الفصل الثاني

نظرية الأعداد

مقدمة:

تهتم نظرية الأعداد بدراسة الأعداد الصحيحة، ودراسة خواصها، سنقوم بمراجعة بعض المفاهيم الأساسية في نظرية الأعداد وتطويرها فيما يخدم الحاجة إلى استخدامها في تطبيقات علوم الحاسب.

الأعداد الصحيحة:

تستخدم الأعداد الصحيحة عند مناقشة تقنيات الإحداثيات وهذه الأعداد هي:

$$\ldots - 4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$$

ونرمز لمجموعة الأعداد الصحيحة بالرمز $\mathbb{Z}$ وتقسم إلى مجموعتين، مجموعة الأعداد الزوجية (even):

$$-4, -2, 0, 2, 4, \ldots$$

مجموعة الأعداد الفردية odd:

$$-5, -3, -1, 3, 5, \ldots$$

يأخذ العدد الصحيح الزوجي الشكل $2n$ حيث n عدد صحيح ما.

ويأخذ العدد الصحيح الفردي الشكل $2n + 1$ من أجل n عدد صحيح ما.

العمليات الأساسية وخواصها:

نعلم أن العمليات الأساسية على الأعداد هي (الجمع – والطرح – الضرب والقسمة).

إن عمليتي الجمع والضرب تتمتع بالخواص التالية:

من أجل $m, n, k \in \mathbb{Z}$

١ – الخاصة التبديلية:

$$m + n = n + m$$
$$m . n = n . m$$

٢ – الخاصة التجميعية:

$$(m + n) + k = m + (n + k)$$
$$(m . n) . k = m . (n . k)$$

٣ – خاصة التوزيع:

1) $m(n + k) = (m . n) + (m . k)$
2) $(m + n) = mk + nk$

تمثيل الأعداد الصحيحة:

نفرض b عدداً صحيحاً موجباً أكبر من الواحد، إذا كان n عدداً صحيحاً موجباً عندها يمكن تمثيله بالشكل:

$$n = a_k b^k + a_{k-1} b^{k-1} \dots + a_1 b + a_0$$

حيث k هو عدد صحيح غير سالب وكذلك $a_0, \ a_1,\dots,a_k$ هي أعداد صحيحة غير سالبة أقل من b، $a_k \neq 0$. يفيدنا هذا الشكل بكتابة العدد الصحيح في أنظمة العد المختلفة.

قابلية القسمة:

خوارزمية القسمة:

من أجل أي عددين صحيحين $b, \ a$ حيث أحدهما وليكن a موجباً فإنه يوجد عددان صحيحان وحيدان q , بحيث تتحقق العلاقة:

$$b = qa + r \qquad 0 \le r < a$$

نسمي q ناتج قسمة b على a، r باقي القسمة وإذا كان $r = 0$ يتحقق التكافؤ الآتي:

$$a|b \Leftrightarrow b = q\,a \Leftrightarrow r = 0$$

قابلية القسمة:

تعريف:

نقول عن عدد صحيح مختلف عن الصفر a إنه قاسم (divisor) للعدد الصحيح b وكتب a|b إذا وفقط إذا وجد عدد صحيح c يحقق b = c . a وإذا لم يتحقق ذلك نقول إن a لا يقسم b ونكتب $a \nmid b$.

مثال:

4 يقسم 12 لأن $4 \times 3 = 12$ ونكتب 4|12.

نتائج:

١ – $\forall a \in \mathbb{Z} \Rightarrow a . 1 = a$، وبالتالي 1|a، وإذا كان $a \neq 0$ فإن a|a.

٢ – $a . 0 = 0$ وذلك مهما يكن $a \in \mathbb{Z}$ وبالتالي a|0.

٣ – إن كل قاسم موجب x لعدد صحيح a يوافقه قاسم سالب x – وبالعكس $x|a \Leftrightarrow -x|a$.

