

## المعادلات الخطية والقاسم المشترك الأكبر

### Linear Equations and the Greatest Common Divisor

افرض أن  $a$  و  $b$  عدنان صحيحان غير سالبين ( Whole numbers )، سنبحث عن جميع الأعداد المحتملة التي يمكن أن نحصل عليها بإضافة مضاعف ل  $a$  إلى مضاعف ل  $b$ . بمعنى آخر، سنبحث عن جميع الأعداد التي من الممكن الحصول عليها من القاعدة  $ax + by$  حيث  $x, y \in \mathbb{Z}$ .

جدول لـ قيم  $42x + 30y$ .

	$x = -3$	$x = -2$	$x = -1$	$x = 0$	$x = 1$	$x = 2$	$x = 3$
$y = -3$	-216	-174	-132	-90	-48	-6	36
$y = -2$	-186	-144	-102	-60	-18	24	66
$y = -1$	-156	-114	-72	-30	12	54	96
$y = 0$	-126	-84	-42	0	42	84	126
$y = 1$	-96	-54	-12	30	72	114	156
$y = 2$	-66	-24	18	60	102	144	186
$y = 3$	-36	6	48	90	132	174	216

لاحظ أننا سنسمح بقيم سالبة وموجبة ل  $x$  و  $y$ . على سبيل المثال، افرض أن

$a = 42$  و  $b = 30$ ، القائمة التالية تقدم بعض قيم  $ax + by$ .

الملاحظة الأولى التي نلاحظها من خلال التدقيق بالقائمة السابقة أن جميع المدخلات في القائمة تقبل القسمة على 6 ، وهذه ليست مفاجأة ؛ لأن كلاً من 42 و 30 يقبل القسمة على 6 ؛ وعليه فإن أي عدد على الصورة

$$42x + 30y = 6(7x + 5y)$$

من مضاعفات العدد 6. بصورة أكثر تعميماً، يمكننا ملاحظة أن أي عدد على الصورة  $ax + by$  يقبل القسمة على  $\gcd(a, b)$  ؛ لأن كلا من  $a$  و  $b$  يقبل القسمة على  $\gcd(a, b)$ .

الملاحظة الثانية، والمثيرة أكثر للدهشة، هي أن القاسم المشترك الأكبر للعددين 42 و 30 ، والذي هو 6 ، يظهر في القائمة ؛ لذا ومن القائمة نستطيع أن نرى أن

$$42 \cdot (-2) + 30 \cdot 3 = 6 = \gcd(42, 30)$$

التدقيق في أمثلة إضافية يقودنا إلى الاستنتاج التالي :

أصغر قيمة موجبة لـ
$ax + by$
يساوي $\gcd(a, b)$

هناك عدة طرق لإثبات أن ذلك صحيح. سنأخذ المنحى الاستنتاجي ( Constructive approach ) كما فعلنا مع خوارزمية إقليدس. ميزة هذه الطريقة أنها تعطي إستراتيجية إيجاد القيم المناسبة لـ  $x$  و  $y$ . بمعنى آخر سنقدم طريقة لإيجاد الأعداد الصحيحة لـ  $x$  و  $y$  والتي هي حل للمعادلة.

$$ax + by = \gcd(a, b).$$

بما أن، وكما لاحظنا سابقاً، أي عدد  $ax + by$  يقبل القسمة على  $\gcd(a, b)$ ؛ فإن هذا يعني أن أصغر قيمة موجبة لـ  $ax + by$  هي بالضبط  $\gcd(a, b)$ .

السؤال الآن هو، كيف يمكننا حل المعادلة  $ax + by = \gcd(a, b)$ ؟ إذا كان  $a$  و  $b$  عددين صغيرين، فمن الممكن تخمين الحل. على سبيل المثال، المعادلة:

$$10x + 35y = 5$$

حلها  $x = -3$  و  $y = 1$ ، والمعادلة:

$$7x + 11y = 1$$

حلها  $x = -3$  و  $y = 2$ .

