التطابقات

د/ فهد الشمري

٣,١ الخواص الأساسية للتطابقات

Basic Properties of Congruences

تعريف

ليكن $n \in \mathbb{Z}$ و $a,b \in \mathbb{Z}^+$. نقول إن

a يطابق b قياس n ونكتب $a \equiv b \pmod{n}$ إذا كان $n | a-b$

فإذا كان $n \nmid a-b$ نقول إن a لا يطابق b قياس n كما نكتب $a \not\equiv b \pmod{n}$.

مثال١

الحـل

مبرهنة١,٣ ليكن $n \in \mathbb{Z}$. إذا كان $a,b \in \mathbb{Z}$ فإن

$a \equiv b \pmod{n} \quad \Leftrightarrow \quad$ وجد عدد صحيح k بحيث $a = b + kn$

البرهان.

٣,٢ التطابقات الخطية

Linear Congruences

إذا كان x متغيرا، نسمي

$x^{10} - x + 2 \equiv 7 \pmod{14}$ تطابق من الدرجة 10

$3x + 2 \equiv 5 \pmod{9}$ تطابق خطي

التطابق الخطي له الصورة: $ax \equiv b \pmod{n}$ ، حيث $a,b \in \mathbb{Z}$ و $n \in \mathbb{Z}^+$

- ❖ يوجد حل للتطابق $\Leftrightarrow$ $n \mid ax - b$ $\Leftrightarrow$ يوجد $y \in \mathbb{Z}$ بحيث $ax - b = ny$ أي $ax - ny = b$
- ❖ إذا كان x_0 حلا للتطابق، وكان $x_1 \equiv x_0 \pmod{n}$ فإن x_1 هو أيضا حل. أي أن مجموعة الأعداد $[x_0]$ كلها حلول.

نريد معرفة حلول التطابق غير المتطابقة قياس n:

مبرهنة ٣,٦ للتطابق الخطي $ax \equiv b \pmod{n}$ حل $\Leftrightarrow$ $(a,n) \mid b$. وإذا كان x_0 حلا فإن الحلول غير المتطابقة قياس n هي: $x = x_0 + \frac{n}{(n,a)}k$ حيث $k = 0,1,\ldots,(a,n)-1$.

البرهان. التطابق المعطى يكافئ المعادلة الديوفنتية $ax - ny = b$ والتي لها حل إذا وفقط إذا $(a,n) \mid b$. إذا كان x_0 و y_0 حلا لهذه الأخيرة فإن جميع الحلول الصحيحة هي:

$$x = x_0 + \frac{n}{(n,a)}k$$

$$y = y_0 + \frac{a}{(n,a)}k$$ ، حيث $k \in \mathbb{Z}$.

سوف نبرهن أن حلول التطابق: $x = x_0 + \frac{n}{(n,a)}k$ لقيم k من 0 إلى $(n,a) - 1$

تحقق: ❶ غير متطابقة قياس n ❷ كل حل يطابق أحد هذه الحلول.

❶ نفرض لغرض التناقض أن

$$x_0 + \frac{n}{(n,a)}k_1 \equiv x_0 + \frac{n}{(n,a)}k_2 \pmod{n}$$ حيث $0 \le k_1 < k_2 \le (n,a) - 1$

ولكن هذا يعني أن

$$\begin{aligned} & x_0 + \frac{n}{(n,a)}k_1 \equiv x_0 + \frac{n}{(n,a)}k_2 \pmod{n} \\ \Leftrightarrow & \frac{n}{(n,a)}k_1 \equiv \frac{n}{(n,a)}k_2 \pmod{n} \\ \Leftrightarrow & k_1 \equiv k_2 \left(\bmod \frac{n}{\frac{n}{(n,a)}}\right) \\ \Leftrightarrow & k_1 \equiv k_2 \pmod{(n,a)} \Leftrightarrow (n,a) \mid k_2 - k_1 \end{aligned}$$

وهذا مستحيل لأن $0 \le k_2 - k_1 \le (n,a)$.

❷ لنعتبر أي حل صحيح $x = x_0 + \frac{n}{(n,a)}k$ حيث $k \in \mathbb{Z}$. باستخدام خوارزمية القسمة نستطيع كتابة

$$k = q(n,a) + r$$ حيث $0 \le r \le (n,a) - 1$

بالتعويض عن k نجد أن $x \equiv x_0 + \frac{n}{(n,a)}r \pmod{n}$ كما أردنا.

مثال ٢ جد الحلول غير المتطابقة قياس 18 للمعادلة: $21x \equiv 12 \pmod{18}$.

