/\sum_{i=0}^{p}\alpha_i$$

لدينا $10\equiv 1[3]$

إذن $\forall i\in\{1,2,...,p\}\ \ 10^i\equiv 1[3]$

يعني $\alpha_i 10^i\equiv\alpha_i[3]$

إذن:

$$\sum_{i=1}^{p}\alpha_i 10^i\equiv\sum_{i=1}^{p}\alpha_i[3]$$

إذن: $\sum_{i=1}^{p}\alpha_i 10^i+\alpha_0\equiv\sum_{i=1}^{p}\alpha_i[3]$

أي: $x\equiv\sum_{i=0}^{p}\alpha_i[3]$

إذن:

$$3/x\Leftrightarrow x\equiv 0[3]$$
$$\Leftrightarrow\sum_{i=0}^{p}\alpha_i\equiv 0[3]\qquad\left(x\equiv\sum_{i=0}^{p}\alpha_i[3]\right)$$
$$\Leftrightarrow 3\Big/\sum_{i=0}^{p}\alpha_i$$

وبالتالي: $3\Big/x\Leftrightarrow 3\Big/\sum_{i=0}^{p}\alpha_i$

- لنبين أن: $4/x\Leftrightarrow 4/\overline{\alpha_1\alpha_0}$

لدينا: $\forall i\in\{2,...,p\}: 10^i=10^2.10^{i-2}$

$$=100.10^{i-2}$$
$$=4.25.10^{i-2}$$

إذن $\forall i\in\{2,...,p\}\qquad 10^2\equiv 0[4]$

إذن $\alpha_i 10^i\equiv 0[4]$

إذن: $\sum_{i=2}^{p}\alpha_i.10^i\equiv 0[4]$

إذن

$$\sum_{i=2}^{p}\alpha_i 10^2+\alpha_1 10+\alpha_0\equiv\alpha_1 10+\alpha_0[4]$$

يعني: $x\equiv\alpha_1.10+\alpha_0[4]$

يعني $x\equiv\overline{\alpha_1\alpha_0}[4]$

إذن:

$$4/x\Leftrightarrow x\equiv 0[4]$$
$$\Leftrightarrow\overline{\alpha_1\alpha_0}\equiv 0[4]\ \left(x\equiv\overline{\alpha_1\alpha_0}[4]\right)$$
$$\Leftrightarrow 4/\overline{\alpha_1\alpha_0}$$

وبالتالي: $4/x\Leftrightarrow 4/\overline{\alpha_1\alpha_0}$

- لنبين أن: $11/x \Leftrightarrow \alpha_0+\alpha_1+...\equiv \alpha_1+\alpha_3+...[11]$

لدينا: $\forall i\in\{1,...,p\} \quad 10\equiv -1[11]$

إذن $10^i\equiv(-1)^2[11]$

إذن $\alpha_i 10^i\equiv\alpha_i(-1)^i[11]$

إذن: $\sum_{i=1}^{p}\alpha_i 10^i\equiv\sum_{i=1}^{p}\alpha_i(-1)^i[11]$

أي: $\sum_{i=1}^{p}\alpha_i 10^i+\alpha_0\equiv\sum_{i=1}^{p}\alpha_i(-1)^i+\alpha_0[11]$

يعني: $x\equiv\sum_{i=1}^{p}\alpha_i(-1)^i[11]$

يعني: $x\equiv\sum_{i=0}^{p}\alpha_i(-1)^2+\sum_{i=0}^{p}\alpha_i(-1)^i[11]$

$x\equiv\sum_{i=0}^{p}\alpha_i-\sum_{i=0}^{p}\alpha_i[11]$

إذن: $11/x\Leftrightarrow x\equiv 0[11]$

$\Leftrightarrow\sum_{i=0}^{p}\alpha_i-\sum_{i=0}^{p}\alpha_i\equiv 0[11]$

$\Leftrightarrow\sum_{i=0}^{p}\alpha_i\equiv\sum_{i=0}^{p}\alpha_i[11]$

بالتالي: $11/x\Leftrightarrow\alpha_0+\alpha_2+...=\alpha_1+\alpha_3+...[11]$

خاصية:

نعتبر العدد $x=\overline{\alpha_p\alpha_{p-1}...\alpha_0}_{(10)}$

لدينا:

*) $2/x\Leftrightarrow$ α_0 زوجي

*) $3/x\Leftrightarrow 3/\sum_{i=0}^{p}\alpha_i$

*) $4/x\Leftrightarrow 4/\overline{\alpha_1\alpha_0}$

*) $5/x\Leftrightarrow\alpha_0\in\{0,5\}$

*) $9/x\Leftrightarrow 9/\sum_{i=0}^{p}\alpha_i$

*) $11/x\Leftrightarrow\alpha_0+\alpha_2+\alpha_4+...\equiv\alpha_1+\alpha_3+\alpha_5+...[11]$

*) $25/x\Leftrightarrow\overline{\alpha_1\alpha_0}\in\{\overline{00},\overline{25},\overline{50},\overline{75}\}$

تمرين تطبيقي:

حدد الأعداد الطبيعية غير المنعدمة a,b,c بحيث:

$\overline{bbac}_{(7)}=\overline{abca}_{(11)}$

نلاحظ أن a,b,c أصغر قطعا من 11 و 7.

وبالتالي فهي محصورة قطعا بين 0 و 7.

وبالتالي فهي محصورة بين 1 و 6.

لدينا:

$\overline{bbac}_{(7)}=\overline{abca}_{(11)}\Leftrightarrow b7^3+b7^2+a7+c=a11^3+b11^2+c11+a$

$\Leftrightarrow 343b+49b+7a+c=1331a+121b+11c+a$

$\Leftrightarrow 1325a-271b+10c=0$

$\Leftrightarrow 1325a+10c=271b$

$\Leftrightarrow 5(265a+2c)=271b$ (1)

إذن $5/271b$

ولدينا: $271\wedge 5=1$ إذن حسب Gauss نستنتج أن $5/b$

وبما أن $1\le b\le 6$ فإن $b=5$

وبالتعويض في (1) نحصل على:

$5(265a+2c)=271.5$

يعني $265a+2c=271$

يعني $2c=271-265a$ (*)

ولدينا $2c\rangle 0$ إذن $271-265a\rangle 0$

يعني: $0<a<\frac{271}{265}=1$

إذن: $a=1$

وبالتعويض في (*) نجد: $c=3$

بالتالي: $\begin{cases}a=1\\b=5\\c=3\end{cases}$