يمكننا أيضاً ملاحظة أنه قد يكون هناك أكثر من حل، حيث  $x = 8$  و  $y = -5$  هو حل آخر للمعادلة  $7x + 11y = 1$ . على أي حال، إذا كان  $a$  و  $b$  عددين كبيرين، فإن طريقة التخمين أو التجربة والخطأ لن تكون مجدية.

سنبدأ بتوضيح طريقة خوارزمية إقليدس لحل المعادلة:

$$ax + by = \gcd(a, b)$$

من خلال مثال محدد، لذلك لنحاول حل المعادلة:

$$22x + 60y = \gcd(22, 60)$$

الخطوة الأولى تكون باستخدام خوارزمية إقليدس لحساب  $\gcd$ . نجد أن:

$$60 = 2 \times 22 + 16$$

$$22 = 1 \times 16 + 6$$

$$16 = 2 \times 6 + 4$$

$$6 = 1 \times 4 + 2$$

$$4 = 2 \times 2 + 0$$

هذا يبين أن  $\gcd(22, 60) = 2$  ، وهي حقيقة واضحة دون اللجوء لخوارزمية

إقليدس. على كل حال ، فإن الحسابات التي أجريناها مهمة ؛ لأننا سنستخدم نواتج

القسمة والبواقي لحل المعادلة  $22x + 60y = 2$ .

الخطوة الأولى هي إعادة كتابة المعادلة على الشكل :

$$b = 22 \quad a = 60 \quad \text{حيث} \quad 16 = a - 2b$$

الخطوة التالية هي تعويض هذه القيمة بدلاً من الـ 16 الموجودة في المعادلة الثانية

من خوارزمية إقليدس ، هذا يعطي (تذكر أن  $b = 22$ ).

$$b = 1 \times 16 + 6 = 1 \times (a - 2b) + 6,$$

أعد ترتيب هذه المعادلة بحيث تضع 6 في طرف لوحدها فينتج :

$$6 = b - (a - 2b) = -a + 3b$$

الآن عوض القيمتين 16 و 6 في المعادلة الثالثة ،  $16 = 2 \times 6 + 4$  ;

$$a - 2b = 16 = 2 \times 6 + 4 = 2(-a + 3b) + 4$$

مرة أخرى نقوم بوضع الباقي 4 في طرف لوحده لنحصل على :

$$4 = (a - 2b) - 2(-a + 3b) = 3a - 8b.$$

أخيراً ، نستخدم المعادلة  $6 = 1 \times 4 + 2$  لنحصل على :

$$-a + 3b = 6 = 1 \times 4 + 2 = 1 \times (3a - 8b + 2)$$

بإعادة ترتيب هذه المعادلة نحصل على الحل المطلوب  $-4a + 11b = 2$ .

$$(\text{للتحقق من صحة الحل: } -4 \times 60 + 11 \times 22 = -240 + 242 = 2.)$$

يمكن تلخيص الحسابات السابقة بالطريقة المجدولة الفعالة التالية. لاحظ أن المعادلات في الطرف الأيسر تمثل خوارزمية إقليدس، بينما المعادلات في الطرف الأيمن

تُحسب الحل للمعادلة  $ax + by = \gcd(a, b)$

$$a = 2 \times b + 16$$

$$b = 1 \times 16 + 6$$

$$16 = 2 \times 6 + 4$$

$$6 = 1 \times 4 + 2$$

$$4 = 2 \times 2 + 0$$

$$16 = a - 2b$$

$$6 = b - 1 \times 16$$

$$= b - 1 \times (a - 2b)$$

$$= -a + 3b$$

$$4 = 16 - 2 \times 6$$

$$= (a - 2b) - 2 \times (-a + 3b)$$

$$= 3a - 8b$$

$$2 = 6 - 1 \times 4$$

$$= (-a + 3b) - 1 \times (3a - 8b)$$

$$= -4a + 11b$$

لماذا تعمل هذه الطريقة؟ الجدول التالي يوضح ذلك. نبدأ بأول خطوتين من

خوارزمية إقليدس والتي تضم الكميتين  $a$  و  $b$  ونبدأ العمل نزولاً.