الحل بما أن $(18,21) = 3 \mid 12$ فإن معادلة التطابق لها 3 حلول غير متطابقة قياس 18. نوجد أحدها بإحدى الطريقتين:

❶ باستخدام خوارزمية إقليدس نوجد أحد حلول المعادلة الديوفنتية $21x + 18y = 12$.

❷ بالتجريب في أعداد نظام الرواسب التام قياس 18 $\{0,1,2,\ldots,17\}$:
معادلة التطابق أعلاه تكافئ المعادلة $3x \equiv 12 \pmod{18}$ والتي لها الحل $x \equiv 4 \pmod{18}$. الحلول غير المتطابقة هي

$x = 4 + \frac{18}{3}k = 4 + 6k$ حيث $k = 0,1,2$. ■

يمكن الاستفادة من هذه الطريقة في حل المعادلات الديوفنتية.

مثال ٣ جد حلول المعادلة الديوفنتية: $9x + 5y = 13$.

الحل هذه المعادلة تكافئ التطابق $9x \equiv 13 \pmod{5}$ الذي يكافئ $4x \equiv 3 \pmod{5}$. وحيث $(5,4) = 1 \mid 3$ فإن التطابق له حل وحيد قياس 5:

$$x \equiv 4^{-1}3 \equiv 2 \pmod{5}$$

نحصل بذلك على الجزء الأول من حل العام للمعادلة الأصلية $x = 2 + 5k$، نعوض الآن في المعادلة لنحصل على:

$$y = -1 - 9k$$

٣,٣ أنظمة التطابقات الخطية بمتغير واحد

Systems of Linear Congruences in One Variable

مثال E جد أصغر عدد صحيح موجب x يحقق:

- ❖ إذا قسم على 3 بقي 2
- ❖ وإذا قسم على 4 بقي 3
- ❖ وإذا قسم على 5 بقي 4

الحـــل العدد المطلوب لابد أن يحقق التطابقات الثلاثة:

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{4}$$
$$x \equiv 4 \pmod{5}$$

❖ ليتحقق التطابق الأول يجب أن يكون x على الصورة: $x = 2 + 3k_1$ حيث $k_1 \in \mathbb{Z}$.

❖ لتحقق التطابق الثاني يجب اختيار k_1 بحيث:

$$\begin{aligned} 2 + 3k_1 &\equiv 3 \pmod{4} \\ \Leftrightarrow 3k_1 &\equiv 1 \pmod{4} \\ \Leftrightarrow k_1 &\equiv 3 \pmod{4} \end{aligned}$$

أي يجب أن يكون k_1 على الصورة : $k_1 = 3 + 4k_2$ لأي $k_2 \in \mathbb{Z}$. لذا فإن x يحقق التطابقين الأول والثاني إذا وفقط إذا كان x على الصورة: $x = 2 + 3(3 + 4k_2)$ أي $x = 11 + 12k_2$ لأي $k_2 \in \mathbb{Z}$.

❖ لتحقق التطابق الثالث يجب اختيار k_2 بحيث:

$$\begin{aligned} 11 + 12k_2 &\equiv 4 \pmod{5} \\ \Leftrightarrow 12k_2 &\equiv -7 \pmod{5} \\ \Leftrightarrow 2k_2 &\equiv 3 \pmod{5} \\ \Leftrightarrow k_2 &\equiv 2^{-1}3 \pmod{5} \\ \Leftrightarrow k_2 &\equiv 4 \pmod{5} \end{aligned}$$

أي أن k_2 لابد على الصورة: $k_2 = 4 + 5k_3$ لأي $k_3 \in \mathbb{Z}$ ، وبالتالي فإن x يحقق التطابقات الثلاث إذا وفقط إذا كان على الصورة: $x = 11 + 12(4 + 5k_3)$ أي $x = 59 + 60k_3$ وذلك لأي $k_3 \in \mathbb{Z}$.

لاحظ أن 59 هو أصغر عدد صحيح موجب يحقق المطلوب.

ليكن لدينا نظام التطابقات الخطي

$$\begin{aligned} a_1 x &\equiv c_1 \pmod{m_1} \\ a_2 x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ a_k x &\equiv c_k \pmod{m_k} \end{aligned} \qquad ✪$$

وليكن x_i حلا لتطابق $a_ix \equiv c_i \pmod{m_i}$ حيث $1 \le i \le k$. الآن x هو حل للنظام ✪ إذا وفقط إذا كان x حلا للنظام

$$\begin{aligned} x &\equiv x_1 \left(\bmod \tfrac{m_1}{(a_1,m_1)}\right) \\ x &\equiv x_2 \left(\bmod \tfrac{m_2}{(a_2,m_2)}\right) \\ &\vdots \\ x &\equiv x_k \left(\bmod \tfrac{m_k}{(a_k,m_k)}\right) \end{aligned} \qquad ✪✪$$

وندرس الآن حلول الأنظمة على الصورة ✪✪.

