نظرية الأعداد

د/ فهد الشمري

٣,١ أعداد فيرما وطريقته في التحليل

Fermat's Numbers & Fermat's Factorization Method

أعداد فيرما هي الأعداد التي يمكن كتابتها على الصورة $2^{2^n} + 1$، حيث $n \geq 0$ عدد صحيح.

تمهيدية(١) يكون العدد الفردي $n > 1$ مؤلفا إذا وفقط إذا وجد عددان صحيحان x و y بحيث $n = x^2 - y^2$ و $x - y > 1$.

البرهان. لنفرض أن n عددا مؤلفا، أي أن $n = rs$ حيث $r, s > 1$. عندئذ $n = \left(\frac{r+s}{2}\right)^2 - \left(\frac{r-s}{2}\right)^2$. وبما أن n فردي فإن r و s فرديان وبالتالي فإن $r + s$ و $r - s$ زوجيان ومنه فإن $\frac{r+s}{2}$ و $\frac{r-s}{2}$ صحيحان.

برهان العكس واضح حيث $n = x^2 - y^2 = (x+y)(x-y)$ و $x - y > 1$ يدل على أن n مؤلف.

فيرما للتحليل:

لإيجاد x و y تحققان $n = x^2 - y^2 \Leftrightarrow x^2 = n + y^2$. حيث $x^2 \geq n$ فإن $x \geq \sqrt{n}$، نبدأ بتجريب قيم لـ x من أول عدد صحيح يلي العدد $\sqrt{n}$ لنجعل

$$\Delta(x) = x^2 - n$$

مربعا كاملا y^2.

مثال١ استخدم طريقة فيرما لتحليل العدد $n = 40391$.

الحــل حيث $201 > \sqrt{40391} > 200$ نبدأ من $x = 201$

x	$\Delta(x) = x^2 - n$
201	$(201)^2 - 40391 = 10$
202	$(202)^2 - 40391 = 413$
203	$(203)^2 - 40391 = 818$
204	$(204)^2 - 40391 = 1225$

$1225 = (35)^2$ مربع كامل، عندئذ

$$n = 40391 = 204^2 - 35^2 = (204+35)(204-35) = 239 \cdot 169$$

حيث 239 أولي والعدد $13^2 = 169$، فقد اكتمل التحليل $239 \cdot 13^2 = 40391$.

ملاحظات:

١. توقف فيرما للتحليل مضمون ففي أسوأ الحالات يكون عند $x = \left(\frac{n+1}{2}\right)$ وعندها يكون n أوليا:
$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2 \Leftrightarrow n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 \Leftrightarrow n = n \cdot 1$

٢. لـ $n = ab$، كلما كان الفرق $a - b$ أصغر كلما كانت طريقة فيرما لتحليل العدد n فعالة أكثر.

٣. يمكن تسهيل الحسابات بدون الحاسبات كما يلي

❖ لاحظ أن $\Delta(x)$ تحقق

$$\begin{aligned}
\Delta(x+1) &= \Delta(x) + 2x + 1 \\
\Delta(x+2) &= \Delta(x+1) + 2x + 3 \\
\Delta(x+3) &= \Delta(x+2) + 2x + 5 \\
&\vdots
\end{aligned}$$

❖ كتابة جميع الحالات الممكنة لآخر خانتين في المربع الكامل. هناك ٢٢ حالة ممكنة.

00 01 04 09 16
21 24 25 29 36
41 44 49 56 61
64 69 76 81 84
89 96

تمرين: استخدم طريقة فيرما لتحليل العدد $n = 2{,}027{,}651{,}281$. (هذا ما طبق فيرما عليه طريقته)

٣,٢ المعادلات الديوفنتية الخطية

Linear Diophantine Equations

المعادلة الديوفنتية هي المعادلة التي تهمنا دراستها وبحث حلولها في الأعداد الصحيحة.

