باب 3

القواسم والمضاعفات والموافقات في $\mathbb{Z}$

1.3 القسمة الإقليدية والقاسم المشترك الأكبر

تعريف 1.3: القاسم

ليكن $a, b \in \mathbb{Z}$. نقول أن b يقسم a ونرمز $b \mid a$ إذا وجد $q \in \mathbb{Z}$ بحيث:

$$a = bq$$

مثال 1.3: أمثلة على القسمة

- $21 \mid 7$ ، $48 \mid 6$ ، a زوجي إذا وفقط إذا كان $2 \mid a$
- لكل $a \in \mathbb{Z}$ لدينا $a \mid 0$ وأيضاً $1 \mid a$
- إذا كان $1 \mid a$ فإن $a = +1$ أو $a = -1$
- $(a \mid b \text{ و } b \mid a) \implies b = \pm a$
- $(a \mid b \text{ و } b \mid c) \implies a \mid c$
- $(a \mid b \text{ و } a \mid c) \implies a \mid b + c$

نظرية 1.3: القسمة الإقليدية

ليكن $a \in \mathbb{Z}$ و $b \in \mathbb{N} \setminus \{0\}$. يوجد عددان صحيحان $q, r \in \mathbb{Z}$ بحيث:

$$a = bq + r \quad \text{و} \quad 0 \leq r < b$$

علاقة على ذلك q و r وحيدان.

ملاحظة 1.3: مصطلحات القسمة الإقليدية

المصطلحات: q هو حاصل القسمة و r هو باقي القسمة.
لدينا إذاً التكافؤ: $r = 0$ إذا وفقط إذا كان b يقسم a.

2.3 القاسم المشترك الاكبر

تعريف 2.3: القاسم المشترك الأكبر

ليكن $a, b \in \mathbb{Z}$ عددين صحيحين، غير منعدمين معاً. أكبر عدد صحيح يقسم كلاً من a و b يسمى القاسم المشترك الأكبر لـ a, b ويرمز له بـ $\gcd(a, b)$.

مثال 2.3: أمثلة على القاسم المشترك الأكبر

- $\gcd(21, 14) = 7$، $\gcd(12, 32) = 4$، $\gcd(21, 26) = 1$
- $\gcd(a, ka) = a$، لكل $k \in \mathbb{Z}$ و $a \neq 0$
- حالات خاصة. لكل $a \neq 0$: $\gcd(a, 0) = a$ و $\gcd(a, 1) = 1$

نظرية 2.3: خاصية القاسم المشترك الأكبر في القسمة

ليكن $a, b \in \mathbb{N}^*$. لنكتب القسمة الإقليدية $a = bq + r$. فإن:

$$\gcd(a, b) = \gcd(b, r)$$

خوارزمية 1.3: خوارزمية إقليدس

نريد حساب القاسم المشترك الأكبر لـ $a, b \in \mathbb{N}^*$. يمكننا افتراض $a \geq b$. نحسب قسمات إقليدية متتالية. القاسم المشترك الأكبر سيكون آخر باقي غير منعدم.

- قسمة a على b، $a = bq_1 + r_1$. بواسطة الخاصية، $\gcd(a, b) = \gcd(b, r_1)$ وإذا كان $r_1 = 0$ فإن $\gcd(a, b) = b$ وإلا نكمل:
- $b = r_1 q_2 + r_2$، $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2)$
- $r_1 = r_2 q_3 + r_3$، $\gcd(a, b) = \gcd(r_2, r_3)$
- $\cdots$
- $r_{k-2} = r_{k-1} q_k + r_k$، $\gcd(a, b) = \gcd(r_{k-1}, r_k)$
- $r_{k-1} = r_k q_k + 0$، $\gcd(a, b) = \gcd(r_k, 0) = r_k$

بما أن الباقي في كل خطوة أصغر من المقسوم عليه، فإن $0 \leq r_{i+1} < r_i$. وبالتالي تنتهي الخوارزمية لأننا متأكدون من الحصول على باقي منعدم، حيث تشكل البواقي متتالية تناقصية من الأعداد الصحيحة الموجبة أو المنعدمة: $b > r_1 > r_2 > \cdots \geq 0$.

مثال 3.3: حساب القاسم المشترك الأكبر

لنحسب القاسم المشترك الأكبر لـ $a = 600$ و $b = 124$.

$$\begin{aligned} 600 &= 124 \times 4 + 104 \\ 124 &= 104 \times 1 + 20 \\ 104 &= 20 \times 5 + 4 \\ 20 &= 4 \times 5 + 0 \end{aligned}$$

إذن $\gcd(600, 124) = 4$.