مبرهنة٣,٣ إذا كانت الأعداد $m_1, m_2, \ldots, m_k$ أولية نسبيا مثنى مثنى فإن النظام

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

له حل وحيد قياس العدد $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

البرهان. لنعتبر الأعداد

$$M_i = \frac{M}{m_i} = \prod_{\substack{j=1 \\ j \ne i}}^{k} m_j = m_1 \cdot m_2 \cdot \ldots \cdot \widehat{m}_i \cdot \ldots \cdot m_k \quad \text{،} \quad \text{لكل } i = 1,2,\ldots,k$$

$(M_i, m_i) = 1$ لأن $(m_j, m_i) = 1$ لكل $j \ne i$. باعتبار z_i هو معكوس لـ M_i قياس m_i سوف نثبت أن العدد

$$x = c_1M_1z_1 + c_2M_2z_2 + \ldots + c_kM_kz_k$$

هو حل للنظام: لكل $i = 1,2,\ldots,k$ لدينا $m_i \mid M_j$ عندما $i \ne j$ وبالتالي

$$\begin{aligned} x &= c_1M_1z_1 + c_2M_2z_2 + \ldots + c_iM_iz_i + \ldots + c_kM_kz_k \\ &\equiv c_1 \cdot 0 \cdot z_1 + c_2 \cdot 0 \cdot z_2 + \ldots + c_i \cdot 1 + \ldots + c_k \cdot 0 \cdot z_k \\ &\equiv c_i \pmod{m_i} \end{aligned}$$

لبرهان أن الحل وحيد قياس M نفرض أن u و v حلان للنظام. هذا يعني $u \equiv v \equiv c_i \pmod{m_i}$ لكل $i = 1,2,\ldots,k$.
إذن $m_i \mid u - v$ لكل $i = 1,2,\ldots,k$ ومنه فإن $M \mid u - v$ أي $u \equiv v \pmod{M}$.

مثال٥ جد أصغر عدد صحيح موجب إذا قسم على 3 بقي 2 وإذا قسم على 4 بقي 3 وإذا قسم على 5 بقي 4.

الحــل المطلوب هو حل النظام

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

الأعداد 3، 4، 5 أولية نسبيا مثنى مثنى نحسب العدد x في مبرهنة الباقي الصينية: لدينا $M = 3 \cdot 4 \cdot 5 = 60$ ، أيضا

$$M_1 = 20 \qquad M_2 = 15 \qquad M_3 = 12$$

كما أن

$$\begin{array}{ccc} 20z_1 \equiv 1 \pmod 3 & 15z_2 \equiv 1 \pmod 4 & 12z_3 \equiv 1 \pmod 5 \\ 2z_1 \equiv 1 \pmod 3 & 3z_2 \equiv 1 \pmod 4 & 2z_3 \equiv 1 \pmod 5 \\ z_1 \equiv 2 \pmod 3 & z_2 \equiv 3 \pmod 4 & z_3 \equiv 3 \pmod 5 \end{array}$$

والحل هو

$$\begin{aligned} x &= 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \\ &= 80 + 135 + 144 \\ &\equiv 20 + 15 + 24 \\ &\equiv 59 \pmod{60} \end{aligned}$$

■

لنعتبر النظام في الحالة العامة:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}\right\} \quad \star$$

لأي $m_1, m_2, \ldots, m_k \in \mathbb{Z}^+$ و $c_1, c_2, \ldots, c_k \in \mathbb{Z}$.

نقول إن النظام $\star$ منسجم إذا كان $c_i \equiv c_j \pmod{(m_i, m_j)}$ لكل $1 \leq i, j \leq k$.

مبرهنة ٣,٤ (أ) النظام $\star$ له حل $\Leftrightarrow$ النظام منسجم.

(ب) حل النظام $\star$ إن وجد فهو وحيد قياس $[m_1, m_2, \ldots, m_k]$.

