I. القسمة الأقليدية / قابلية القسمة / الموافقة :

خاصية القسمة الأقليدية:

مهما يكن العدد الصحيح النسبي a ، ومهما يكن العدد الصحيح الطبيعي ، غير المنعدم، b ، يوجد عددان صحيحان وحيدان q و r ، بحيث :

$$a = b.q + r \quad \text{و} \quad 0 \le r \prec b$$

قابلة القسمة:

a و b عددان صحيحان؛ نقول أن b يقسم a (أو a مضاعف ل b)؛ إذا وفقط إذا وجد عدد صحيح q بحيث:

$$a = b.q$$

الموافقة بترديد n:

نعتبر عددا طبيعيا غير منعدم n .
a و b عددان صحيحان نسبيان؛ نقول أن العدد a موافق للعدد b بترديد n ، إذا وجد عدد صحيح k بحيث:

$$a - b = n.q$$

نكتب : $a \equiv b[\text{modulo } n]$

II. القسمة الأقليدية / قابلية القسمة / الموافقة :

قابلية القسمة:

$$a/a \quad ; \quad (a/b \text{ et } b/c) \Rightarrow a/c \quad ; \quad (a/b \text{ et } b/a) \Rightarrow |a| = |b|$$

$$(a/b \text{ et } c/d) \Rightarrow ac/bd$$

$$(\delta/a \text{ et } \delta/b) \Rightarrow (\forall(\alpha,\beta) \in Z^2) \; ; \; \delta/\alpha.a + \beta.b$$

$$a^n/b \Rightarrow a/b$$

الموافقة:

$$a \equiv b[n] \Leftrightarrow a - b = k.n \Leftrightarrow n/a - b$$

$$\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d[n] \\ a.c \equiv b.d[n] \end{cases}$$

III. القاسم المشترك الأكبر والمضاعف المشترك الأصغر :

القاسم المشترك الأكبر: نرمز له : $d = pgdc(a,b) = a \wedge b$. يحقق القاسم المشترك الأكبر، الخاصيات التالية:

$$(d = a \wedge b) \Leftrightarrow (\exists(a',b') \in Z^2) \; ; \; \begin{cases} a = d.a' \\ b = d.b' \end{cases} \text{ et } a' \wedge b' = 1$$

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

المضاعف المشترك الأصغر: يحقق المضاعف المشترك الأصغر، الخاصيات التالية:

$$(m = a \vee b) \Rightarrow \begin{cases} a/m \\ b/m \end{cases} \; ; \; \begin{cases} a/c \\ b/c \end{cases} \Rightarrow a \wedge b/c$$

خاصية مشتركة:

$$\forall(a,b) \in Z^2; (a \vee b).(a \wedge b) = |a.b|$$

IV. الأعداد الأولية فيما بينها - خاصيات :

الأعداد الأولية فيما بينها:

نقول أن العددين a b أوليان فيما بينهما إذا وفقط إذاكان: $pgcd(a,b)=1$.

مبرهنة كوص:

$$(c/a.b \text{ et } c \wedge a = 1) \Rightarrow (c/b)$$

خاصيات أخرى:

$$(a/c \text{ et } b/c \text{ et } a \wedge b = 1) \Rightarrow (a.b/c)$$

$$(a \wedge b = 1 \text{ et } a \wedge c = 1) \Rightarrow (a \wedge b.c) = 1$$

$$(a \wedge b = 1) \Leftrightarrow \forall(m,n) \in IN^* x IN^* \; ; \; (a^m \wedge b^n = 1)$$

$$(a = b.q + r \text{ et } 0 \le r \prec b) \Rightarrow (a \wedge b = r \wedge b)$$

V. الأعداد الأولية ـ خاصيات :

يكون عدد صحيح، عددا أوليا إذا وفقط إذا كان يقبل قاسمين موجبين بالضبط 2، 3 ، 5، 7 ...العددان 1 و -1 ليسا أوليان.
مجموعة الأعداد الأولية مجموعة غير منتهية...