$$\begin{array}{l}
 a = q_1 b + r_1 \\
 b = q_2 r_1 + r_2 \\
 r_1 = q_3 r_2 + r_3
 \end{array}
 \left|
 \begin{array}{l}
 r_1 = a - q_1 b \\
 r_2 = b - q_2 r_1 \\
 \quad = b - q_2 (a - q_1 b) \\
 \quad = -q_2 a + (1 + q_1 q_2) b \\
 r_3 = r_1 - q_3 r_2 \\
 \quad = (a - q_1 b) - q_3 (-q_2 a + (1 + q_1 q_2) b) \\
 \quad = (1 + q_2 q_3) a - (q_1 + q_3 + q_1 q_2 q_3) b
 \end{array}
 \right.$$

كلما تحركنا من خطوة إلى أخرى ، فإننا سنشكل باستمرار معادلات تبدو على

الصورة آخر باقي = أحد مضاعفات  $a$  مضافاً إليه أحد مضاعفات  $b$

وأخيراً ، نحصل على آخر باقي غير صفري ، والذي نعرف أنه يساوي

$\gcd(a, b)$  ، وهذا يعطينا الحل المطلوب للمعادلة  $\gcd(a, b) = ax + by$ .

المثال التالي ، والذي يتضمن قيماً أكبر لـ  $a$  و  $b$  ، حيث  $a = 12453$

و  $b = 2347$  نقدمه بصورة مجدولة على النحو الآتي ، حيث إن المعادلات في الطرف

الأيسر تمثل خوارزمية إقليدس بينما المعادلات في الطرف الأيمن تحسب الحل للمعادلة

$$ax + by = \gcd(a, b)$$

نستنتج من الجدول السابق أن  $\gcd(12453, 2347) = 1$  ، وأن

$$(x, y) = (304, -1613) \text{ حل للمعادلة :}$$

$$12453x + 2347y = 1.$$

نعرف الآن أن المعادلة :

$$ax + by = \gcd(a, b)$$

$a = 5 \times b + 718$	$718 = a - 5b$
$b = 3 \times 718 + 193$	$193 = b - 3 \times 718$
	$= b - 3 \times (a - 5b)$
	$= -3a + 16b$
$718 = 3 \times 193 + 139$	$139 = 718 - 3 \times 193$
	$= (a - 5b) - 3 \times (-3a + 16b)$
	$= 10a - 53b$
$193 = 1 \times 139 + 54$	$54 = 193 - 139$
	$= (-3a + 16b) - (10a - 53b)$
	$= -13a + 69b$
$139 = 2 \times 54 + 31$	$31 = 139 - 2 \times 54$
	$= (10a - 53b) - 2 \times (-13a + 69b)$
	$= 36a - 191b$
$54 = 1 \times 31 + 23$	$23 = 54 - 31$
	$= -13a + 69b - (36a - 191b)$
	$= -49a + 260b$
$31 = 1 \times 23 + 8$	$8 = 31 - 23$
	$= 36a - 191b - (-49a + 260b)$
	$= 85a - 451b$
$23 = 2 \times 8 + 7$	$7 = 23 - 2 \times 8$
	$= (-49a + 260b) - 2 \times (85a - 451b)$
	$= -219a + 1162b$
$8 = 1 \times 7 + 1$	$1 = 8 - 7$
	$= 85a - 451b - (-219a + 1162b)$
$7 = 7 \times 1 + 0$	$= 304a - 1613b$

دائماً لها حل بعددين صحيحين  $x$  و  $y$ . السؤال الأخير الذي سنقوم بمناقشته في هذا الفصل هو، كم عدد الحلول للمعادلة  $ax + by = \gcd(a, b)$  وكيف نصف جميع هذه الحلول؟

