الأربعاء: 25/3/2014

المحاضرة السادسة:

هل توجد صيغة تعطي كل الأعداد الأولية؟

وضع العلماء صيغاً ظن بعضهم أنها تعطي جميع الأوليات ثم ثبت أن جميعهم خاطئ، من هذه الصيغ:

1- الصيغة $x^2 - x + 41$

تعطي أعداد أولية إذا كانت $x = 0, 1, \ldots, 40$

2- الصيغة $x^2 - 79x + 1601$

تعطي أعداد أولية إذا كانت $x = 0, 1, \ldots, 79$

ديرخليه:

أثبت أنه لا توجد صيغة تعطينا جميع الأعداد الأولية.

ديرخليه:

أثبت أنه إذا كان a, b عددان صحيحان موجبان، $(a, b) = 1$ فإن الصيغة $ax + b$ تعطي أعداد أولية.

مثال:

$(2, 3) = 1 \Rightarrow f(x) = 2x + 3$

$(5, 6) = 1 \Rightarrow f(x) = 5x + 6$

3- فيرما: وضع فيرما الصيغة وظن أنها تعطي أوليات من أجل جميع القيم ما أثبت أويلر أن F_5 عدد مؤلف

$$F_n = 2^{2^n} + 1$$

$$F_0 = 3$$

$$F_1 = 2^2 + 1 = 5$$

$$F_2 = 2^4 + 1 = 17$$

$$F_3 = 2^8 + 1 = 275$$

$F_4 = 2^{16} + 1 = 65537$

$F_5 = 2^{32} + 1 = 4294967297$

$= 641 \times 6700417$ غير أولي.

كيفية إيجاد الأعداد الأولية التي هي أصغر من x ، $x = 100$

مرشحة إيراتوستين:

نكتب جميع الأعداد من 1 إلى x ثم نبدأ بالعدد الأولي الأول وهو 2 نترك ونشطب جميع مضاعفاته ثم نترك أول عدد لم يتم شطبه وسيكون العدد 3 ونشطب جميع مضاعفات 3 وهكذا...

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

يوجد 25 عدداً أولياً من 1 ← 100

مبرهنة الأعداد الأولية: أي تحقق $2 \leq p \leq x$ ، p

إذا كان $\pi(x)$ هو عدد الأعداد الأولية التي هي أقل من x فيكون نهاية $\dfrac{\pi(x)}{\dfrac{x}{\log x}}$ عندما $x \to \infty$ تساوي الواحد.

$$\pi(x) \underset{n\to\infty}{\sim} \frac{x}{\log x}$$

تحليل العدد الفردي بطريقة فيرما إلى عوامله:

مبرهنة:

ليكن n عدداً صحيحاً فردياً موجباً. يمكن كتابة n كحاصل ضرب عددين صحيحين موجبين a و b إذا وفقط إذا أمكن كتابة n على شكل فرق مربعين صحيحين أي:

$$n = x^2 - y^2 \iff n = a.b$$

الإثبات:

$(\Rightarrow)$ إذا كان $n = x^2 - y^2 = (x-y)(x+y) = a.b$

$(\Leftarrow)$

إذا كان $n = a.b$; a, b فرديان $a, b \in \mathbb{Z}^+$

بملاحظة أن:

$$n = a.b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

نجد المطلوب.

مثال:

$$n = 21 = 3 \times 7 = (5)^2 - (2)^2 = 21$$

طريقة فيرما لتحليل العدد الفردي n إلى جداء عاملين: $n \in \mathbb{Z}^+$

* $n = x^2 - y^2 \Rightarrow x^2 - n = y^2$

x, y مجهولين نبدأ بالبحث عن أصغر عدد k بحيث يكون:

$$k^2 > n$$

ثم نبحث ضمن الأعداد التالية:

$$k^2 - n$$
$$(k+1)^2 - n$$
$$\vdots$$

$m \geq \sqrt{n}$

نتابع حتى نحصل على عدد m يحقق ; $m^2 - n = y^2$

نعوض في * فنحصل على $x = m$ (معادلة بمجهولين x, y)

إذا لم نجد مربع عدد نتابع هذه العملية حيث أن هذه العملية منتهية ولا بد أن نصل إلى الخطوة الأخيرة:

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

فيكون n عدد أولي ; $n = n \cdot 1$

مثال: $n = 2027\ 651281$

بعد 11 خطوة بطريقة فيرما وجد أن $n = 44021 \times 46061$

أما بالطريقة التحليلية تحتاج إلى 2850 عملية حتى نحصل على العدد 44021

مثال:

$n = 945$

$$(k-1)^2 \leqslant n \leqslant k^2$$

$$n \leqslant 31^2$$

$$31^2 - 945 = 16 = 4^2$$

$$945 = (31+4)(31-4)$$
$$= 35 \times 27$$
$$= 5 \times 7 \times 3^3$$
$$= 3^3 \times 5 \times 7$$

تمارين وصفحة 60:

حلل الأعداد التالية إلى عواملها الأولية بطريقة فيرما:

$n = 10541$

$$10541 < k^2$$

$$10^2 = 10404 < 10541 < 103^2$$

$102^2 < 10541 < 10609$

$103^2 - 10541 = 68$

$104^2 - 10541 = 275$

$105^2 - 10541 = 11025 - 10541 = 484 = 22^2$

$\Rightarrow x = 105 \qquad y = 22$

$n = (x-y)(x+y) = (105-22)(105+22)$

$= 83 \times 127$

$n = 2931$

$54^2 < 2931 < 55^2$

$5916 < 2931 < 3025$

$55^2 - 2931 = 94$

$56^2 - 2931 = 205$

$57^2 - 2931 = 318$

$\vdots$

$63^2 - 2931 = 1038$

$\underset{\underset{240100}{\parallel}}{490^2} - 2931 = 23769 = 487^2$

$2931 = (490-487)(490+487)$

$= 3 \times 977$

$n = 81518057 \quad , \quad n = 430663 \quad , \quad n = 977$

(وظيفة)

الفصل الرابع:

"معادلات ديوفانتس"

معادلات ديوفانتس الخطية بمجهولين:

تكتب المعادلة بالشكل $n = ax + by$; $a, b, n \in \mathbb{Z}^+$ أعداد

صحيحة موجبة نبحث عن المجاهيل $x, y \in \mathbb{Z}$

- هناك معادلات غير قابلة للحل مثل:

$$2x + 10y = 17$$

ليس لها حل، لأن الطرف الأيمن من المعادلة عدد زوجي والطرف الثاني عدد فردي

ولا يمكن تحقيق المساواة بين الطرفين مهما تكن قيم x و y

- وهناك معادلات لها أكثر من حل مثل:

$$3x + 6y = 18$$

الحلول: $(0, 3)$, $(2, 2)$, $(6, 0)$

مبرهنة:

لتكن لدينا المعادلة $ax + by = c$ (1) ; $c, a, b \in \mathbb{Z}$

$a \cdot b \neq 0$ يكون للمعادلة حل إذا وفقط إذا كان $d(a, b)$ القاسم المشترك الأعظم

للعددين a, b يقسم الطرف الثاني c.

وإذا كان (x_0, y_0) حلاً ما لهذه المعادلة فإن الحل العام (جميع حلول هذه

المعادلة) تعطى بالعلاقات:

$$(2) \begin{cases} x = x_0 + \dfrac{b}{d} t \\ y = y_0 - \dfrac{a}{d} t & ; t \in \mathbb{Z} \end{cases}$$

البرهان:

نعلم أنه إذا كان $d = (a, b)$ فيمكن إيجاد عددين صحيحين a_0, b_0 بحيث يكون:

$$(a_0, b_0) = 1 \quad ; \quad a = a_0 d \qquad b = b_0 d$$

إذا وجد للمعادلة (1) حل وليكن x_0 , y_0 فإن:

$$a x_0 + b y_0 = c$$

$$\Rightarrow d(a_0 x_0 + b_0 y_0) = c \Rightarrow d \mid c$$

وبالعكس إذا كان $d \mid c$ فيمكن أن نكتب

$$c = td \quad ; \quad t \in Z$$

وبما أن d القاسم المشترك الأعظم للعددين a, b فيوجد عددان صحيحان x, y حيث

$$d = ax + by \Rightarrow t.d = a(t.x) + b(t.y) = c$$

نضرب طرفي العلاقة ب t

أي أن:

$tx = x_0$, $ty = y_0$ حل المعادلة

لنثبت الآن أنه إذا عرفنا الحل الخاص x_0 , y_0 للمعادلة (1) فإن أي حل (x, y) يكتب بالنحو (2)

لذا نكتب:

$$a x_0 + b y_0 = c = ax + by$$

$$a(x - x_0) + b(y - y_0) = 0 \Rightarrow a(x - x_0) = b(y_0 - y)$$

ولما كان $d = (a, b)$ فإنه توجد a_0 , b_0 حيث

$$a = a_0 d \qquad , \quad b = b_0 d \qquad (a_0 , b_0) = 1$$

نعوض بالعلاقة الأخيرة:

$$a_0 d (x - x_0) = b_0 d (y_0 - y) \Rightarrow a_0 (x - x_0) = b_0 (y_0 - y) \quad (*)$$

ومنه $a_0 \mid b_0 (y_0 - y)$ ولكن $(a_0 , b_0) = 1$

بالتالي: $a_0 \mid (y_0 - y)$

$$\Rightarrow y_0 - y = a_0 t \Rightarrow y = y_0 - a_0 t \quad ; \quad t \in Z$$

$$\Rightarrow \boxed{y = y_0 - \frac{a}{d} t}$$

نعوض في $(*)$

$$a_0 (x - x_0) = b_0 a_0 t \Rightarrow x = x_0 + b_0 t$$

$$\Rightarrow \boxed{x = x_0 + \frac{b}{d} t} \quad ; \quad t \in Z$$

وهو المطلوب.