$2x^2 + 3y^2 + 5z^4 = 1$	$3x - 6y = 14$	$2x - 3y = 17^{504}$
من الدرجة 4 في 3 مجاهيل	خطية في مجهولين	خطية في مجهولين
ليس لها حل	ليس لها حل	عدد لانهائي من الحلول

مبرهنة(١,١) يوجد حل للمعادلة الديوفنتية ✪ $ax + by = c$ إذا وفقط إذا $(a,b)|c$.

البرهان. ليكن $m,n \in \mathbb{Z}$ تحقق ① $am + bn = (a,b)$

لنفرض أن $(a,b)|c$، إذن يوجد $k \in \mathbb{Z}$ بحيث $c = k(a,b)$. بضرب طرفي ① في k

$$a(mk) + b(nk) = (a,b)k = c$$

أي أن $x = mk$ و $y = nk$ هو حل للمعادلة ✪.

لبرهان العكس، نفرض أن $x_0, y_0 \in \mathbb{Z}$ حل للمعادلة ✪. أي أن

$$ax_0 + by_0 = c$$

بما أن $(a,b)|a$ و $(a,b)|b$ فإن $(a,b)|ax_0 + by_0$ أي $(a,b)|c$.

لحساب أحد الحلول (إن وجد):

مثال٢ جد، إن أمكن، حلا للمعادلة الديوفنتية: $27x + 48y = 150$.

الحـــل بتطبيق خوارزمية القسمة، احسب $(27,48)$:

$$48 = 1 \cdot 27 + 21$$
$$27 = 1 \cdot 21 + 6$$
$$21 = 3 \cdot 6 + 3$$
$$6 = 2 \cdot 3 + 0$$

لأن $3 = (27,48)$ يقسم 150، فللمعادلة حل. نجد أحد الحلول:

$$\begin{aligned} 3 &= 21 - 3 \cdot 6 \\ &= 21 - 3(27 - 1 \cdot 21) = 4 \cdot 21 - 3 \cdot 27 \\ &= 4 \cdot (48 - 27) - 3 \cdot 27 = 27(-7) + 48(4) \end{aligned}$$

نضرب بالعدد 50 $150 = 27(-350) + 48(200)$

لذا فأحد الحلول هو: $x = -350$ و $y = 200$.

مبرهنة(١,٢) **إذا وجد حل $x_0, y_0 \in \mathbb{Z}$ للمعادلة الديوفنتية ✪ $ax + by = c$ ، فإن الحل العام لهذه المعادلة على الصورة:**

$$x = x_0 + k \cdot \frac{b}{(a,b)}$$
$$y = y_0 - k \cdot \frac{a}{(a,b)}$$

حيث $k \in \mathbb{Z}$.

البرهان. نحتاج لإثبات أمرين: ① أن $x_0 + k \cdot \frac{b}{(a,b)}$ ، $y_0 + k \cdot \frac{a}{(a,b)}$ حل، لكل $k \in \mathbb{Z}$

② أن أي حل تكون له هذه الصورة.

① لدينا

$$a\left(x_0 + k \cdot \frac{b}{(a,b)}\right) + b\left(y_0 - k \cdot \frac{a}{(a,b)}\right) = ax_0 + k \cdot \frac{ab}{(a,b)} + by_0 - k \cdot \frac{ab}{(a,b)} = ax_0 + by_0 = c$$

