الفصل الثاني

الأعداد الصحيحة

Integers

في هذا الفصل نقدم بعض المفاهيم والخواص المتعلقة بالأعداد الصحيحة التي سوف يتعرض لها القارئ خلال هذا الكتاب. هنا لن نعطي الخواص في صورة مسلمات ولكن سوف نفترض أن القارئ على دراية بعمليتي جمع وضرب الأعداد الصحيحة والخواص الأساسية لهذه العمليات.

نبدأ أولا ببعض المفاهيم والمصطلحات . العدد الصحيح b يسمى عامل factor أو قاسم divisor للعدد الصحيح a إذا وجد عدد صحيح c بحيث يكون $a=bc$. في هذه الحالة a يسمى مضاعف b multiple . إذا كان b قاسم لـ a فنقول أن b يقسم a ونرمز لذلك بالصورة $b|a$ ($b\nmid a$ تعني أن b لا تقسم a).

لاحظ أنه إذا كان $b|g$ و $b|h$ فإن $b|(mg+nh)$ لأي عددين صحيحين m و n. نترك التحقق منها كتمرين.

تعريف ٢-١. العدد الصحيح الموجب d يسمى قاسم مشترك أكبر greatest common divisor للعددين الصحيحين a و b إذا كان

(i) $d|a$ و $d|b$

(ii) إذا كان $c|a$ و $c|b$ فإن $c|d$.

نرمز للقاسم المشترك الأكبر للعددين الصحيحين a و b بالصورة (a,b) أو $\gcd(a,b)$.

مجموعة الأعداد الصحيحة integers يرمز لها بالرمز $\mathbb{Z}$ ومجموعة الأعداد الصحيحة الموجبة ، وتسمى أيضا مجموعة الأعداد الطبيعية natural numbers يرمز لها بالرمز $\mathbb{N}$.

المجموعة الجزئية غير الخالية S من $\mathbb{Z}$ تسمى مرتبة جيدا well-ordered إذا كانت S تحتوي أصغر عنصر least element. لاحظ أن $\mathbb{Z}$ ليست مرتبة جيدا لأنها لا تحتوي أصغر عنصر ومع ذلك مجموعة الأعداد الطبيعية $\mathbb{N}$ تكون مرتبة جيدا.

مبدأ الترتيب الجيد Principle of Well-Ordering

كل مجموعة جزئية غير خالية من الأعداد الطبيعية $\mathbb{N}$ تكون مرتبة جيدا.

هذه الخاصية مع معرفتنا بجمع وضرب الأعداد الصحيحة تعطينا الأساس لإثبات العديد من الخواص الهامة للأعداد الصحيحة.

الآن نعطي بعض الخواص التي تنتج من خاصية الترتيب الجيد.

مبدأ الاستنتاج الأول First principle of induction

نظرية ٢-٢. نفرض S مجموعة غير خالية من $\mathbb{N}$ بحيث تحقق الخواص التالية:

(i) $1 \in S$ وتسمى خطوة الأساس basic step .

(ii) إذا كان $a \in S$ فإن $a+1 \in S$ وتسمى خطوة الاستنتاج inductive step.

إذن $S = \mathbb{N}$.

البرهان: نفرض $T = \{x \in \mathbb{N} : x \notin S\}$. إذا كانت $T = \phi$ ينتهي البرهان. لذلك نفرض أن $T \neq \phi$. من خاصية الترتيب الجيد يوجد أصغر عنصر. نفرض m هو أصغر عنصر في T . واضح أن $m \neq 1$ لأن $1 \in S$. إذن $m-1 \in S$. ولكن هذا يؤدي إلى $m \in S$ وذلك من (ii). وهذا تناقض. إذن $T = \phi$ وبالتالي $S = \mathbb{N}$.

مبدأ الاستنتاج الثاني Second principle of induction

نظرية ٢-٣. نفرض S مجموعة غير خالية من $\mathbb{N}$ بحيث تحقق الخواص التالية:

(i) $1 \in S$.

(ii) $n \in S$ طالما كان $m \in S$ لكل عدد صحيح m بحيث $n > m$.

إذن $S = \mathbb{N}$.

البرهان: نفرض $T = \{x \in \mathbb{N} : x \notin S\}$. إذا كانت $T = \phi$ ينتهي البرهان. لذلك نفرض أن $T \neq \phi$. من خاصية الترتيب الجيد يوجد أصغر عنصر. نفرض m هو أصغر عنصر في T. من (i) $m \neq 1$. إذن لكل عدد صحيح موجب x بحيث $x < m$ يكون $x \in S$. ولكن من (ii) $m \in S$ وهذا تناقض. إذن $T = \phi$ ويكون $S = \mathbb{N}$.

