الأربعاء: 1/ 4/ 2015

المحاضرة الثامنة:

مبرهنة:

إن جميع الحلول الصحيحة الموجبة لمعادلة فيثاغورث $x^2+y^2=z^2$
حيث y عدد زوجي و $(x,y,z)=1$ تعطى بالعلاقات التالية:

$$x=r^2-s^2 \qquad y=2rs \qquad z=r^2+s^2$$

حيث r, s أعداد صحيحة موجبة و $(r,s)=1$ و r, s أحدهما زوجي والآخر فردي.

الإثبات:

بما أن y عدد زوجي فإنه يكتب $y=2y_1$

$$\Rightarrow y^2=4y_1^2=z^2-x^2$$

$$\Rightarrow y_1^2=\frac{z+x}{2}\cdot\frac{z-x}{2}$$

لنثبت أن $\frac{z-x}{2}$ و $\frac{z+x}{2}$ أوليين فيما بينهما، إذ لو فرضنا أن:

$$\left(\frac{z+x}{2},\frac{z-x}{2}\right)=d>1$$

فإن d يقسم التركيب الخطي لهما أي يقسم مجموعهما وهو z وفرقهما وهو x
$d\mid x$ و $d\mid z$ وهذا غير ممكن لأن $(x,z)=1$
فإذا افترضنا أن x, y, z غير سالبة ولاحظنا أن جداء العددين الصحيحين
$\frac{z-x}{2}$, $\frac{z+x}{2}$ يساوي y_1^2

وحسب التمهيدية (4) يوجد عددان r, s بحيث: $(r,s)=1$

$$\frac{z+x}{2}=r^2 \qquad \frac{z-x}{2}=s^2$$

ومنه نجد أنّ:

$z=r^2+s^2$, $r>s$, $x=r^2-s^2$, $y=2y_1=2rs$

وبما أنّ y زوجي فإن z, x فرديان.

ولأن $z=r^2+s^2$ فردي

نجد أنّ r, s أحدهما فردي والآخر زوجي

لنثبت أن العلاقات تحقق فيثاغورث.

$$x^2+y^2=(r^2-s^2)^2+4r^2s^2$$

$$=r^4-2r^2s^2+s^4+4r^2s^2$$

$$=r^4+2r^2s^2+s^4$$

$$=(r^2+s^2)^2=z^2$$

أي إنّ محققة من أجل جميع الأعداد الصحيحة r, s

وأخيراً إذا ضربنا قيم x, y, z بالعدد الصحيح $k \neq 0$ فإننا نحصل على جميع ثلاثيات فيثاغورث وهو المطلوب.

مثال:

أوجد ثلاثيات فيثاغورث الأولية حيث أنّ $x=15$

الحل:

لدينا: $x=r^2-s^2=(r-s)(r+s)=15$

توجد حالتان:

1) $\left.\begin{array}{l} r-s=1 \\ r+s=15 \end{array}\right\} \Rightarrow$ $r=8$, $s=7$, $(7,8)=1$

وثلاثية فيثاغورث في هذه الحالة $(15, 112, 113)$

/ /

2) $\left.\begin{array}{l} r-s=3 \\ r+s=5 \end{array}\right\} \Rightarrow \begin{array}{l} r=4 \\ s=1 \end{array}$

$(4,1)=1$

وثلاثية فيثاغورث

$(15, 8, 17)$

مثال: صفحة 73

أثبت أن نصف قطر الدائرة الماسة داخلاً لأضلاع مثلث فيثاغورث هو عدد صحيح دوماً.

الحل:

ليكن R نصف قطر الدائرة ، x و y طولي الضلعين القائمين في المثلث و z طول الوتر.

نحسب مساحة المثلث:

$$S=\frac{1}{2}xy=\frac{1}{2}R(x+y+z)$$

$$\Rightarrow R=\frac{x.y}{x+y+z} \quad (1)$$

نعوض قيم x و y و z التالية في العلاقة (1)

$$x=k(r^2-s^2) \qquad y=(2rs)k \qquad z=(r^2+s^2)k$$

$$\Rightarrow R=\frac{2k^2rs(r^2-s^2)}{2k^2r+2krs}=\frac{krs(r^2-s^2)}{r^2+rs}$$

$$R=\frac{krs(r-s)(r+s)}{r(r+s)}=ks(r-s)$$

وهو عدد صحيح دوماً

ومنه $R \in Z^+$ عدد صحيح دوماً

/ /

مثال: (2) صفحة 72

أثبت أنه إذا كان (x, y, z) ثلاثي فيثاغورث أولي فإن أحد الأعداد x, y, z يقبل القسمة على 3.