مثال 4.3: حساب القاسم المشترك الأكبر

لنحسب $\gcd(9945, 3003)$.

$$\begin{aligned} 9945 &= 3003 \times 3 + 936 \\ 3003 &= 936 \times 3 + 195 \\ 936 &= 195 \times 4 + 156 \\ 195 &= 156 \times 1 + 39 \\ 156 &= 39 \times 4 + 0 \end{aligned}$$

إذن $\gcd(9945, 3003) = 39$.

3.3 الأعداد الأولية فيما بينها

تعريف 3.3: الأعداد الأولية فيما بينها

عددان صحيحان a, b أوليان فيما بينها إذا كان $\gcd(a, b) = 1$.

مثال 5.3: أعداد أولية فيما بينها

لكل $a \in \mathbb{Z}$، a و $a + 1$ أوليان فيما بينها. بالفعل ليكن d قاسماً مشتركاً لـ a و $a + 1$. فإن: d يقسم أيضاً $a + 1 - a$. إذن d يقسم 1 ولكن حينئذ $d = -1$ أو $d = +1$. القاسم الأكبر لـ a و $a + 1$ هو إذاً 1. وبالتالي $\gcd(a, a + 1) = 1$.

مثال 6.3: التحليل باستخدام القاسم المشترك الأكبر

لأي عددين صحيحين $a, b \in \mathbb{Z}$، لنضع $d = \gcd(a, b)$. التحليل التالي غالباً ما يكون مفيداً:

$$\begin{cases} a = a'd \\ b = b'd \end{cases} \quad \text{مع} \quad a', b' \in \mathbb{Z} \quad \text{و} \quad \gcd(a', b') = 1$$

نظرية 3.3: نظرية بيزو

ليكن a, b عددين صحيحين. يوجد عددان صحيحان $u, v \in \mathbb{Z}$ بحيث:

$$au + bv = \gcd(a, b)$$

ملاحظة 2.3: معاملات بيزو

العددان الصحيحان u, v هما معاملات بيزو. يتم الحصول عليهما بـ "الرجوع إلى الخلف" في خوارزمية إقليدس.

مثال 7.3: حساب معاملات بيزو

لنحسب معاملات بيزو لـ $a = 600$ و $b = 124$. نعيد الحسابات التي أجريناها لإيجاد $\gcd(600, 124) = 4$. الجزء الأيسر هو خوارزمية إقليدس. الجزء الأيمن يُحصل عليه من الأسفل إلى الأعلى. نعبر عن القاسم المشترك الأكبر باستخدام السطر الأخير حيث الباقي غير منعدم. ثم نستبدل باقي السطر السابق، وهكذا حتى نصل إلى السطر الأول.

$$\begin{aligned} 600 &= 124 \times 4 + 104 & 4 &= 600 \times 6 + 124 \times (-29) \\ 124 &= 104 \times 1 + 20 & 4 &= 124 \times (-5) + (600 - 124 \times 4) \times 6 \\ 104 &= 20 \times 5 + 4 & 4 &= 124 \times (-5) + 104 \times 6 \\ 20 &= 4 \times 5 + 0 & 4 &= 104 - 20 \times 5 \end{aligned}$$

إذن من أجل $u = 6$ و $v = -29$ يكون $600 \times 6 + 124 \times (-29) = 4$.

مثال 8.3: حساب معاملات بيزو

لنحسب معاملات بيزو المطابقة لـ $\gcd(9945, 3003) = 39$.

$$
\begin{aligned}
9945 &= 3003 \times 3 + 936 & 39 &= 9945 \times (-16) + 3003 \times 53\\
3003 &= 936 \times 3 + 195 & 39 &= \cdots\\
936 &= 195 \times 4 + 156 & 39 &= \cdots\\
195 &= 156 \times 1 + 39 & 39 &= 195 - 156 \times 1\\
156 &= 39 \times 4 + 0
\end{aligned}
$$

عليك إنهاء الحسابات. نحصل على $39 = 3003 \times 53 + 9945 \times (-16)$.

نتيجة 1.3: خاصية القاسم المشترك

إذا كان $d \mid a$ و $d \mid b$ فإن $d \mid \gcd(a, b)$.

مثال 9.3: توضيح خاصية القاسم المشترك

مثال: $16 \mid 4$ و $24 \mid 4$ إذن 4 يجب أن يقسم $\gcd(16, 24)$ الذي يساوي فعلاً 8.