ملاحظة. مبدأ الاستنتاج الأول ومبدأ الاستنتاج الثاني متكافئان.

نظرية ٢-٤. (خوارزمية القسمة) Division algorithm

نفرض $a,b\in\mathbb{Z}$ و $b>0$. إذن يوجد عدد صحيحان وحيدان $q,r\in\mathbb{Z}$ بحيث $a=bq+r$ حيث $0\le r<b$.

البرهان: نفرض $S=\{a-bx : x\in\mathbb{Z}\}$. واضح أن S تحتوي عدد صحيح موجب a . إذن من خاصية الترتيب الجيد S تحتوي عنصر أصغر عدد صحيح موجب وليكن $m=a-bx$. إذا كان $m>b$ فإن $m-b=a-b(x+1)\in S$ وهذا يناقض اختيار m . إذن $m\le b$.

إذا كان $m=b$ فإن $a-bx=b$ يؤدي إلى $a=b(x+1)$. لذلك نختار $q=x+1$ و $r=0$.

إذا كان $m<b$ نختار $q=x$ و $r=m$.

لإثبات أن العددان وحيدان نفرض أن $a=bq+r=bq'+r'$.

إذن $b(q-q')=r-r'$. وحيث أن $|r-r'|<b$ فإن $q-q'=0$.

إذن $q=q'$ ومنها نحصل على $r=r'$.

تعريف ٢-٥. العدد الصحيح غير الصفري p يسمى أولي prime إذا كان $p\neq\pm1$ وعوامل p هي $\pm1,\pm p$ فقط.

وبتعبير آخر نقول أن العدد الصحيح p (>1) يكون أولي إذا وفقط إذا كان لأي عدد صحيح آخر n إما $(p,n)=1$ أو $p\mid n$.

تمهيدية ٢-٦. إذا كان a و b عددان صحيحان ليس كلاهما صفر فإن $\gcd(a,b)$ يكون موجود ووحيد، علاوة على ذلك يمكننا إيجاد عددين صحيحين m_0 و n_0 بحيث $\gcd(a,b)=m_0a+n_0b$.

البرهان: نفرض $M=\{ma+nb : m,n\in\mathbb{Z}\}$. حيث أن أحد العنصرين a و b ليس صفر، إذن M تحتوي أعداد ليست صفرية. وحيث أن $x=ma+nb\in M$ فإن $-x=(-m)a+(-n)b\in M$. لذلك M دائما تحتوي أعداد صحيحة موجبة. إذن M يكون لها أصغر عدد صحيح موجب c في M وبالتالي c يكون على الصورة m_0a+n_0b. سوف نوضح أن $c=\gcd(a,b)$.

لاحظ أنه إذا كان $d\mid a$ و $d\mid b$ فإن $d\mid m_0a+n_0b$ ، لذلك $d\mid c$. الآن يجب أن نبين أن $c\mid a$ و $c\mid b$. نفرض $x=ma+nb$ أي عنصر في M. من خوارزمية القسمة $x=tc+r$ حيث $0\le r<c$. إذن $ma+nb=t(m_0a+n_0b)+r$. إذن $r=(m-t\,m_0)a+(n-t\,n_0)b$ يجب أن تكون في M . وحيث $0\le r$ و $r<c$. من إختيار c ، $r=0$. إذن $x=tc$. إذن نحن أثبتنا أن $c\mid x$ لأي $x\in M$. ولكن $a=1a+0b\in M$ و $b=0a+1b\in M$. إذن $c\mid a$ و $c\mid b$. إذن أثبتنا أن c يحقق خاصية $\gcd(a,b)$ المطلوبة. الآن نبرهن على أن $\gcd(a,b)$

يكون وحيد. نفرض أن $d=\gcd(a,b)$ ونفرض أن d' قاسم مشترك آخر ونود إثبات أن $d'|d$. نفرض $a=d'h$ و $b=d'k$. لذلك $d=ma+nb=md'h+nd'k=d'(mh+nk)$ ومن ثم d' يجب أن يقسم d ويكون d هو القاسم المشترك الأكبر الوحيد. وهذا يكمل البرهان.

نتيجة ٢-٧ . إذا كان a و b أوليان نسبيا فإنه يوجد عددان صحيحان m و n بحيث $ma+nb=1$.

الخوارزمية الإقليدية. Euclidean Algorithm

تمهيدية ٢-٦ تسمح لنا بحساب القاسم المشترك الأكبر لعددين صحيحين.