الحل:

إذا كان $3 \mid y$ تحققت المسألة

إذا كان $3 \nmid y$ فإن $3 \nmid 2rs$ ؛ $y = 2rs$

$\Rightarrow 3 \nmid r \quad , \quad 3 \nmid s$

أي يمكن أن نكتب حسب خوارزمية القسمة:

$3 \nmid r$: $r = 3p + 1$ أو $r = 3p + 2$

و $3 \nmid s$: $s = 3q + 1$ أو $s = 3q + 2$

ومنه فإن:

$$x = r^2 - s^2 = (3p+1)^2 - (3q+2)^2$$
$$= 9p^2 + 6p + 1 - 9q^2 - 12q - 4$$
$$= 9(p^2 - q^2) - 6(-2qp) - 3 = 3M \Rightarrow 3 \mid x$$

$$x = r^2 - s^2 = (3p+1)^2 - (3q+1)^2$$
$$= 9p^2 + 6p + 1 - 9q^2 - 6q - 1$$
$$= 9p^2 - 9q^2 + 6p - 6q = 3N$$

$\Rightarrow 3 \mid x$

الباب الثاني:

الفصل الأول: "التطابقات"

تعريف التطابق:

ليكن $a,b \in \mathbb{Z}$ و $m \in \mathbb{Z}^+$ نقول إنّ العدد a يطابق العدد b بالمقاس m ونكتب $a \equiv b \pmod{m}$ إذا كان $m \mid (a-b)$

أو يوجد $q \in \mathbb{Z}$ بحيث $a-b=qm \Leftarrow a=mq+\underset{\text{الباقي}}{b}$

mod نقرأ مقاس

أما إذا كان:

$$m \nmid a-b \quad \Leftrightarrow \quad a \not\equiv b \pmod{m}$$

فإننا نقول إنّ a لا يطابق b بالمقاس m

مثال:

$$5=m \mid (7-2) \Leftarrow 7 \equiv 2 \pmod{5}$$

صفوف البواقي:

إذا كان m عدداً صحيحاً أكبر من الواحد و $a \in \mathbb{Z}$ فإنه يوجد عددان وحيدان q,r بحيث يكون $0 \leq r < m$

$$a=mq+r$$

إن القيم التي تأخذها r:

$$r \in \{0,1,2,\dots,m-1\}$$

نأخذ جميع الأعداد التي تترك باقي r من المجموعة في صف باقي 6 حيث نضع كل الأعداد الصحيحة التي باقي قسمتها على m يساوي أحد الأعداد r_i في صف واحد نسميه صف الباقي r_i فنحصل على m من هذه الصفوف.

* كل عددان ينتميان إلى صف واحد يكون الفرق بينهما من مضاعفات m

* الفرق بين كل عددين من صف واحد هو من مضاعفات m.

مثال:

$m = 6$ فإن صفوف البواقي هي:

$r = 0, 1, 2, 3, 4, 5$

صف الباقي $[0]$:

$\{ ---, -12, -6, 0, 6, 12, 18, -- \}$

صف الباقي $[1]$:

$\{ ---, -11, -5, 1, 7, 13, 19, -- \}$

صف الباقي $[2]$: إذا طرحنا أي عددين سيكون من مضاعفات 6

$\{ ---, -10, -4, 2, 8, 14, 20, -- \}$

صف الباقي $[3]$:

$\{ ---, -9, -3, 3, 9, 15, 21, -- \}$

صف الباقي $[4]$:

$\{ ---, -8, -2, 4, 10, 16, 22, -- \}$

صف الباقي $[5]$:

$\{ --, -7, -1, 5, 11, 17, 23, -- \}$

وبذلك نكون وزعنا جميع الأعداد الصحيحة على الصفوف.

مجموعة البواقي التامة:

تعريف: الفرق بين كل عددين هو من مضاعفات m

نسمي مجموعة الأعداد الصحيحة A التي عدد عناصرها يساوي m التي ينتمي كل عنصر منها إلى صف واحد فقط من صفوف بواقي العدد m مجموعة البواقي التامة بالمقياس m.

مثال:

$A = \{0, 1, 2, 3, 4\}$ مجموعة بواقي تامة بالمقياس 5

$B=\{0,6,12,-2,4\}$ مجموعة بواقي تامة بالمقاس 5.