٤ – إذا كان العد الصحيح $a \neq 0$ فإن كلاً من العدد a وقيمته المطلقة |a| يقسم الآخر.

٥ – إذا كان a يقسم كلاً من العددين b, c فإنه يقسم أي تركيب خطي لهما bx + cy حيث y,x عددين صحيحين نعبر عن هذه الخاصية رمزياً بالشكل:

$$\forall x,y \in \mathbb{Z} \qquad a|b \wedge a|c \Rightarrow a|(bx + cy)$$

٦ – إذا كان العدد a يقسم العدد b فإن a يقسم حاصل ضرب b بأي عدد صحيح c أي إن:

$$a|b \Rightarrow a|bc \ \forall c \in \mathbb{Z}$$

٧ – إذا كان العدد a يقسم العدد b وكان b بدوره يقسم العدد c فإن a يقسم c أي:

$$a|b \wedge b|c \Rightarrow a|c$$

(نقول إن علاقة القسمة متعدية).

٨ – إذا كان كل من العددين a,b عدداً صحيحاً موجباً وكان a|b فإن $a \le b$ أي أن:

$$a|b \wedge a > 0 \wedge b > 0 \Rightarrow a \le b$$

٩ – إذا كان العدد a يقسم العدد b فإن القيمة المطلقة لـ a تقسم القيمة المطلقة لـ b.

$$a|b \Rightarrow |a| \mid |b|$$

١٠ – إذا كان كل من العدين a, b يقسم الآخر فإن $|a| = |b|$ أي: $(a = \pm b)$

$$a|b \wedge b|a \Rightarrow |a| = |b|$$

١١ – تصنف الأعداد وفق صفات محددة:

أ – كل عدد صحيح b يكتب بالشكل 2k أو 2k+1 حيث k عدد صحيح يتعلق بالعدد b.

ب – إن مربع أي عدد صحيح b يكتب بأحد الشكلين:

4k أو 4k + 1

ملاحظة:

يمكن أن يكون للعدد الصحيح أكثر من قاسم.

الأعداد الأولية:

نقول عن العدد الصحيح $p > 1$ إنه عدد أولي إذا كانت قواسمه الموجبة هي p, 1 فقط.

والعدد الأكبر من 1 وليس بعدد أولي ندعوه عدد مركب.

الأعداد الأولية الأقل من 100 هي:

11	7	5	3	2
29	23	19	17	13
47	43	41	37	31
71	67	61	59	53
97	89	83	79	73

للأعداد الأولية خواص كثيرة هامة للعديد من التطبيقات في علوم الحاسب.

المبرهنة الأساسية في الحساب:

إن أي عدد صحيح أكبر من 1 يمكن أن يكتب بشكل وحيد على أنه أولي أو أنه جداء لعددين أوليين أو أكثر حيث نكتب العوامل الأولية بترتيب غير متناقص.

مثال:

اكتب العوامل الأولية للأعداد التالية:

$$128 \ , 1000 \ , 89 \ , 50$$

$50 = 2 \,.\, 5 \,.\, 5 = 2 \,.\, 5^2$

$89 = 89$

$1000 = 2^3 \,.\, 5^3$

$128 = 2^7$

مبرهنة:

إذا كان n عدداً صحيحاً مركباً فإن للعدد n قاسماً أولياً أصغر أو يساوي $\sqrt{n}$. بتعبير آخر إذا كان العدد الصحيح الموجب n عدداً مركباً فإن للعدد n عاملاً أولياً p بحيث $p^2 \leq n$.

مثال:

أثبت أن 53 هو عدد أولي.

الحل:

أقرب عدد مربع لـ 53 هو 49 وجذر 49 هو 7 هذا يعني أن $\sqrt{53}$ لا يتجاوز 7 ,5 ,3 ,2 والعدد 53 لا يقبل القسمة على أي منه فهو عدد أولي.