مثال٢-٨. دعنا نحسب gcd للعددين 945 و 2415. لاحظ أن

$$2415=945\cdot 2+525$$

$$945=525\cdot 1+420$$

$$525=420\cdot 1+105$$

$$420=105\cdot 4+0$$

إذا عكسنا الخطوات نجد أن 105 تقسم 420 ، 105 تقسم 525 ، 105 تقسم 945 و 105 تقسم 2415. لذلك 105 تقسم كلا من 945 و 2415. إذا كان d قاسم مشترك آخر لـ 945 و 2415 فإن d سوف يقسم 105 ومن ثم $\gcd(945,2415)=105$.

إذا عملنا خلال هذه المتتابعة من المعادلات باتجاه عكسي يمكننا الحصول على عددين r و s بحيث $945r+2415s=105$. لاحظ أن

$$\begin{aligned}105&=525+(-1)\cdot 420\\&=525+(-1)\cdot[945+(-1)\cdot 525]\\&=2\cdot 525+(-1)\cdot 945\\&=2\cdot[2415+(-2)\cdot 945]+(-1)\cdot 945\\&=2\cdot 2415+(-5)\cdot 945\end{aligned}$$

لذلك $r=-5$ و $s=2$. لاحظ أن r و s ليسا وحيدان حيث أن $r=41$ و $s=-16$ أيضا تصلح.

لحساب $\gcd(a,b)=d$ استخدمنا تكرار القسمة للحصول على متتابعة تناقصية من الأعداد الصحيحة الموجبة $r_1>r_2>\ldots>r_n=d$. أي أن

$$b=aq_1+r_1$$

$$a=r_1q_2+r_2$$

$$r_1=r_2q_3+r_3$$

$$\vdots$$

$$r_{n-2}=r_{n-1}q_n+r_n$$

$$r_{n-1}=r_nq_{n+1}$$

لإيجاد r و s بحيث $ar+bs=d$ نبدأ من المعادلة الأخيرة ونعوض في المعادلة السابقة لها

$$\begin{aligned} d &= r_n \\ &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= -q_n r_{n-3} + (1+q_n q_{n-1})r_{n-2} \\ &\vdots \\ &= ra + sb \end{aligned}$$

هذه الطريقة التي استخدمناها للحصول على القاسم المشترك الأكبر d لعددين a و b على صورة تركيبة خطية منهما تسمى الخوارزمية الإقليدية.

يقال أن العددان الصحيحان a و b أوليان نسبيا relatively prime (أو a أولي بالنسبة إلى b والعكس) إذا كان $(a,b)=1$. أي إذا كان القاسم المشترك الأكبر لهما هو 1.

تمهيدية ٢-٩. إذا كان $(a,b)=1$ وكان $a|bc$ فإن $a|c$.

البرهان: حيث أن a و b أوليان نسبيا ، من نتيجة ٢-٧ يمكننا إيجاد عددان صحيحان m و n بحيث $ma+nb=1$. لذلك $mac+nbc=c$. الآن $a|mac$ ومن الفرض $a|nbc$ ، إذن $a|(mac+nbc)$. حيث أن $mac+nbc=c$ ، نستنتج أن $a|c$.

نتيجة ٢-١٠. إذا كان عدد أولي يقسم حاصل ضرب أعداد صحيحة فإنه يجب أن يقسم على الأقل أحد هذه الأعداد.

تعريف ٢-١١. نفرض a عدد صحيح. القيمة المطلقة absolute value (أو المقياس modulus) $|a|$ للعدد a تعرف كما يلي

$$|a|=\begin{cases} a & \text{if} \quad a\geq 0 \\ -a & \text{if} \quad a<0 \end{cases}$$

نظرية ٢-١٢. (النظرية الأساسية للحساب)

كل عدد صحيح $n\geq 2$ إما يكون أولي أو يكون حاصل ضرب أعداد أولية.

البرهان: باستخدام مبدأ الاستنتاج، حيث أن 2 عدد أولي، إذن النتيجة تكون صحيحة عندما $n=2$.

نفرض $n>2$. إذا كانت n عدد أولي ، ينتهي البرهان. وإلا نفرض أن $n=ab$ حيث $2\leq a<n$ و $2\leq b<n$. إذا كان a و b أوليان، ينهي البرهان. وإلا نفرض أن $a=p_1p_2...$ و $b=q_1q_2...$. إذن $n=p_1p_2..q_1q_2...$ حيث $p_1,p_2,....$ و $q_1,q_2,....$ أعداد أولية.