البرهان. (أ) لنفرض أن النظام له حل وليكن x_0، أي لكل $i = 1, 2, \ldots, k$، $x_0 \equiv c_i \pmod{m_i}$. لكل $1 \leq i, j \leq k$،
$(m_i, m_j) \mid m_i$ و $(m_i, m_j) \mid m_j$ $\Leftarrow$ $x_0 \equiv c_i \pmod{(m_i, m_j)}$ و $x_0 \equiv c_j \pmod{(m_i, m_j)}$
إذن $c_i \equiv c_j \pmod{(m_i, m_j)}$.
لنفرض الآن أن النظام منسجم ونثبت أن له حل: بتحليل الأعداد إلى قوى عواملها الأولية

$$\begin{aligned} m_1 &= p_{11}^{n_{11}} \cdot p_{12}^{n_{12}} \cdot \ldots \cdot p_{1t_1}^{n_{1t_1}} \\ m_2 &= p_{21}^{n_{21}} \cdot p_{22}^{n_{22}} \cdot \ldots \cdot p_{2t_2}^{n_{2t_2}} \\ &\vdots \\ m_k &= p_{k1}^{n_{k1}} \cdot p_{k2}^{n_{k2}} \cdot \ldots \cdot p_{kt_k}^{n_{kt_k}} \end{aligned}$$

فالنظام أعلاه يكافئ

$$\begin{array}{ccc} & & x \equiv c_1 \pmod{p_{11}^{n_{11}}} \\ & & x \equiv c_1 \pmod{p_{12}^{n_{12}}} \\ x \equiv c_1 \pmod{m_1} & \Leftrightarrow & \vdots \\ & & x \equiv c_1 \pmod{p_{1t_1}^{n_{1t_1}}} \\ \vdots & \vdots & \vdots \\ & & x \equiv c_k \pmod{p_{k1}^{n_{k1}}} \\ & & x \equiv c_k \pmod{p_{k2}^{n_{k2}}} \\ x \equiv c_k \pmod{m_k} & \Leftrightarrow & \vdots \\ & & x \equiv c_k \pmod{p_{kt_k}^{n_{kt_k}}} \end{array}$$

نهمل جميع التطابقات قياس قوى العامل الأولي p ماعدا تطابقا واحدا قياس p لأكبر قوة ممكنة. ليكن $x \equiv c_i \pmod{p^r}$ من التطابقات المهملة. إذن تم الاحتفاظ بتطابق من الشكل $x \equiv c_j \pmod{p^s}$ حيث $s \geq r$. لدينا $p^s \mid m_j$ و $p^r \mid m_i$ وحيث $s \geq r$ فإن $p^r \mid m_j \Leftarrow p^r \mid (m_i, m_j)$. لأن النظام منسجم

$p^r \mid (m_i, m_j)$ $\qquad c_i \equiv c_j \pmod{(m_i, m_j)} \Rightarrow c_i \equiv c_j \pmod{p^r}$

لأن $p^r \mid p^s$ $\qquad x \equiv c_j \pmod{p^s} \Rightarrow x \equiv c_j \pmod{p^r}$

لنحصل على التطابق المهمل $x \equiv c_i \pmod{p^r}$. وهكذا فإن النظام المكون من التطابقات الباقية يكافئ ☆ وقياساته أولية نسبيا مثنى مثنى. من مبرهنة الباقي الصينية يوجد حل للنظام ☆ وهذا الحل وحيد قياس حاصل ضرب القياسات.

(ب) واضح من ملاحظة أن حاصل ضرب القياسات يساوي $[m_1, m_2, \ldots, m_k]$.

كطريقة للحل:

❶ لمعرفة إن كان الحل موجودا: تأكد من تحقق $c_i - c_j \mid (m_i, m_j)$ لكل i و j.

❶ اكتب $[m_1, m_2, \ldots, m_k] = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_r^{n_r}$ (عوامل أولية مختلفة)، ثم كون نظام التطابقات المكافئ بتعيين تطابق واحد قياس $p_j^{n_j}$ لكل $j = 1, 2, \ldots, r$ وذلك حسب القاعدة:

$$x \equiv c_i \pmod{p_j^{n_j}} \text{ إذا كان } p_j^{n_j} \mid m_i$$

❸ استخدم مبرهنة الباقي الصينية لإيجاد الحل.

مثال٦ حل نظام التطابقات

$$\begin{aligned} x &\equiv 3 \pmod{10} \\ x &\equiv 8 \pmod{15} \\ x &\equiv 5 \pmod{84} \end{aligned}$$

الحــل

٣,٤ بعض التطابقات الخاصة

مبرهنة٣,٥ (أويلر) ليكن $n \in \mathbb{Z}^+$. إذا كان $(a,n)=1$ فإن $a^{\varphi(n)} \equiv 1 \pmod n$ حيث $\varphi(n)$ هي دالة أويلر.