ملاحظات هامة:

١ – مجموعة الأعداد الأولية مجموعة غير منتهية.

٢ – كل الأعداد الزوجية أعداد غير أولية عدا 2.

٣ – كل الأعداد التي آحادها 5 هي أعداد غير أولية فقط العدد 5 هو عدد أولي.

٤ – أي عدد يكون مجموع أرقامه من مضاعفات العدد 3 هو عدد غير أولي.

٥ – إن الأعداد الأولية الكبيرة تلعب دوراً هاماً في التعمية (cryptography).

٦ – أعداد ميرسين الأولية هي أعداد تعطى بالعلاقة $2^p - 1$ حيث p هو أولي.

القاسم المشترك الأعظم:

بفرض a ,b عددان صحيحان مغايران للصفر، نعرف القاسم المشترك الأكبر لهما بأنه القاسم الأكبر d بحيث يكون $d|a$ و $d|b$ ونرمز له بالرمز $\gcd(a,b)$.

ملاحظة:

أصغر قواسم العدد هو العدد (1) وأكبر القواسم هو العدد نفسه.

إيجاد القاسم المشترك الأكبر لعددين أو أكثر:

١ – نقوم بتحليل كل عدد إلى عوامله الأولية ونكتبه على شكل جداء قوى.

٢ – يكون القاسم المشترك الأكبر هو جداء قوى العوامل المشتركة بأصغر أس.

بتعبير آخر لإيجاد القاسم المشترك الأكبر لعددين صحيحين a ,b (ليس كلاهما مساوياً للصفر معاً) نكتب العددين بالشكل:

$$a = p_1^{a1} p_2^{a2},\dots,p_n^{an}$$
$$b = p_1^{b1} p_2^{b2},\dots,p_n^{bn}$$

حيث أن كل أس هو عدد صحيح غير سالب، وأن كل الأعداد الأولية التي تحدث في التحليل إلى عوامل أولية في كل من a ,b موجودة في الاثنين معاً بأس صفري إذا كان ضرورياً عندئذ يعطى القاسم المشترك الأعظم من خلال العلاقة:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2 b_2)},\dots,p_n^{\min(a_n b_n)} \qquad (1)$$

الأعداد الأولية النسبية:

نقول عن العددين a ,b بأنهما عددين أوليين نسبياً إذا كان القاسم المشترك الأعظم لها هو 1.

الأعداد الأولية مثنى مثنى:

نقول عن الأعداد الصحيحة $a_1,a_2,\dots,a_n$ بأنها أعداد أولية نسبياً مثنى مثنى إذا كان $\gcd(a_i,a_j) = 1$ ومن أجل كل القيم $1 \le i < j \le n$.

أمثلة:

بين فيما إذا كانت الأعداد التالية أولية نسبياً مثنى مثنى: 17 , 25 , 12.

الحل:

$\gcd(17,25) = 1$
$\gcd(17,12) = 1$
$\gcd(12,25) = 1$

وهذا يعني بأنها أولية مثنى مثنى.

المضاعف المشترك الأصغر:

إن المضاعف المشترك الأصغر للعددين الصحيحين b,a الموجبين هو العدد الصحيح الموجب الأصغر الذي يقسم كلاً من العددين b,a ونرمز للمضاعف المشترك الأصغر للعددين b,a بالرمز Icm(a,b).

ملاحظة:

ليكن b,a عددان صحيحان عندئذ يكون:

$$ab = \gcd(a,b) \,.\, \text{Icm}(a,b)$$

إيجاد المضاعف المشترك الأصغر لعددين أو أكثر:

١ – نحلل كلاً من هذه الأعداد إلى عوامله الأولية.

٢ – يكون المضاعف المشترك الأصغر هو جداء قوى العوامل المشتركة والعوامل غير المشتركة بأكبر أس ظهر عند التحليل.