لنبدأ بالحالة التي يكون فيها العدان  $a$  و  $b$  أوليين نسبياً، أي  $\gcd(a, b) = 1$ ، وسنفرض أن  $(x_1, y_1)$  هو حل للمعادلة :

$$ax + by = 1.$$

بالإمكان توليد حلول أخرى بطرح أحد مضاعفات  $b$  من  $x_1$  وإضافة نفس المضاعف لـ  $a$  إلى  $y_1$ . بمعنى آخر، لأي عدد صحيح  $k$  نحصل على الحل الجديد

$$^{(1)} (x_1 + kb, y_1 - ka).$$

الحسابات التالية تبين أن الزوج السابق يمثل فعلاً حلاً للمعادلة

$$: ax + by = 1$$

$$a(x_1 + kb) + b(y_1 - ka) = ax_1 + akb + by_1 - bka = ax_1 + by_1 = 1$$

على سبيل المثال إذا بدأنا بـ  $(-1, 2)$  كحل للمعادلة  $5x + 3y = 1$  فإن  $(-1 + 3k, 2 - 5k)$  تولد لنا حلولاً جديدة للمعادلة. لاحظ أن  $k$  يمكن أن يكون عدداً موجباً، سالباً أو صفراً. بتعويض بعض القيم الخاصة بدلا من  $k$  نحصل على

الحلول

$$\dots(-13, 22), (-10, 7), (-7, 12), (-4, 7), (-1, 2), \\ (2, -3), (5, -8), (8, -13), (11, -8) \dots$$

(١) هندسياً، نحن بدأنا من نقطة معلومة  $(x_1, y_1)$  واقعة على الخط  $ax + by = 1$  واستخدمنا حقيقة أن ميل الخط يساوي  $-a/b$  لإيجاد نقطة جديدة  $(x_1 + t, y_1 - (a/b)t)$ . للحصول على نقاط جديدة بإحداثيات صحيحة، نحتاج لجعل  $t$  من مضاعفات  $b$ . تعويض  $t = kb$  يعطي الحل الصحيح الجديد  $(x_1 + kb, y_1 - ka)$ .



لاحظ أننا ما زلنا في الحالة الخاصة والتي فرضنا فيها أن  $\gcd(a, b) = 1$ . بالإمكان إثبات أن هذه العملية ستعطينا جميع الحلول الممكنة. افترض أن  $(x_1, y_1)$  و  $(x_2, y_2)$  حلان للمعادلة  $ax + by = 1$ ، بمعنى أن:

$$ax_2 + by_2 = 1 \quad \text{و} \quad ax_1 + by_1 = 1$$

بضرب المعادلة الأولى بـ  $y_2$  والمعادلة الثانية بـ  $y_1$  والطرح نحصل على:

$$ax_1y_2 - ax_2y_1 = y_2 - y_1.$$

بطريقة ماثلة إذا قمنا بضرب المعادلة الأولى بـ  $x_2$  والمعادلة الثانية بـ  $x_1$  والطرح نحصل على:

$$bx_2y_1 - bx_1y_2 = x_2 - x_1.$$

لذلك إذا فرضنا أن  $k = x_2y_1 - x_1y_2$  سنجد أن:

$$x_2 = x_1 + kb \quad \text{و} \quad y_2 = y_1 - ka$$

وهذا يعني أن الحل الثاني  $(x_2, y_2)$  قد تم الحصول عليه من الحل الأول  $(x_1, y_1)$  وذلك بإضافة مضاعف لـ  $b$  إلى  $x_1$  وطرح نفس المضاعف لـ  $a$  من  $y_1$ . مما سبق نستنتج أن جميع الحلول للمعادلة  $ax + by = 1$  يمكن الحصول عليها من الحل الأول  $(x_1, y_1)$  وذلك بتعويض قيم مختلفة لـ  $k$  في  $(x_1 + kb, y_1 - ka)$ . ماذا يحدث إذا كان  $\gcd(a, b) > 1$ . لجعل المعادلة تبدو أكثر سهولة سنفرض أن  $\gcd(a, b) = g$ . نعرف من خوارزمية إقليدس أنه يوجد على الأقل حل واحد للمعادلة:

$$ax + by = g.$$

لكن  $g$  يقسم كلا من  $a$  و  $b$  ؛ وعليه فإن  $(x_1, y_1)$  حل للمعادلة الأبسط

التالية :

$$\frac{a}{g}x + \frac{b}{g}y = 1.$$

الآن بتطبيق ما عملناه سابقاً، يمكننا أن نعلم أن أي حل آخر يمكن الحصول

عليه بتعويض قيم  $k$  في الصيغة :

$$(x_1 + k \cdot \frac{b}{g}, y_1 - k \cdot \frac{a}{g}).$$

وبهذا نكون قد أنهينا النقاش حول حلول المعادلة  $ax + by = g$  ، وسنلخصه

في النظرية التالية.