② ليكن x_1 ، y_1 حلا لهذه المعادلة، أي $ax_1 + by_1 = c$

وبما أن x_0 و y_0 حل، لدينا $ax_0 + by_0 = c$

بطرح المعادلة الثانية من الأولى نجد أن $a(x_1 - x_0) + b(y_1 - y_0) = 0$

أي أن $a(x_1 - x_0) = -b(y_1 - y_0)$

بالقسمة على (a,b)،

$$\frac{a}{(a,b)}(x_1 - x_0) = -\frac{b}{(a,b)}(y_1 - y_0)$$

وهذا يعني أن $\frac{b}{(a,b)} \Big| \frac{a}{(a,b)}(x_1 - x_0)$ ولكن $\left(\frac{b}{(a,b)}, \frac{a}{(a,b)}\right) = 1$ ، نتيجة(١) لمبرهنة(١،٦)، إذن $\frac{b}{(a,b)} \Big| (x_1 - x_0)$. لـذا يوجـد $k \in \mathbb{Z}$ بحيـث $(x_1 - x_0) = k \cdot \frac{b}{(a,b)}$ ، أي $x_1 = x_0 + k \cdot \frac{b}{(a,b)}$. أخـيرا، بـالتعويض $(x_1 - x_0) = k \cdot \frac{b}{(a,b)}$ في $\frac{a}{(a,b)}(x_1 - x_0) = -\frac{b}{(a,b)}(y_1 - y_0)$ لدينا

$$\frac{a}{(a,b)} \cdot k \cdot \frac{b}{(a,b)} = -\frac{b}{(a,b)}(y_1 - y_0)$$
$$-\frac{a}{(a,b)} \cdot k = (y_1 - y_0)$$
$$y_1 = y_0 - k \cdot \frac{a}{(a,b)}$$

لإيجاد جميع الحلول:

مثال٣ جد الحل العام للمعادلة الديوفنتية: $27x + 48y = 150$.

الحـــل من مثال٢ لدينا الحل $x = -350$ و $y = 200$. الحلول الصحيحة الآن معطاة بالحل العام:

$$x = -350 + k \cdot \frac{48}{(27,48)} \quad \Rightarrow \quad x = -350 + 16k$$
$$y = 200 - k \cdot \frac{27}{(27,48)} \quad \Rightarrow \quad y = 200 - 9k$$

حيث $k \in \mathbb{Z}$.

ملاحظات:

للحلول الموجبة

يهمنا في كثير من الأحيان بحث الحلول الصحيحة الموجبة، هذه يمكن إيجادها من الحل العام:

مثال E جد جميع الحلول الصحيحة الموجبة للمعادلة الديوفنتية: $27x + 48y = 150$.

الحــل من الحل العام:

$$x = -350 + 16k$$
$$y = 200 - 9k$$

نجد الحلول الموجبة بحل المتراجحتين:

$-350 + 16k > 0$ و $200 - 9k > 0 \Leftrightarrow \frac{200}{9} > k > \frac{350}{16} \Leftrightarrow 22\frac{2}{9} > k > 21\frac{7}{8}$

$\Leftrightarrow k = 22$. أي يوجد حل صحيح موجب وحيد وهو: $x = 2$ و $y = 2$.

طريقة أويلر لحل المعادلة الديوفنتية:

مثال D جد حلول المعادلة الديوفنتية: ① $27x + 48y = 150$.

الحــل اقسم حدود المعادلة على $(27, 48) = 3$ ، لنحصل على المعادلة المكافئة: ② $9x + 16y = 50$

اكتب المجهول الذي لمعامله أصغر قيمة مطلقة بدلالة باقي الحدود:

$$x = \frac{50}{9} - \frac{16}{9}y \Leftrightarrow x = 5 - y - \frac{7}{9}y + \frac{5}{9}$$

لاحظ أن x و y حل للمعادلة ① $\Leftrightarrow$ x و y حل للمعادلة ② $\Leftrightarrow$

$x = 5 - y - \frac{7}{9}y + \frac{5}{9}$ ضع $-\frac{7}{9}y + \frac{5}{9} = z_1 \Leftrightarrow -7y + 5 = 9z_1$.

اكتب y بدلالة الحدود الأخرى ثم بسط:

$y = -\frac{9}{7}z_1 + \frac{5}{7} \Leftrightarrow y = -z_1 - \frac{2}{7}z_1 + \frac{5}{7}$. ضع $-\frac{2}{7}z_1 + \frac{5}{7} = z_2 \Leftrightarrow -2z_1 + 5 = 7z_2$.