البرهان. لنعتبر أن $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ مجموعة أعداد تمثل نظام رواسب مختزل قياس n. حيث $(a,n)=1$ فالمجموعة $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ هي أيضا نظام رواسب مختزل. لأن كل عدد من المجموعة الثانية يتطابق قياس n مع واحد من الأولى:

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi(n)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \pmod n$$
$$a^{\varphi(n)} r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \pmod n$$
$$a^{\varphi(n)} \equiv 1 \pmod n \qquad \text{لأن } \left(r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)}, n\right) = 1$$

ملاحظة: عكس مبرهنة أويلر أيضا صحيح: إذا كان $a^{\varphi(n)} \equiv 1 \pmod n$ فإن $(a,n)=1$.

البرهان. إذا كان $a^{\varphi(n)} \equiv 1 \pmod n$ فإن $(a^{\varphi(n)}, n) = 1 \Leftarrow (a,n)=1$.

نتيجة(١) (مبرهنة فيرما الصغرى) إذا كان p أوليا وكان a عددا صحيحا بحيث $p \nmid a$ فإن $a^{p-1} \equiv 1 \pmod p$.

البرهان. بما أن p أولي فإن $p \nmid a$ تعني $(a,p)=1$، كما أن $\varphi(p) = p-1$. وبالتالي $a^{p-1} \equiv 1 \pmod p$.

نتيجة(٢) إذا كان p أوليا فإن $a^p \equiv a \pmod p$ لكل $a \in \mathbb{Z}$.

البرهان. إذا كان $p \nmid a$، لدينا $a^{p-1} \equiv 1 \pmod p \Leftarrow a^p \equiv a \pmod p$.

إذا كان $p \mid a$ فإن $a \equiv 0 \pmod p$ وأيضا $a^p \equiv 0 \pmod p \Leftarrow a^p \equiv a \pmod p$.

نتيجة(٣) إذا كان $(a,n)=1$ فإن:

(أ) $a^{\varphi(n)-1}$ نظير ضربي للعدد a قياس n.

(ب) الحل الوحيد للتطابق: $ax \equiv b \pmod n$ هو $x \equiv a^{\varphi(n)-1} b \pmod n$

البرهان. (أ) $a \cdot a^{\varphi(n)-1} = a^{\varphi(n)} \equiv 1 \pmod n$.

(ب) بما أن $a^{-1} \equiv a^{\varphi(n)-1} \pmod n$ فإن $ax \equiv b \pmod n \Leftrightarrow x \equiv a^{\varphi(n)-1} b \pmod n$.

مثال١١ أوجد خانتي الآحاد والعشرات للعدد 3^{8882}.

الحــل بما أن $(3,100)=1$ سوف نستخدم مبرهنة أويلر. لدينا $\varphi(100) = 40$:

$$3^{8882} = 3^{222\cdot 40+2} = \left(3^{40}\right)^{222} \cdot 3^2 \equiv 1^{222} \cdot 9$$
$$\equiv 9 \pmod{100}$$

مثال ٦ إذا كان $(mn,42)=1$ فأثبت أن $168 \mid m^6-n^6$.

الحل في البداية لاحظ أن $168=42\cdot 4=7\cdot 3\cdot 2^3$، ومن مبرهنة فيرما

❖ $m^6 \equiv 1(\bmod 7)$، $n^6 \equiv 1(\bmod 7) \Leftarrow m^6-n^6 \equiv 0(\bmod 7)$

❖ $m^2 \equiv 1(\bmod 3)$، $n^2 \equiv 1(\bmod 3) \Leftarrow m^6 \equiv 1(\bmod 3)$، $n^6 \equiv 1(\bmod 3) \Leftarrow$ $m^6-n^6 \equiv 0(\bmod 3)$

❖ الآن $m \equiv n \equiv 1(\bmod 2) \Leftarrow m-n \equiv 0(\bmod 2)$ ولأن $m^3-n^3=(m-n)(m^2+2mn+n^2)$ $\Leftarrow 4 \mid m^3-n^3$. وحيث $2 \mid m^3+n^3$ فإن $8 \mid (m^3-n^3)(m^3+n^3)=m^6-n^6$.

وبما أن $(7,3,8)=1$ فإن $168=7\cdot 3\cdot 8 \mid m^6-n^6$.

العدد شبه الأولي

نقول إن العدد المؤلف $n \in \mathbb{Z}^+$ شبه أولي للأساس b إذا تحقق $b^n \equiv b(\bmod n)$

تمهيدية. ليكن p أوليا. إذا كان $a \in \{1,2,\ldots,p-1\}$ يحقق $a^2 \equiv 1(\bmod p)$ فإن $a \in \{1,p-1\}$.