خاصيات: *ليكن p عددا أوليا، لدينا:*

$(p/a.b) \Rightarrow (p/a \quad ou \quad p/b)$

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

$(p/a_1.a_2...a_n) \Leftrightarrow \exists i \in (1,2,...,n) \; ; \quad (p/a_i)$

$(p/a) \Rightarrow p \wedge a = p \quad et \quad (p \text{ ne divise pas } a) \Rightarrow p \wedge a = 1$

VI. جوارزمية أقليدس :

نعتبر العددين الصحيحين الطبيعيين a و b ، بحيث:
a >b
نقسم العدد a (العدد الأكبر) على العدد b ونجد:

$(1): \quad a = b.q_0 + r_0 \quad et \quad 0 \le r_0 \prec b$

إذا كان $r_0 = 0$ ، فإن pgcg(a,b) = b
إذا كان $r_0 \# 0$ ، نقسم b على r_0 ، ونجد:

$(2): \quad b = r_0.q_1 + r_1 \quad et \quad 0 \le r_1 \prec r_0 \prec b$

إذا كان $r_1=0$ ، فإن $pgcd(a,b)=pgcd(b,r_0)=r_0$

إذا كان $r_1 \# 0$ ، نقسم r_0 على r_1 ، ونجد:
الخ.
بعد عدد محدود من العمليات نحصل على باقي منعدم (ذلك لأن متتالية البواقي هي متتالية تناقصية لأعداد صحيحة) ليكن r_n آخر باقي غير منعدم ، يكون لدينا إذن:

$$pgcd(a,b)=pgcd(b,r_0)=...=pgcd(r_{n-1}, r_n)=r_n$$

VII. تفكيك عدد صحيح الى جداء عوامل أولية :

كل عدد صحيح طبيعي غير منعدم ومخالف للعدد1 ، يتفكك بشكل وحيد على شكل:

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_n^{\alpha_n}$$

بحيث تكون الأعداد *pi* أولية، والأعداد α_i صحيحة غير منعدمة.

VIII. مجموعة أصناف التكافؤ : Z/n.Z

علاقة التوافق:

$$a \equiv b[n] \Leftrightarrow a - b = k.n \Leftrightarrow n/a-b$$

هي علاقة تكافؤ في مجموعة الأعداد الصحيحة النسبية، منسجمة مع قانوني الجمع و الضرب:

$$\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d[n] \\ a.c \equiv b.d[n] \end{cases}$$

صنف تكافؤ العدد الصحيح النسبي x ، هو المجموعة المعرفة كما يلي:

$$\alpha = \bar{x} = \{y \in Z / \quad y \equiv x[\text{modulo } n]\}$$

يرمز لمجموعة أصناف التكافؤ : Z/n.Z

$$Z/n.Z = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, ..., \overline{n-2}, \overline{n-1}\}$$

يعرف الجمع والضرب في هذه المجموعة كما يلي:

$$\begin{cases} \bar{a} + \bar{b} \equiv \overline{a+b} \\ \bar{a}.\bar{b} \equiv \overline{a.b} \end{cases}$$

(Z/n.Z , + , x) حلقة واحدية تبادلية، بصفة عامة غير تكاملية.
إذا كان العدد n أوليا، فإن (Z/n.Z , + , x) يكون جسما.

$$(\bar{a} \text{ inversible dans } Z/n.Z) \Leftrightarrow (a \wedge n = 1)$$

IX. نظمات العد :

ليكن x عددا صحيحا أكبر من أو يساوي 2.
كل عدد صحيح b يمكن أن يكتب على الشكل :

$$b = a_n.x^n + a_{n-1}.x^{n-1} + ...+ a_1.x + a_0$$

بحيث:

$$a_n \ne 0 \quad et \quad (\forall i \in [0,n]) \; ; \quad a_i \in [0, n-1]$$

نكتب:

$$(1): \quad b = \overline{a_n a_{n-1} ... a_1 a_0}^{(x)}$$

ونقول أن هذه الكتابة هي الكتابة المختصرة للعدد b في نظمة العد الذي أساسه x .

X. تحديد القاسم المشترك الأكبر والمصاعف المشترك الأصغر لعددين :

نعتبر :

$$a = \prod_{i=1}^{n} p_i^{\alpha_i} \quad et \quad b = \prod_{i=1}^{n} p_i^{\beta_i}$$

التفكيك الى جداء عوامل أولية للعددينم a و b . نجد:

$$a \wedge b = \prod_{i=1}^{n} p_i^{\inf(\alpha_i, \beta_{ic})}$$

$$a \vee b = \prod_{i=1}^{n} p_i^{\sup(\alpha_i, \beta_{ic})}$$