

الحسابيات

(1) تذكير:

(1) قابلية القسمة في \mathbb{Z}

ليكن a و b من \mathbb{Z} نقول أن b يقسم a و نكتب b/a إذا وجد k من \mathbb{Z} بحيث $a = kb$

$$(\forall a \in \mathbb{Z}) \quad a/a \quad \diamond$$

$$(\forall (a,b,c) \in \mathbb{Z}^3) \quad \begin{cases} a/b \\ b/c \end{cases} \Rightarrow a/c \quad \diamond$$

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

(2) القسمة الأقليدية في \mathbb{Z}

ليكن a من \mathbb{Z} و b من \mathbb{N}^* يوجد زوج وحيد (q,r) من $\mathbb{Z} \times \mathbb{N}$ بحيث:

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

(2) الموافقة بترديد n

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

نقول إن a يوافق b بترديد n إذا وفقط إذا كان $n/a - b$ و نكتب $a \equiv b [n]$

$$\forall a \in \mathbb{Z} \quad a \equiv a [n] \quad \diamond$$

$$\forall (a,b) \in \mathbb{Z}^2 \quad a \equiv b [n] \Rightarrow b \equiv a [n] \quad \diamond$$

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

$$\forall a \in \mathbb{Z} \quad n \in \mathbb{N}^* \quad \diamond$$

$$a \equiv r [n] \quad \text{إذا كان } r \text{ هو باقي قسمة } a \text{ على } n \text{ فإن } a \equiv r [n]$$

❖ ليكن $n \in \mathbb{N}^*$ و a و b من \mathbb{Z}
إذا كان r هو باقي قسمة a على n و r' هو باقي قسمة b على n
فإن : $a \equiv b [n] \Leftrightarrow r = r'$

❖ ليكن $n \in \mathbb{N}$
 $\forall (a,b,c,d) \in \mathbb{Z}^4 \quad \begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d [n] \\ ac \equiv bd [n] \end{cases}$

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

$\forall (a,b) \in \mathbb{Z}^2; (\forall m \in \mathbb{N}) \quad a \equiv b [n] \Rightarrow a^m \equiv b^m [n]$

مجموعة أصناف تكافؤ

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

نسمي صنف تكافؤ x المجموعة التي نرمز لها ب \bar{x} أو \dot{x} و هي معرفة بما يلي : $\bar{x} = \{y \in \mathbb{Z} / y \equiv x [n]\}$

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

$$\bar{x} = \{x + nk / k \in \mathbb{Z}\} \quad \triangleright$$

$$\bar{x} = \bar{y} \Leftrightarrow x \equiv y [n] \quad \triangleright$$

$$\bar{x} \cap \bar{y} = \emptyset \Leftrightarrow x \not\equiv y [n] \quad \triangleright$$

$$(n \in \mathbb{N}^*) \quad \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\} \quad \triangleright$$

$$\overline{x+y} = \bar{x} + \bar{y} \quad \triangleright$$

$$\overline{x \cdot y} = \bar{x} \cdot \bar{y} \quad \triangleright$$

➤ الجمع و الضرب تبادليان في $\mathbb{Z}/n\mathbb{Z}$

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

➤ $\bar{0}$ هو العنصر المحايد بالنسبة للجمع

➤ $\bar{1}$ هو العنصر المحايد بالنسبة للضرب

➤ $-\bar{x} = \overline{-x}$ هو مقابل \bar{x}

نقول أن $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ حلقة تبادلية وواحدية

3) القاسم المشترك الأكبر

ليكن a و b عددين صحيحين نسبيين غير منعدمين
❖ نرسم للقاسم المشترك الأكبر ل a و b : $\Delta(a,b)$ أو $\text{pgcd}(a,b)$ أو $a \wedge b$ و هو أكبر قاسم مشترك موجب
قطعا للعددين a و b

• ليكن a و b من \mathbb{Z}^*

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

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

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

• خوارزمية أقليدس

ليكن a و b من \mathbb{N}^*

إذا كان r هو باقي قسمة a على b ($\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$) فإن $a \wedge b = b \wedge r$

• ليكن a و b من \mathbb{N}^*

القاسم المشترك الأكبر لعددين a و b هو آخر باقي غير منعدم في القسمة المتتالية

4) المضاعف المشترك الأصغر:

ليكن a و b عددين صحيحين نسبيين غير منعدمين
❖ نرمز للمضاعف المشترك الأصغر ل a و b : $M(a,b)$ أو $ppcm(a,b)$ أو $a \vee b$ و هو أصغر مضاعف
مشترك موجب للعددين a و b

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

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

• $(a \wedge b) \times (a \vee b) = |ab|$

• $(ac \vee bc) = |c| \cdot (a \vee b)$

5) الأعداد الأولية فيما بينها:

❖ ليكن a و b من \mathbb{Z}^*
 a و b أوليان فيما بينهما إذا وفقط إذا كان $a \wedge b = 1$

مبرهنة بوزو (Bezout)