البرهان. $p \mid a^2-1 \Leftarrow p \mid (a-1)(a+1) \Leftarrow p \mid a-1$ أو $p \mid a+1 \Leftrightarrow a \in \{1,p-1\}$.

مبرهنة ٣,٦ (ولسن) إذا كان p أوليا فإن $(p-1)! \equiv -1(\bmod p)$

البرهان. المبرهنة واضحة في حالة $p=2$، وعليه نفرض أن $p>2$. من التمهيدية تتكون المجموعة $\{2,\ldots,p-2\}$ تتكون من أزواج كل عدد ونظيره، لذا فالضرب

$$2\cdot 3\cdot\ldots\cdot p-2 \equiv 1(\bmod p)$$

لنجد أن

$$(p-1)! \equiv p-1 \equiv -1(\bmod p)$$

لتوضيح ما فعلناه في البرهان السابق اعتبر $p=17$:

$$2\cdot 3\cdot 5\cdot\ldots\cdot 15=(2\cdot 9)(3\cdot 6)(4\cdot 13)(5\cdot 7)(8\cdot 15)(10\cdot 12)(11\cdot 14) \equiv 1(\bmod p)$$

والحقيقة أن عكس مبرهنة ولسن أيضا صحيح.

مبرهنة ٣,٧ (عكس ولسن) إذا كان $(n-1)! \equiv -1(\bmod n)$ فإن n عدد أولي.

البرهان. لنفرض أن n مؤلفا عندها يوجد له قاسم أولي q وحيث $q \le n-1$ فإن $q \mid (n-1)!$ وبما أن $n \mid (n-1)!+1$ فإن $q \mid (n-1)!+1$ لنستنتج أن $q \mid ((n-1)!+1)-(n-1)!=1$ وهذا مستحيل.

ملاحظات:

❖ ولسن وعكسها تقدمان طريقة لاختبار أولية العدد الصحيح ولكن ذلك غير مفيد في الحسابات إذ أن المضروب يصبح كبيرا بسرعة مع كبر العدد n.

❖ من المفيد في كثير من المسائل تذكر أن أي مجموعة رواسب مختزلة قياس p تطابق المجموعة المعتادة $\{1,2,\ldots,p-1\}$ وبالتالي فإن ضرب أعداد نظام رواسب مختزل قياس p أيضا يطابق $-1(\bmod p)$.

بعض التطبيقات على مبرهنتي فيرما وولسن

مبرهنة٣،٦ ليكن p عددا أوليا فرديا. يوجد حل للتطابق $x^2 \equiv -1 (\bmod p) \Leftrightarrow p \equiv 1 (\bmod 4)$، وفي هذه الحالة فأحد الحلول هو $x = \left(\frac{p-1}{2}\right)!$.

البرهان. لنفرض وجود عدد x يحقق $x^2 \equiv -1 (\bmod p)$، برفع طرفي التطابق للقوة $\frac{p-1}{2}$ نجد أن

$$(-1)^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 (\bmod p)$$

العدد $(-1)^{\frac{p-1}{2}}$ إما يساوي 1 أو -1 وحيث p فردي فإن $-1 \not\equiv 1 (\bmod p)$ وعليه فإن $(-1)^{\frac{p-1}{2}} = 1$. إذن $\frac{p-1}{2}$ زوجي، $2 \mid \frac{p-1}{2}$ وبالتالي $2 \cdot 2 \mid 2 \cdot \frac{p-1}{2}$ أي $4 \mid p-1 \Leftrightarrow p \equiv 1 (\bmod 4)$.

لنفرض الآن أن $p \equiv 1 (\bmod 4)$ ونثبت أنه يوجد حل. لدينا

$$(p-1)! \equiv -1 (\bmod p) \qquad ✪$$

نعيد كتابة $(p-1)!$ بطريقة أخرى كما يلي

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot p-2 \cdot p-1 \\ &= 1 \cdot 2 \cdot \ldots \cdot j \cdot \ldots \cdot \frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right) \cdot \ldots \cdot (p-j) \cdot \ldots \cdot (p-2) \cdot (p-1)\end{aligned}$$