نتيجة 2.3: معيار أولية الأعداد

ليكن a, b عددين صحيحين. a و b أوليان فيما بينها إذا وفقط إذا وجد $u, v \in \mathbb{Z}$ بحيث:

$$au + bv = 1$$

$\Rightarrow \gcd(a, b) = 1$

برهان 1.3: برهان معيار أولية الأعداد

الاتجاه $\Rightarrow$ هو نتيجة لنظرية بيزو.
للإتجاه $\Leftarrow$ نفترض أنه يوجد u, v بحيث $au + bv = 1$. بما أن $\gcd(a, b) \mid a$ فإن $\gcd(a, b) \mid au$. بالمثل $\gcd(a, b) \mid bv$. إذن $\gcd(a, b) \mid au + bv = 1$. إذن $\gcd(a, b) = 1$.

ملاحظة 3.3: ملاحظة حول معاملات بيزو

إذا وجدنا عددين صحيحين u', v' بحيث $au' + bv' = d$، فإن هذا لا يعني أن $d = \gcd(a, b)$.

نعلم فقط حينئذ أن $d \mid \gcd(a,b)$. على سبيل المثال $a = 12, b = 8$; $12\times1+8\times3 = 36$ و $\gcd(a,b) = 4$.

نتيجة 3.3: توطئة غوس

ليكن $a, b, c \in \mathbb{Z}$. إذا كان $a \mid bc$ و $\gcd(a,b) = 1$ فإن $a \mid c$.

برهان 2.3: برهان توطئة غوس

بما أن $\gcd(a,b) = 1$ فإنه يوجد $u, v \in \mathbb{Z}$ بحيث $au + bv = 1$. نضرب هذه المساواة في c للحصول على $acu + bcv = c$. لكن $a \mid acu$ وبالافتراض $a \mid bcv$ إذن a يقسم $acu + bcv = c$.

مثال 10.3: تطبيق توطئة غوس

مثال: إذا كان $4 \mid 7 \times c$، وبما أن 4 و 7 أوليان فيما بينها، فإن $4 \mid c$.

4.3 معادلات $ax + by = c$

مبرهنة 1.3: حل معادلات ديوفانتوس

نعتبر المعادلة

$$ax + by = c \quad (E)$$

حيث $a, b, c \in \mathbb{Z}$.

1. المعادلة (E) تقبل حلولاً $(x,y) \in \mathbb{Z}^2$ إذا وفقط إذا كان $\gcd(a,b) \mid c$.
2. إذا كان $\gcd(a,b) \mid c$ فإنه يوجد حتى عدد لا نهائي من الحلول الصحيحة وهي بالضبط $(x,y) = (x_0 + \alpha k, y_0 + \beta k)$ مع $x_0, y_0, \alpha, \beta \in \mathbb{Z}$ ثابتة و k يجتاز $\mathbb{Z}$.

مثال 11.3: حل معادلة ديوفانتوس

إيجاد الحلول الصحيحة للمعادلة:

$$161x + 368y = 115 \quad (E)$$

• **الخطوة الأولى.** هل توجد حلول؟ خوارزمية إقليدس. ننفذ خوارزمية إقليدس لحساب القاسم المشترك الأكبر لـ $a = 161$ و $b = 368$.

$$\begin{aligned} 368 &= 161 \times 2 + 46 \\ 161 &= 46 \times 3 + 23 \\ 46 &= 23 \times 2 + 0 \end{aligned}$$

إذن $\gcd(368, 161) = 23$. بما أن $115 = 5 \times 23$ فإن $\gcd(368, 161) \mid 115$. طبقاً لنظرية بيزو، المعادلة (E) تقبل حلولاً صحيحة.

• **الخطوة الثانية.** إيجاد حل خاص: الرجوع في خوارزمية إقليدس. ننفذ الرجوع في خوارزمية إقليدس لحساب معاملات بيزو.

$$\begin{aligned} 368 &= 161 \times 2 + 46 \\ 161 &= 46 \times 3 + 23 \\ 46 &= 23 \times 2 + 0 \end{aligned}$$

$$\begin{aligned} 23 &= 161 \times 7 + 368 \times (-3) \\ 23 &= 161 + (368 - 2 \times 161) \times (-3) \\ 23 &= 161 - 3 \times 46 \end{aligned}$$

نجد إذاً $161 \times 7 + 368 \times (-3) = 23$. بما أن $115 = 5 \times 23$ بالضرب في 5 نحصل على:

$$161 \times 35 + 368 \times (-15) = 115$$

هكذا $(x_0, y_0) = (35, -15)$ هو حل خاص للمعادلة (E).