**نظرية (١, ٦) ( نظرية المعادلة الخطية ).** ليكن  $a$  و  $b$  عددين صحيحين غير

صفرين، وليكن  $\gcd(a, b) = g$ . المعادلة :

$$ax + by = g$$

دائماً لها حل  $(x_1, y_1)$  في  $\mathbb{Z}$  ، وهذا الحل يمكن إيجاده بطريقة خوارزمية

إقليدس. عندئذ أي حل للمعادلة يمكن الحصول عليه بالتعويض بأعداد صحيحة  $k$  في

الصيغة :

$$(x_1 + k \cdot \frac{b}{g}, y_1 - k \cdot \frac{a}{g}).$$

على سبيل المثال، نرى أن  $x = -4$  ،  $y = 11$  هو حل للمعادلة :

$$60x + 22y = \gcd(60, 22) = 2$$

وعليه ؛ فإن نظرية المعادلة الخطية تنص على أن كل حل يمكن الحصول عليه بالتعويض عن  $k$  بأعداد صحيحة في الزوج :

$$(-4 + 11k, 11 - 30k).$$

بشكل خاص ، إذا أردنا حلاً يتضمن قيمة موجبة لـ  $x$  فبإمكاننا أخذ  $k = 1$  والتي تعطينا أصغر حل  $(x, y) = (7, -19)$ .  
في هذا الفصل أثبتنا أن المعادلة :

$$ax + by = \gcd(a, b),$$

دائماً لها حل. هذه الحقيقة مهمة جداً لأسباب نظرية وعملية ، وسنستخدمها مراراً وتكراراً في دراستنا اللاحقة. على سبيل المثال ، سنحتاج حل المعادلة  $ax + by = 1$  عند دراستنا للتشفير في الفصل الثامن عشر. وفي الفصل التالي سنستخدم هذه المعادلة في دراستنا النظرية حول تحليل الأعداد إلى عواملها الأولية.

## تمارين

(٦.١) وجد حل في  $\mathbb{Z}$  للمعادلة  $12345x + 67890y = \gcd(12345, 67890)$

(b) أوجد حلاً في  $\mathbb{Z}$  للمعادلة  $54321x + 9876y = \gcd(54321, 9876)$

(٦.٢) صف جميع الحلول الصحيحة لكل معادلة من المعادلات التالية :

(a)  $105x + 121y = 1$

(b)  $12345x + 67890y = \gcd(12345, 67890)$

(c)  $54321x + 9876y = \gcd(54321, 9876)$

(٦.٣) طريقة حل المعادلة  $ax + by = \gcd(a, b)$  المشروحة في هذا الفصل تنطوي

على قدر كبير من التلاعب والتعويض الخلفي . هذا التمرين يصف طريقة بديلة

وسهلة لحساب  $y, x$  خصوصاً عند تنفيذها في الكمبيوتر.

(a) بين أن الخوارزمية الموصوفة في الشكل رقم (٦, ١) تحسب القاسم المشترك الأكبر  $g$  للعددين الصحيحين الموجبين  $a, b$  بالإضافة إلى حل  $(x, y)$  في  $\mathbb{Z}$  للمعادلة  $ax + by = \gcd(a, b)$ .

(b) نفذ هذه الخوارزمية على كمبيوتر باستخدام لغة برمجة من اختيارك.

(c) استخدم برنامجك لحساب  $g = \gcd(a, b)$  وإيجاد حلول صحيحة للمعادلة  $ax + by = g$  للأزواج  $(a, b)$  التالية:

$$(i) (19789, 23548)$$

$$(ii) (31875, 8387)$$

$$(iii) (22241739, 19848039)$$

(d) ماذا يحدث لبرنامجك إذا كان  $b = 0$ ؟ جَهِّز البرنامج ليتعامل مع هذه الحالة بشكل صحيح.