حدود الضرب هي تماما الأزواج j و $p-j$ حيث $j = 1,2,\ldots,\frac{p-1}{2}$، كما أن

$$j(p-j) = jp - j^2 \equiv -j^2 (\bmod p)$$

لكل $j = 1,2,\ldots,\frac{p-1}{2}$. إذن لدينا التطابق

$$\begin{aligned}(p-1)! &\equiv -1^2 \cdot -2^2 \cdot \ldots \cdot -j^2 \cdot \ldots \cdot -\left(\frac{p-1}{2}\right)^2 \\ &\equiv (-1)^{\frac{p-1}{2}} \cdot 1^2 \cdot 2^2 \cdot \ldots \cdot j^2 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)^2 \\ &\equiv \left(1 \cdot 2 \cdot \ldots \cdot j \cdot \ldots \cdot \frac{p-1}{2}\right)^2 \\ &\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 (\bmod p)\end{aligned}$$

لأن $p \equiv 1 (\bmod 4)$ فإن $(-1)^{\frac{p-1}{2}} = 1$. من التطابق ✪ نرى أن $x = \left(\frac{p-1}{2}\right)!$ هو حل للتطابق $x^2 \equiv -1 (\bmod p)$.

مثال٩ حل التطابق $x^2 \equiv -1 (\bmod 29)$.

الحـــل لأن $29 \equiv 1 (\bmod 4)$، فيوجد حل كما أن أحد هذه الحلول هو $x = \left(\frac{29-1}{2}\right)! = 14!$

مثال١٠ هل يمكن تجزئة أي 6 أعداد متتالية لمجموعتين بحيث ضرب أعداد الأولى يساوي ضرب أعداد الثانية؟

الحـــل سوف نثبت أن ذلك مستحيل. لنعتبر أن الأعداد الستة هي

$$n, n+1, n+2, n+3, n+4, n+5$$

بتجزئة المجموعة $\{n, n+1, n+2, n+3, n+4, n+5\}$ إلى مجموعتين لنعتبر أن ضرب أعداد الأولى يساوي a وأن ضرب أعداد الثانية يساوي b.

لأنها ستة أعداد متعاقبة، فالعدد 7 إما يقسم عددا واحدا فقط أو أن جميعها لا تقبل القسمة على 7. في الحالة الأولى العدد 7 يقسم واحد فقط من العددين a و b، لذا a و b مختلفان. وإذا كان العدد 7 لا يقسم أي من الأعداد الستة، فإن

$$n\cdot(n+1)\cdot(n+2)\cdot(n+3)\cdot(n+4)\cdot(n+5) \equiv 6! \equiv -1 \pmod 7$$

أي أن $ab \equiv -1 \pmod 7$. لو فرضنا أن $a = b$ فالتطابق السابق هو $a^2 \equiv -1 \pmod 7$ وبالتالي $x = a$ هو حل للتطابق $x^2 \equiv -1 \pmod 7$ وهذا مستحيل لأن $7 \not\equiv 1 \pmod 4$.

نتيجة(E) يوجد عدد لانهائي من الأعداد الأولية على الصورة $p = 4k+1$.

البرهان. لنفرض لغرض التناقض أن $\{p_1, p_2, \ldots, p_k\}$ هي مجموعة جميع الأعداد الأولية التي على الصورة $4k+1$. لنعتبر العدد

$$(2p_1p_2\ldots p_k)^2 + 1$$

إذا كان p قاسما أوليا لهذا العدد فإن p فردي، ومنه سوف يحقق التطابق $(2p_1p_2\ldots p_k)^2 \equiv -1 \pmod p$. من المبرهنة السابقة لابد أن $p \equiv 1 \pmod 4$ ومن الفرض يوجد $1 \le i \le k$ بحيث $p = p_i$ ومنه ينتج $p \mid 1$ وهذا تناقض.

مثالII أثبت أنه يوجد عدد لا نهائي من ألأعداد الأولية التي على الصورة $p = 4k+3$.

الحــل لنفرض لغرض التناقض أن $\{p_1, p_2, \ldots, p_l\}$ هي جميع الأعداد الأولية التي على الصورة $4k+3$. لنعتبر العدد $2p_1p_2\ldots p_l + 1$ لاحظ أن

- ❖ $2p_1p_2\ldots p_l + 1 \equiv 2(-1)^l + 1 \equiv 2(\pm 1) + 1 \equiv 3 \pmod 4$
- ❖ ضرب الأعداد على الصورة $4k+1$ هو أيضا على الصورة $4k+1$.

وبالتالي فالعدد $2p_1p_2\ldots p_l + 1$ لابد له قاسم أولي q على الصورة $4k+3$. من الفرض لابد أن $q = p_i$ ولكن هذا يعني $q \mid 2p_1p_2\ldots p_l + 1$ و $q \mid 2p_1p_2\ldots p_l \Leftarrow q \mid (2p_1p_2\ldots p_l + 1) - (2p_1p_2\ldots p_l)$ أي $q \mid 1$ وهذا مستحيل.

