

I- القسمة الإقليدية في Z:

$\forall (a, b) \in Z^2 \exists!(q, r) \in Z^* \times \mathbb{N} / a = bq + r$
بحيث $0 \leq r < |b|$
① عندما نحدد الزوج (q, r) نقول أننا أجرينا أجرين القسمة الإقليدية ل a على b .
② a يسمى المقسوم و b المقسوم عليه و q الخارج و r الباقي.

II- قابلية القسمة في Z:

① ليكن a و b في Z .
 $a/b \Leftrightarrow \exists k \in Z / b = ka$
② $\forall a \in Z : a/a$
③ $\forall (a, b) \in Z^2 \forall n \in \mathbb{N}^* : a^n / b \Rightarrow a/b$
④ $\forall (a, b) \in Z^2 : a|b \Leftrightarrow |a| = |b|$
⑤ $\forall (a, b, c) \in Z^3$
 $d/a \text{ و } d|b \Rightarrow \forall (\alpha, \beta) \in Z^2 : d|\alpha a + \beta b$

III- الموافقة بترديد:

① $a \equiv b [n] \Leftrightarrow a - b = kn (k \in Z) \Leftrightarrow n|a - b$
② $a \equiv b [n] \Leftrightarrow ac \equiv bc [n]$
③ $a \equiv b [n] \Leftrightarrow a + c \equiv b + c [n]$
④ $\begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Leftrightarrow ac \equiv bd [n]$
⑤ $\begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Leftrightarrow a + c \equiv b + d [n]$

IV- القاسم المشترك الأكبر:

ليكن a و b و d في Z .
① d قاسم مشترك ل a و b يعني أن $d|a$ و $d|b$.
② أكبر قاسم مشترك موجب للعديدين a و b يسمى القاسم المشترك الأكبر ل a و b و يرمز له ب :
 $a \wedge b$ أو $\text{pgdc}(a, b)$ أو $\Delta(a; b)$
③ $d = a \wedge b \Rightarrow d|a \text{ و } d|b$
④ $\begin{cases} d'|a \\ d'|b \end{cases} \Rightarrow d'|a \wedge b$
⑤ $a \wedge b = 1 \Leftrightarrow a$ و b أوليان فيما بينهما
⑥ $d = a \wedge b \Leftrightarrow \begin{cases} \exists (a', b') \in Z^2 / a' \wedge b' = 1 \\ a = d.a' \text{ و } b = d.b' \end{cases}$
⑦ $d = a \wedge b \Rightarrow \exists (u, v) \in Z^2 / d = ua + vb$
⑧ (bezout) $a \wedge b = 1 \Leftrightarrow ua + vb = 1$
⑨ $\begin{cases} a|c \text{ و } b|c \\ a \wedge b = 1 \end{cases} \Rightarrow ab|c$

(Gauss) $\forall (a, b, c) \in Z^3 : \begin{cases} d|ab \\ d \wedge a = 1 \end{cases} \Rightarrow d|b$ ⑩
 $\forall (a, b, c) \in Z \begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Leftrightarrow a \wedge bc = 1$ ⑪
 $\forall (n, m) \in \mathbb{N}^{*2} : a \wedge b = 1 \Leftrightarrow a^n \wedge b^m = 1$ ⑫
 $[a = bq + r / 0 \leq r < b] \Rightarrow a \wedge b = b \wedge r$ ⑬

V- المضاعف المشترك الأكبر:

ليكن a و b و m من Z .
① m مضاعف مشترك ل a و b $\Leftrightarrow a/m$ و b/m
② أصغر مضاعف مشترك موجب للعديدين a و b يسمى المضاعف المشترك الأصغر ل a و b و يرمز له ب :
 $\text{ppcm}(a; b)$ أو $a \vee b$
③ $m = a \vee b \Rightarrow a/m$ و b/m
④ $\forall (a, b, c) \in Z^3 : \begin{cases} a|c \\ b|c \end{cases} \Rightarrow (a \vee b)|c$
⑤ $\forall (a, b, c) \in Z^2 : (a \vee b)(a \wedge b) = |a.b|$

VI- الأعداد الأولية:

① ليكن a و d في Z . نقول إن d قاسم فعلي ل a إذا كان d يقسم a و يخالف الأعداد : $a, -a, 1, -1$.
② نقول أن عددا صحيحا نسبيا a أولي إذا كان مخالف ل 1 و -1 و ليس له قواسم فعلية.
⊗ ملحوظة :
- الأعداد : $0, -1, 1$ ليست أولية.
- مجموعة الأعداد الأولية لا منتهية.
ليكن p عدد أولي.