(e) من المفيد في التطبيقات اللاحقة أن يكون لديك حل فيه  $x > 0$ . عدّل برنامجك بحيث يعطيك دائماً حلاً فيه  $x > 0$ . [مساعدة: إذا كان  $(x, y)$  حلاً، فإن  $(x + b, y - a)$  حل أيضاً.]

- ١- اجعل  $w = b, v = 0, g = a, x = 1$ .
- ٢- إذا كان  $w = 0$  فاجعل  $y = (g - ax)/b$  وأعط القيم  $(g, x, y)$ .
- ٣- اقسم  $g$  على  $w$  بوجود باقي ،  $g = qw + t$  ، حيث  $0 \leq t < w$ .
- ٤- اجعل  $S = x - qv$ .
- ٥- اجعل  $(x, g) = (v, w)$ .
- ٦- اجعل  $(v, w) = (s, t)$ .
- ٧- اذهب إلى الخطوة (2).

الشكل رقم (٦, ١). خوارزمية فعّالة لحل المعادلة  $ax + by = \gcd(a, b)$ .

(٦, ٤) (a) أوجد أعداداً صحيحة  $z, y, x$  تحقق المعادلة

$$6x + 15y + 20z = 1$$

(b) تحت أي شروط على  $a, b, c$  يكون للمعادلة

$$ax + by + cz = 1$$

حل ؟ صف طريقة عامة لإيجاد حل عندما يتوفر أحد الحلول.

(c) استخدم الطريقة التي أوجدتها في (b) لإيجاد حل في  $\mathbb{Z}$  للمعادلة

$$155x + 341y + 385z = 1$$

(٦, ٥) افرض أن  $\gcd(a, b) = 1$ . برهن أنه لكل عدد صحيح  $c$  ، فإن المعادلة

$ax + by = c$  لها حل صحيح لكل من  $x$  و  $y$ . (مساعدة: أوجد حل

للمعادلة  $au + bv = 1$  واضربه في  $c$ ).

أوجد حل للمعادلة  $37x + 47y = 103$ . حاول جعل  $x$  و  $y$  أصغر ما يمكن.

(٦, ٦) أحياناً نكون مهتمين بإيجاد الحلول غير السالبة فقط للمعادلة  $ax + by = c$ .

(a) اشرح لماذا لا توجد حلول للمعادلة  $3x + 5y = 4$  عندما  $x \geq 0$  ,  $y \geq 0$ .

(b) اعمل قائمة لبعض الأعداد التي على الشكل  $3x + 5y$  ، عندما  $x \geq 0$  ,  $y \geq 0$ . اعمل تخميناً عن القيم غير الممكنة للأعداد التي على الشكل  $3x + 5y$  ، ثم برهن أن تخمينك صحيح.

(c) لكل قيمة من قيم  $(a, b)$  التالية، أوجد أكبر عدد ليس على الشكل  $ax + by$  عندما  $x \geq 0$  ,  $y \geq 0$ .

(i)  $(a, b) = (3, 7)$       (ii)  $(a, b) = (5, 7)$       (iii)  $(a, b) = (4, 11)$

(d) ليكن  $\gcd(a, b) = 1$  ، باستخدام النتائج التي حصلت عليها في (c) ، أوجد صيغة تخمينية بدلالة  $a$  ,  $b$  تجد من خلالها أكبر عدد ليس على الشكل  $ax + by$  عندما  $x \geq 0$  ,  $y \geq 0$  ؟ اختبر صحة تخمينك لقيمتين على الأقل لـ  $(a, b)$ .

(e) برهن أن صيغتك التخمينية في (d) صحيحة.

(f) حاول تعميم هذه المسألة على مجموع ثلاثة حدود  $ax + by + cz$  عندما  $x \geq 0$  ,  $y \geq 0$  ,  $z \geq 0$ . مثلاً ، ما هو أكبر عدد ليس على الشكل

$6x + 10y + 15z$  ، حيث  $x, y, z$  أعداد غير سالبة؟