• **الخطوة الثالثة.** البحث عن جميع الحلول. ليكن $(x, y) \in \mathbb{Z}^2$ حلاً للمعادلة (E). نعلم أن (x_0, y_0) هو أيضاً حل. هكذا:

$$161x_0 + 368y_0 = 115 \quad \text{و} \quad 161x + 368y = 115$$

(لا فائدة من تعويض x_0 و y_0 بقيمتهما). طرح هاتين المعادلتين يؤدي إلى:

$$161 \times (x - x_0) + 368 \times (y - y_0) = 0$$

$$\Rightarrow 23 \times 7 \times (x - x_0) + 23 \times 16 \times (y - y_0) = 0$$
$$\Rightarrow 7(x - x_0) = -16(y - y_0) \quad (*)$$

لقد بَسَّطنا بـ 23 وهو القاسم المشترك الأكبر لـ 161 و 368. (انتباه، لا تنسوا هذا التبسيط، وإلا سيكون الاستنتاج التالي خاطئاً.)

هكذا $7 \mid 16(y - y_0)$، وبما أن $\gcd(7, 16) = 1$ فطبقاً للغة غاوس $7 \mid y - y_0$. يوجد إذاً $k \in \mathbb{Z}$ بحيث $y - y_0 = 7 \times k$. بالعودة إلى المعادلة $(*)$: $7(x - x_0) = -16(y - y_0)$. نحصل الآن على $7(x - x_0) = -16 \times 7 \times k$ إذن $x - x_0 = -16k$. (نفس k لـ x و y). لدينا إذاً $(x, y) = (x_0 - 16k, y_0 + 7k)$. ليس صعباً رؤية أن أي زوج من هذا الشكل هو حل للمعادلة (E). يبقى فقط تعويض (x_0, y_0) بقيمتهما فنحصل على:
الحلول الصحيحة لـ $161x + 368y = 115$ هي $(x, y) = (35 - 16k, -15 + 7k)$، حيث k يجتاز $\mathbb{Z}$.
للتأكد، خذوا قيمة عشوائية لـ k وتحققوا من أنكم تحصلون فعلاً على حل للمعادلة.

5.3 المضاعف المشترك الاصغر

تعريف 4.3: أصغر مضاعف مشترك

أصغر مضاعف مشترك لـ a, b هو أصغر عدد صحيح ≥ 0 يقبل القسمة على a و b.

مثال 12.3: أصغر مضاعف مشترك

على سبيل المثال $\operatorname{lcm}(12, 9) = 36$.

القاسم المشترك الأكبر وأصغر مضاعف مشترك مرتبطان بالصيغة التالية:

مبرهنة 2.3: العلاقة بين القاسم المشترك الأكبر وأصغر مضاعف مشترك

إذا كان a, b عددين صحيحين (غير منعدمين معاً) فإن:

$$\gcd(a, b) \times \operatorname{lcm}(a, b) = |ab|$$

برهان 3.3: برهان العلاقة بين القاسم المشترك الأكبر وأصغر مضاعف مشترك

نضع $d = \gcd(a,b)$ و $m = \frac{|ab|}{\gcd(a,b)}$. للتبسيط نفترض $a > 0$ و $b > 0$. نكتب $a = da'$ و $b = db'$. إذن $ab = d^2a'b'$ وبالتالي $m = da'b'$. إذن $m = ab' = a'b$ هو مضاعف لـ a و b.

يبقى أن نبين أنه أصغر مضاعف. إذا كان n مضاعفاً آخر لـ a و b فإن $n = ka = \ell b$ إذن $kda' = \ell db'$ و $ka' = \ell b'$. لكن $\gcd(a',b') = 1$ و $a' \mid \ell b'$ إذن $a' \mid \ell$. إذن $a'b \mid \ell b$ وهكذا $m = a'b \mid \ell b = n$.

مبرهنة 3.3: خاصية أصغر مضاعف مشترك

إذا كان $a \mid c$ و $b \mid c$ فإن $\operatorname{lcm}(a,b) \mid c$.