اكتب ثم بسط $z_1 = -\frac{7}{2}z_2 + \frac{5}{2} \Leftarrow z_1 = -3z_2 + 2 - \frac{1}{2}z_2 + \frac{1}{2}$ ضع $-\frac{1}{2}z_2 + \frac{1}{2} = z_3 \Leftrightarrow 1 + z_2 = -2z_3 + 1$

والآن z_3 ليس عليها شرط وبدلالتها نحصل على الحل العام.

$$z_2 = -2z_3 + 1$$
$$z_1 = 7z_3 - 1$$
$$y = -9z_3 + 2$$
$$x = 16z_3 + 2$$

لاحظ أن الحل العام:

$$x = 2 + 16z_3$$
$$y = 2 - 9z_3$$

تمرين

الحل العام للمعادلة الديوفنتية: $68x + 100y = 24$ هو

$$x = 18 + 25k$$
$$y = -12 - 17k$$

٣,٢,١ المعادلة الديوفنتية الخطية العامة — General Linear Diophantine Equation

تمهيدية(٢) لتكن $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. يوجد أعداد صحيحة $y_1, y_2, \ldots, y_n \in \mathbb{Z}$ تحقق

$$(a_1, a_2, \ldots, a_n) = a_1y_1 + a_2y_2 + \ldots + a_ny_n$$

مبرهنة(١,٣) يوجد حل للمعادلة $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c \iff (a_1, a_2, \ldots, a_n)|c$.

البرهان.

لحلول المعادلة الديوفنتية الخطية:

سوف نستخدم طريقة أويلر والتي لتطبيقها نحتاج لمعرفة القاسم المشترك الأعظم لمجموعة من الأعداد الصحيحة $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ ، وفيما يلي توضيح ذلك:

لإيجاد $(a_1, a_2, \ldots, a_n)$ **:** بفرض أن الأعداد غير سالبة،

١. ابحث عن أصغر عدد صحيح موجب وليكن a_1 واجر خوارزمية القسمة:

$$a_2 = a_1q_2 + r_2 \qquad ,0 \le r_2 < a_1$$
$$a_3 = a_1q_3 + r_3 \qquad ,0 \le r_3 < a_1$$
$$\vdots$$
$$a_n = a_1q_n + r_n \qquad ,0 \le r_n < a_1$$

لاحظ أن $(a_1, r_2, r_3, \ldots, r_n) = (a_1, a_2, a_3, \ldots, a_n)$. الآن عين القيم الجديدة:

$$a_1, a_i := r_i \qquad ,\forall i \ge 2$$

أعد تطبيق الخطوة السابقة لتعيين قيم جديدة لـ $r_i{}'s$ وهكذا حتى يصبح $a_i = 0 \; ,\forall i \ge 2$. عندها $(a_1, a_2, \ldots, a_n) = a_1$ ، (لا تنس a_1 هذه من الخطوة الأخيرة)

مثال٦ جد جميع حلول المعادلة الديوفنتية: $2x + 3y + 4z = 5$.

الحــل حيث $(2, 3, 4) = 1$ ، يوجد حل. نستخدم طريقة أويلر:

$$2x = 5 - 4z - 3y$$
$$x = \tfrac{5}{2} - 2z - \tfrac{3}{2}y = 2 - 2z - y + \tfrac{1}{2} - \tfrac{1}{2}y$$

نضع $\frac{1}{2} - \frac{1}{2}y = w_1$ ، ومنه $1 - y = 2w_1$ أي $y = 1 - 2w_1$.

$$x = 2 - 2z - (1 - 2w_1) + w_1 = 1 - 2z + 3w_1$$

وهكذا فحلول المعادلة الديوفنتية هي

$$x = 1 - 2z + 3w_1$$
$$y = 1 - 2w_1$$