③ $p|a^n \Rightarrow p|a$
④ $p|ab \Rightarrow p|a$ أو $p|b$
⑤ $p|a_1 \times a_2 \times \dots \times a_n \Rightarrow \exists i \in \{1, \dots, n\} : p|a_i$
⑥ $p \wedge a = p \Rightarrow p|a$
⑦ $p \nmid a \Rightarrow p \wedge a = 1$

VII- خوارزمية إقليدس:

ليكن a و b في \mathbb{N} بحيث : $a > b$.
نتجز القسمة ل a على b :
 $0 \leq r_0 \leq b$ و $a = bq_0 + r_0$
* إذا كان : $r_0 = 0$
فإن : $b|a$ و بالتالي : $a \wedge b = b$.
* إذا كان : $0 < r_0 < b$
نتجز القسمة الإقليدية ل b على r_0 .
 $0 \leq r_1 < r_0 < b$ و $b = r_0q_1 + r_1$
* إذا كان : $r_1 = 0$

X - نظمات العد:

① ليكن x عدد صحيح طبيعي بحيث $x \geq 2$:
كل عدد صحيح طبيعي b يمكن أن يكتب على شكل:
$$b = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1 \cdot x + a_0$$

حيث $\forall i \in [0; n] : a_i \in [0; n-1]$ و $a_n \neq 0$
و نكتب بصيغة مختصرة: $b = \overline{a_n a_{n-1} \dots a_1 a_0}^{(n)}$
نقول أن $\overline{a_n a_{n-1} \dots a_1 a_0}^{(n)}$ هو التمثيل المختصر للعدد b
في نظمة العد ذات الأساس x .
② إذا كان x و y من ممثلين في نظمة العد b :
$$y = \overline{c_m c_{m-1} \dots c_1 c_0}^{(b)}$$
 و $x = \overline{a_n a_{n-1} \dots a_1 a_0}^{(b)}$
و كان: $m > n$ فإن $y > x$.
③ إذا كان:
$$y = \overline{c_n c_{n-1} \dots c_1 c_0}^{(b)}$$
 و $x = \overline{a_n a_{n-1} \dots a_1 a_0}^{(b)}$
و $c_{i+1} = a_{i+1}$ ، $c_{n-1} = a_{n-1}$ ، $c_n = a_n$
و $c_i \neq a_i$ فإن ترتيب x و y هو نفس ترتيب a_i و c_i

فإن $b \mid r_0$ و بالتالي: $a \wedge b = b \wedge r_0 = r_0$.

* إذا كان: $r_1 \neq 0$

ننجز القسمة الإقليدية ل r_0 على r_1 .

$$0 \leq r_2 \leq r_1 \text{ و } r_0 = r_1 q_2 + r_2$$

* بعد إعادة نفس الطريقة عدة مرات سوف نحصل على
باق منعدم و القاسم المشترك ل و آخر باقي غير منعدم.

VIII - تفكيك عدد صحيح نسبي غير منعدم إلى جداء عوامل أولية:

① كل عدد صحيح نسبي n غير منعدم مخالف ل 1 و -1
يمكن أن يكتب بكيفية وحيدة على الشكل:

$$n = \varepsilon \times p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r} \quad (\varepsilon = \pm 1)$$

حيث: p_1 و p_2 و و p_r أعداد أولية موجبة و
مختلفة مثلي، مثلي.

α_1 و α_2 و و α_r أعداد صحيحة طبيعية غير
منعدمة.

② إذا كان $a = \prod_{i=1}^n p_i^{\alpha_i}$ و $b = \prod_{i=1}^n p_i^{\beta_i}$

(p_i أعداد مختلفة مثلي مثلي.

و $\alpha_i, \beta_i \in \mathbb{N}$ و $1 \leq i, j \leq n$ فإن:

$$a \vee b = \prod_{i=1}^n p_i^{\sup(\alpha_i, \beta_i)} \text{ و } a \wedge b = \prod_{i=1}^n p_i^{\inf(\alpha_i, \beta_i)}$$

IX - المجموعة Z/nZ :

① $\forall (a; b) \in Z^2 : a \equiv b[n] \Leftrightarrow a - b = k.n$

العلاقة " \equiv " علاقة تكافؤ.

② صنف تكافؤ x ($x \in Z$):

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

$$\bar{x} = \{x + k.n / k \in Z\}$$

③ مجموعة أصناف التكافؤ بالنسبة للعلاقة " \equiv " تكتب
على شكل $Z/nZ = \{\bar{0}; \bar{1}; \dots; \overline{(n-1)}\}$ حيث:

$$\forall (\bar{x}; \bar{y}) \in Z/nZ \times Z/nZ :$$

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

$$\text{④}$$

$$\text{⑤ } (Z/nZ; +)$$
 زمرة تبادلية.

$$\text{⑥ } (Z/nZ; +; \bar{x})$$
 حلقة تبادلية وواحدية وتكون جسم

$$\text{⑦ } a \wedge n = 1 \Leftrightarrow Z/nZ$$
 قابل للقلب في

$$\text{⑧ } (\exists \bar{x} \in Z/nZ / \bar{x} \times a = \bar{a} \times \bar{x} = \bar{1})$$
 قابل للقلب يعني:

يقوم بعمل عظيم ذاك الذي لا يؤجل عمل اليوم إلى الغد