6.3 الموافقات (Congruences)

تعريف 5.3: الموافقة

ليكن $n \geq 2$ عدداً صحيحاً. نقول أن a موافق لـ b بتردد n، إذا كان n يقسم $b - a$. نرمز حينئذ:

$$a \equiv b \pmod{n}$$

ملاحظة 4.3: رموز وصيغ أخرى للموافقة

نرمز أحياناً بـ $a = b \pmod{n}$ أو $a \equiv b[n]$. صيغة أخرى هي:

$$a \equiv b \pmod{n} \iff \exists k \in \mathbb{Z} \quad a = b + kn$$

ملاحظة 5.3: علاقة الموافقة بالقسمة

لاحظ أن n يقسم a إذا وفقط إذا كان $a \equiv 0 \pmod{n}$.

مبرهنة 4.3: خصائص الموافقات

1. علاقة «الموافقة بتردید n» هي علاقة تكافؤ:
   - (انعكاسية) $a \equiv a \pmod{n}$
   - (تناظرية) إذا كان $a \equiv b \pmod{n}$ فإن $b \equiv a \pmod{n}$
   - (متعدية) إذا كان $a \equiv b \pmod{n}$ و $b \equiv c \pmod{n}$ فإن $a \equiv c \pmod{n}$
2. إذا كان $a \equiv b \pmod{n}$ و $c \equiv d \pmod{n}$ فإن $a + c \equiv b + d \pmod{n}$
3. إذا كان $a \equiv b \pmod{n}$ و $c \equiv d \pmod{n}$ فإن $a \times c \equiv b \times d \pmod{n}$
4. إذا كان $a \equiv b \pmod{n}$ فإن لكل $k \geq 0$، $a^k \equiv b^k \pmod{n}$

برهان 4.3: برهان خصائص الموافقات

1. سهل.
2. سهل
3. لنبرهن الخاصية الضربية: $a \equiv b \pmod{n}$ إذن يوجد $k \in \mathbb{Z}$ بحيث $a = b + kn$ و $c \equiv d \pmod{n}$ إذن يوجد $\ell \in \mathbb{Z}$ بحيث $c = d + \ell n$. إذن:

$$a \times c = (b + kn) \times (d + \ell n) = bd + (b\ell + dk + k\ell n)n$$

   وهو بالضبط على الشكل $bd + mn$ مع $m \in \mathbb{Z}$. إذن $ac \equiv bd \pmod{n}$.
4. هذه نتيجة للنقطة السابقة: مع $a = c$ و $b = d$ نحصل على $a^2 \equiv b^2 \pmod{n}$. نكمل بالاستقراء.

7.3 تمارين

تمرين 1.3

مع العلم أنّ:

$$96842 = 256 \times 375 + 842$$

أوجد، **دون إجراء القسمة**، باقي قسمة العدد 96842 على كلٍّ من العددين 256 و 375.

تمرين 2.3

بين أن $\forall n \in \mathbb{N}$:

$n(n+1)(n+2)(n+3)$ يقبل القسمة على 24,

$n(n+1)(n+2)(n+3)(n+4)$ يقبل القسمة على 120.

تمرين 3.3

بين أنه إذا كان n عددا طبيعيا مجموع مربعي عددين صحيحين، فإن باقي قسمة n على 4 لا يساوي أبدا 3.

تمرين 4.3

بين أن العدد $7^n + 1$ يقبل القسمة على 8 إذا كان n فرديا، وفي حالة n زوجي، أعط باقي قسمته على 8.

تمرين 5.3

أوجد باقي قسمة العدد 100^{1000} على 13.

تمرين 6.3

احسب القاسم المشترك الأكبر للأعداد التالية:

1. 126, 230

2. $390,\ 720,\ 450$

3. $180,\ 606,\ 750$

تمرين 7.3

احسب باستعمال خوارزمية إقليدس: $\text{pgcd}(18480, 9828)$. واستنتج كتابة العدد 84 على شكل combinasion خطية للعددين 18480 و 9828.

تمرين 8.3

حل في $\mathbb{Z}$ المعادلة: $1665x + 1035y = 45$.

تمرين 9.3

بين أنه إذا كان a و b عددين صحيحين أوليين فيما بينهما، فإن $a + b$ و ab أوليان فيما بينهما أيضاً.

تمرين 10.3

ليكن a و b عددين صحيحين أكبر من أو يساوي 1. بين أن:

1. $(2^a - 1) \mid (2^{ab} - 1)$
2. $2^p - 1$ أولي $\Rightarrow p$ أولي
3. $\text{pgcd}(2^a - 1, 2^b - 1) = 2^{\text{pgcd}(a,b)} - 1$