ليكن a و b من \mathbb{Z}^*

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

❖ ليكن a و b و c من \mathbb{Z}^*

$$ac \wedge bc = |c| \cdot (a \wedge b)$$

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

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

❖ ليكن a و b و c من \mathbb{Z}^*

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

مبرهنة كوص (Gauss)

$$\text{ليكن } a \text{ و } b \text{ و } c \text{ من } \mathbb{Z}^* \begin{cases} a/c \\ b/c \end{cases} \Rightarrow ab/c \\ a \wedge b = 1$$

$$\text{ليكن } a \text{ و } b \text{ من } \mathbb{Z}^* \text{ و } n \in \mathbb{N}^* \begin{cases} ax \equiv ay [n] \\ a \wedge n = 1 \end{cases} \Rightarrow x \equiv y [n]$$

(6) حل المعادلة $ax + by = c$ في \mathbb{Z}^2 :

نعتبر المعادلة $ax + by = c$ حيث a و b من \mathbb{Z}^* و c من \mathbb{Z} و نضع $a \wedge b = d$

- المعادلة $ax + by = c$ تقبل حلا في \mathbb{Z}^2 إذا و فقط إذا كان d/c
- نفترض أن الزوج (x_0, y_0) حل خاص للمعادلة $ax + by = c$

$$S = \left\{ \left(x_0 + k \frac{b}{d}; y_0 - k \frac{a}{d} \right) / k \in \mathbb{Z} \right\} \text{ هي مجموعة حلول المعادلة } ax + by = c$$

(7) الأعداد الأولية :

$$\diamond \text{ ليكن } p \in \mathbb{Z}^* \setminus \{-1, 1\}$$

نقول أن p أولي إذا و فقط إذا كان له أربع قواسم بالضبط : 1 و -1 و p و $-p$

ملاحظة :

- إذا كان p أولي فإن $-p$ أولي
- طريقة لتحديد الأعداد الأولية الموجبة :

$$\text{ليكن } n \in \mathbb{N}^* \setminus \{1\} \text{ للتحقق هل } n \text{ أولي :}$$

$$\blacksquare \text{ أولا نحسب } \sqrt{n}$$

$$\blacksquare \text{ ثانيا نحدد جميع الأعداد الأولية الأصغر من } \sqrt{n}$$

- إذا كان n لا يقبل القسمة على أي من هذه الأعداد الأولية الأصغر من جذر مربعه فهو يكون أوليا
أما إذا قبل القسمة على أحدها فهو غير أولي

$$\begin{aligned} & \checkmark \text{ ليكن } a_1, a_2, \dots, a_n \text{ من } \mathbb{Z} \text{ و } p \text{ عدد أولي} \\ & p / a_1 \times a_2 \times \dots \times a_n \Rightarrow (\exists i \in \{1, 2, \dots, n\}) : p / a_i \\ & \checkmark \text{ ليكن } p, p_1, p_2, \dots, p_n \text{ أعداد أولية} \\ & p / p_1 \times p_2 \times \dots \times p_n \Rightarrow (\exists i \in \{1, 2, \dots, n\}) : |p| = |p_i| \end{aligned}$$

(8) مبرهنة فيرما :

$$\begin{aligned} & \text{ليكن } p \text{ عدد أولي موجب ، لدينا :} \\ & (\forall a \in \mathbb{Z}) \quad a^p \equiv a [p] \quad \triangleright \\ & a \wedge p = 1 : \text{ بحيث } (\forall a \in \mathbb{Z}) \quad a^{p-1} \equiv 1 [p] \quad \triangleright \end{aligned}$$

(9) نظمت العد :

$$\begin{aligned} & \diamond \text{ ليكن } b \in \mathbb{N}^* \setminus \{1\} \\ & \text{كل عدد } n \text{ من } \mathbb{N}^* \text{ يكتب بطريقة وحيدة على شكل : } n = a_p b^p + a_{p-1} b^{p-1} + \dots + a_1 b + a_0 \\ & \text{بحيث : لكل } i \text{ من } \{0, 1, 2, \dots, p\} \text{ و } a_i \in \mathbb{N} \text{ و } a_p \neq 0 \text{ و } 0 \leq a_i < b \\ & \text{و نكتب } n = \overline{a_p a_{p-1} \dots a_1 a_0}_{(b)} \end{aligned}$$

❖ نعتبر العدد $n = \overline{a_p a_{p-1} \dots a_1 a_0}_{(10)}$

$$2/n \Leftrightarrow a_0 \text{ زوجي} \bullet$$

$$3/n \Leftrightarrow 3 / \sum_{i=0}^{i=p} a_i \bullet$$

$$4/n \Leftrightarrow 4 / \overline{a_1 a_0} \bullet$$

$$5/n \Leftrightarrow a_0 \in \{0, 5\} \bullet$$

$$9/n \Leftrightarrow 9 / \sum_{i=0}^{i=p} a_i \bullet$$

$$11/n \Leftrightarrow \sum_{i:\text{pair}} a_i \equiv \sum_{i:\text{impair}} a_i [11] \bullet$$

$$25/n \Leftrightarrow \overline{a_1 a_0} \in \{\overline{00}, \overline{25}, \overline{50}, \overline{75}\} \bullet$$