تعريف ٢-١٣. نفرض n عدد صحيح موجب و a,b عددان صحيحان. نقول أن a تتآلف congruent مع b بمقياس n إذا كان $a-b$ يقبل القسمة على n (أو n يقسم $a-b$)، أي إذا وجد عدد صحيح k بحيث $a-b=kn$. ونعبر عن ذلك بالصورة $a\equiv b \pmod n$.

مثال٢-١٤.

(أ) $13\equiv 3(\text{mod } 5)$ و $-10\equiv 8 \pmod 6$.

(ب) إذا كان $x \equiv 0 \pmod{m}$ فإن m تقسم x.

(جـ) إذا كانت n تقسم m وكان $x \equiv y \pmod{n}$ فإن $x \equiv y \pmod{m}$.

(د) كل عددين صحيحين يكونا متآلفين بمقياس 2 إذا وفقط إذا كانا زوجيان معا أو فرديان معا.

نظرية ٢-١٥. علاقة التآلف بمقياس n تكون علاقة تكافؤ على مجموعة الأعداد الصحيحة لأي $n \in \mathbb{Z}$.

البرهان : نفرض R هي علاقة التآلف بمقياس n على مجموعة الأعداد الصحيحة، أي نفرض أن aRb إذا وفقط إذا كان $a \equiv b \pmod{n}$ لكل $a,b \in \mathbb{Z}$.

حيث أن $a-a=0=0n$ ، إذن $a \equiv a \pmod{n}$ أي aRa وتكون R عاكسة.

نفرض $a,b \in \mathbb{Z}$ بحيث aRb . إذن يوجد $r \in \mathbb{Z}$ بحيث $a-b=rn$. إذن $b-a=-nr=n(-r)$ حيث $-r \in \mathbb{Z}$. إذن bRa وتكون R متماثلة.

أخيرا نفرض أن aRb و bRc . إذن يوجد $r,s \in \mathbb{Z}$ بحيث $a-b=rn$ و $b-c=sn$.

إذن $a-c=(a-b)+(b-c)=rn+sn=(r+s)n$. وحيث أن $r+s \in \mathbb{Z}$ ، إذن aRc وتكون R متعدية وبالتالي علاقة تكافؤ.

تعريف ٢-١٦ . نفرض $x \in \mathbb{Z}$. فصل التكافؤ

$$[x]=\{y \in \mathbb{Z}: x \equiv y \pmod{}\}$$

يسمى فصل انتلاف x مقياس n ويرمز له أحيانا بالرمز $\overline{x}$.

مثال ٢-١٧.

(ا) يوجد فصلا انتلاف مقياس 2 ، مجموعة الأعداد الزوجية ومجموعة الأعداد الفردية.

(ب) يوجد أربعة فصول انتلاف مقياس 4

$$\bar{0}=\{...,-8,-4,0,4,8,...\}$$

$$\bar{1}=\{...,-7,-3,1,5,9,...\}$$

$$\bar{2}=\{...,-6,-2,2,6,10,...\}$$

$$\bar{3}=\{...,-5,-1,3,7,11,...\}$$

على وجه العموم يوجد عدد n فصل انتلاف مقياس n

$$\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}$$

مجموعة فصول الانتلاف مقياس n يرمز لها بالرمز $\mathbb{Z}_n$ ، أي أن

$$\mathbb{Z}_n=\{\bar{0},\bar{1},\bar{2},...,\overline{n-1}\}$$

تمارين ٢

١- نفرض $a|b$ و $b|a$ أثبت أن $a=\pm b$.

٢- إذا كان b يقسم كلا من g و h بين أن b أيضا يقسم $mg+nh$.

٣- إذا كان $a|x$ و $b|x$ و $(a,b)=1$ فبرهن على أن $(ab)|x$.

٤- نفرض $(m,n)=1$. إذا أعطينا a و b فبرهن على أنه يوجد x بحيث $x\equiv a \bmod m$ و $x\equiv b \bmod n$.

٥- برهن على أن n يكون أولي إذا وفقط إذا كان في $\mathbb{Z}_n$ $[a][b]=[0]$ يؤدي إلى $[a]=[b]=[0]$.

٦- نفرض a و b عددان صحيحان، المضاعف المشترك الأصغر لـ a و b يرمز له بالرمز $[a,b]$ ويعرف بأنه العدد الصحيح الموجب d بحيث (i) $a|d$ و $b|d$ و (ii) كلما كان $a|x$ و $b|x$ فإن $d|x$. برهن أن $[a,b]$ موجود وأن $[a,b]=\frac{ab}{(a,b)}$ إذا كان $a>0$ و $b>0$.