$\{0,1,2,\dots,m-1\}$ مجموعة بواقي تامة بالمقاس m

خواص التطابقات:

الأعداد $a,b,c,d\in\mathbb{Z}$, $m>0$

1) إنّ علاقة التطابق هي علاقة تكافؤ على مجموعة الأعداد الصحيحة.

البرهان:

إذا كان $a,b,c\in\mathbb{Z}$ و $m\in\mathbb{Z}^{+}$ فإنّ:

$a\equiv a \pmod{m}$ لأنّ $m\mid a-a$

و

$$a\equiv b \pmod{m} \Rightarrow b\equiv a \pmod{m}$$

لأنّ:

$$m\mid a-b \Rightarrow m\mid b-a$$

و

$$a\equiv b \pmod{m} \wedge b\equiv c \pmod{m} \Rightarrow a\equiv c \pmod{m}$$

لأنّ:

$$a-b=k_1 m \quad \wedge \quad b-c=k_2 m \Rightarrow a-c=(k_1+k_2)m$$

2) إذا كان $a\equiv b \pmod{m}$ و $k\in\mathbb{Z}$ فإنّ $ka\equiv kb \pmod{m}$

لأنّ $a-b=Mm$ فإذا ضربنا الطرفين بالعدد k نجد:

$$ka-kb=(KM)m$$

3) إذا كان $a\equiv b \pmod{m}$ $\wedge$ $c\equiv d \pmod{m}$

فإنّ:

$$a\pm c\equiv b\pm d \pmod{m}$$

البرهان:

لما كان $a-b=M_1 m$ و $c-d=M_2 m$

فإن:

$$(a-b)\pm(c-d)=(M_1\pm M_2)m$$

أي

$(a\pm c)-(b\pm d)=Mm$ و $M=M_1\pm M_2$

ويمكن تعميم هذه الخاصية فنكتب:

إذا كان $a_i\equiv b_i\,(\mathrm{mod}\,m)$ من أجل جميع القيم $i=1,2,\dots,n$

فإن:

$\sum_{i=2}^{n} a_i \equiv \sum_{i=1}^{n} b_i\,(\mathrm{mod}\,m)$ ويمكن إثبات ذلك بطريقة الاستقراء الرياضي.

4)- مبرهنة:

إذا كان

$a\equiv b\,(\mathrm{mod}\,m)$ و $c\equiv d\,(\mathrm{mod}\,m)$ فإن $a.c=bd\,(\mathrm{mod}\,m)$

لدينا

$$a\equiv b\,(\mathrm{mod}\,m) \Rightarrow ac\equiv bc\,(\mathrm{mod}\,m)$$

و

$$c\equiv d\,(\mathrm{mod}\,m) \Rightarrow bc\equiv bd\,(\mathrm{mod}\,m)$$

أي

$a.c\equiv bd\,(\mathrm{mod}\,m)$ وهو المطلوب

5) إذا كان $a\equiv b\,(\mathrm{mod}\,m)$ فإن $a^n\equiv b^n\,(\mathrm{mod}\,m)$ حيث $n\geqslant 0$

البرهان:

الخطوة الأساسية في الاستقراء:

من أجل $n=0$ و $n=1$ العلاقة محققة.

خطوة الاستقراء: لنفرض صحتها من أجل $n=k$ ولنثبت صحتها من أجل $n=k+1$

لذا نكتب

$$a^k \equiv b^k \pmod m$$

وحسب الخاصة (4) نكتب

$$a.a^k \equiv b.b^k \pmod m$$

الأمر الذي يثبت صحة العلاقة

$$a^{k+1} \equiv b^{k+1} \pmod m$$ المطلوبة

أي أن العلاقة صحيحة $\forall n \geq 0$

6) إذا كان $a \equiv b \pmod m$ وإذا كان $f(x) = \sum_{i=0}^{n} a_i x^i$ حيث $a_i \in \mathbb{Z}$

$n \geq i \geq 0$ فإن:

$$f(a) \equiv f(b) \pmod m$$

البرهان:

بما أن $a \equiv b \pmod m$ فإن $a^i \equiv b^i \pmod m$ حسب الخاصة (5)

وكذا

$a_i a^i \equiv a_i b^i \pmod m$ أي:

$$\sum_{i=0}^{n} a_i a^i \equiv \sum_{i=0}^{n} a_i b^i \pmod m$$

أي:

$$f(a) \equiv f(b) \pmod m$$

انتهت المحاضرة ...