بتعبير آخر لإيجاد المضاعف المشترك الأصغر لعددين صحيحين b, a نكتب العددين بالشكل:

$$a = p_1^{a1} p_2^{a2},\ldots,p_n^{an}$$

$$b = p_1^{b1} p_2^{b2},\ldots,p_n^{bn}$$

يكون المضاعف المشترك الأصغر:

$$\text{Icm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2 b_2)},\ldots,p_n^{\max(a_n b_n)} \qquad (2)$$

ملاحظة:

المضاعف المشترك الأصغر لأعداد أولية فيما بينها مثنى مثنى هو حاصل جداء تلك الأعداد.

تمارين محلولة

١ – أوجد المضاعف المشترك الأصغر للعددين 12 ,18.

الحل:

نحلل العددين فنجد:

$$\begin{array}{r|l} 18 & 2 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array} \qquad \begin{array}{r|l} 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$

نكتب العددين بشكل جداء قوى:

$$12 = 2^2 \times 3$$
$$18 = 2 \times 3^2$$
$$\text{Icm} = 3^2 \times 2^2 = 9 \times 4 = 36$$

٢ – أوجد القاسم المشترك الأكبر للعددين 180 ,168.

الحل:

نحلل العددين فنجد:

$$\begin{array}{r|l} 168 & 2 \\ 84 & 2 \\ 42 & 2 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array} \qquad \begin{array}{r|l} 180 & 2 \\ 90 & 2 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

نكتب العددين بشكل جداء قوى:

$$180 = 2^2 \times 3^2 \times 5$$
$$168 = 2^3 \times 3 \times 7$$

القاسم المشترك الأكبر:

$$\gcd(180,168) = 2^2 \times 3 = 12$$

٣ – بيّن فيما إذا كان الأعداد 4, 5, 9 أولية فيما بينها، ثم أوجد القاسم المشترك الأكبر والمضاعف المشترك الأصغر.

الحل:

نكتب هذه الأعداد بشكل جداء قوى نجدك

$9 = 3^2$
$4 = 2^2$
$5 = 5$

$$\text{Gcd}(9,4) = 1 \qquad \gcd(9,5) = 1 \qquad \gcd(4,5) = 1$$

إذن الأعداد السابقة أولية فيما بينها.

وعليه يكون القاسم المشترك الأكبر هو الواحد.

والمضاعف المشترك الأصغر جداء هذه الأعداد:

$$\text{lcm}(9,4,5) = 3^2 \times 2^2 \times 5 = 180$$

٤ – بين فيما إذا كان العدد 101 هو عدد أولي.

الحل:

نأخذ $\sqrt{101}$

$\sqrt{101} \cong 10.09$

نأخذ الأعداد الأولية الأصغر من 10، وهي 2,3,5,7 نبحث في قابلية لـ 101 على كل من هذه الأعداد.

نلاحظ أن 101 لا يقبل القسمة على أي عدد من هذه الأعداد وبالتالي فهو عدد أولي.

تمارين للحل

تمرين (١):

أوجد القاسم المشترك الأكبر للأعداد:

1575 4851 645

تمرين (٢):

أوجد المضاعف المشترك الأصغر للأعداد:

30 20 15

تمرين (٣):

أوجد المضاعف المشترك الأصغر والقاسم المشترك الأكبر للعددين باستخدام القاعدتين (1) و (2):

$$a = 2^3 \,.\, 3^5 \,.\, 7^2$$
$$b = 2^4 \,.\, 3^3$$

تمرين (٤):

أوجد الأعداد الصحيحة الموجبة التي تصغر 30 والتي عي أعداد أولية نسبياً.

تمرين (٥):

أثبت أن العدد 107 هو عدد أولي.

تمرين (٥):

بين فيما إذا كانت الأعداد الصحيحة الواردة في d,c,b,a التالية:

a) 21, 34, 55
b) 14, 17, 85
c) 25, 41, 49, 64
d) 17, 18, 19, 23

أعداد أولية نسبياً مثنى مثنى.