إذا كان $(a, n) = 1$ فمن مبرهنة أويلر $a^{\varphi(n)} \equiv 1 \pmod n$ وقد يتحقق ذلك لقوة أصغر من $\varphi(n)$ وفي جميع الأحوال لدينا التعريف التالي.

رتبة العدد الصحيح قياس n

إذا كان $(a, n) = 1$ فنعرف رتبة a قياس n بالعدد k ونكتب $\mathrm{ord}_n(a) = k$ إذا كان k هو أصغر عدد صحيح موجب يحقق $a^k \equiv 1 \pmod n$.

مثال ١٢ احسب $\mathrm{ord}_{10}(3)$.

الحــل لدينا

$$\begin{aligned} 3^2 &\equiv 9 \pmod{10} \\ 5^2 \equiv 3^3 &\equiv 7 \pmod{10} \\ 3^4 &\equiv 1 \pmod{10} \end{aligned}$$

أي أن $\mathrm{ord}_{10}(3) = 4$.

مبرهنة ٣,٩ (خواص الرتبة) ليكن $n \in \mathbb{Z}^+$ و $a \in \mathbb{Z}$ حيث $(a,n) = 1$.

❶ $a^m \equiv 1 \pmod{n} \Leftrightarrow \mathrm{ord}_n(a) \mid m$.

❷ $\varphi(n) \mid \mathrm{ord}(a)$

❸ $a^r \equiv a^s \pmod{n} \Leftrightarrow r \equiv s \pmod{\mathrm{ord}_n(a)}$

❹ الأعداد $a, a^2, a^3, \ldots, a^{\mathrm{ord}_n(a)}$ غير متطابقة قياس n.

❺ $\mathrm{ord}_n(a^m) = \dfrac{\mathrm{ord}_n(a)}{(m, \mathrm{ord}_n(a))}$.

❻ $\mathrm{ord}_n(a^m) = \mathrm{ord}_n(a) \Leftrightarrow (m, \mathrm{ord}_n(a)) = 1$.

البرهان. ❶ لنفرض أن $a^m \equiv 1 \pmod{n}$، نستخدم خوارزمية القسمة لكتابة

$$m = \mathrm{ord}_n(a) \cdot q + r \quad \text{حيث} \quad 0 \le r < \mathrm{ord}_n(a)$$

نحسب الآن

$$a^m = a^{\mathrm{ord}_n(a) \cdot q + r} = a^{\mathrm{ord}_n(a) \cdot q} \cdot a^r \equiv a^r \pmod{n}$$

لأن $r < \mathrm{ord}_n(a)$ فلابد أن $r = 0$. الاتجاه الآخر واضح.

❷ واضح من ❶.

❸

$$\begin{aligned} & r \equiv s \pmod{\mathrm{ord}(a)} \Leftrightarrow r - s = t \cdot \mathrm{ord}(a) \Leftrightarrow r = s + k \cdot \mathrm{ord}(a) \\ & \Leftrightarrow a^r = a^{s + t \cdot \mathrm{ord}(a)} \equiv a^s \pmod{n} \end{aligned}$$

❹ واضح من ❸.

❺ احسب

$$(a^m)^{\frac{\mathrm{ord}_n(a)}{(m, \mathrm{ord}_n(a))}} = \left(a^{\mathrm{ord}_n(a)}\right)^{\frac{m}{(m, \mathrm{ord}_n(a))}} \equiv 1^{\frac{m}{(m, \mathrm{ord}_n(a))}} \equiv 1 \pmod{n}$$

الآن لنعتبر $(a^m)^t \equiv 1 \pmod{n}$ وبالتالي فإن $\dfrac{\mathrm{ord}_n(a)}{(m, \mathrm{ord}_n(a))} \mid \dfrac{m}{(m, \mathrm{ord}_n(a))} \cdot t \Leftarrow \mathrm{ord}_n(a) \mid mt$ ولكن

$$\left(\frac{\operatorname{ord}(a)}{(m,\operatorname{ord}(a))},\frac{m}{(m,\operatorname{ord}(a))}\right)=1$$

لنستنتج أن $t \mid \frac{\operatorname{ord}_n(a)}{(m,\operatorname{ord}_n(a))}$ ويصبح بالتعريف هو رتبة العدد a^m أي $\operatorname{ord}_n(a^m)$.

❻ واضح من ❺.

مثال١٣ احسب $\operatorname{ord}_{14}(5)$.

الحـــل حيث أن $\varphi(14)=6$ و $\operatorname{ord}_{14}(5)$ هو قاسم لـ $\varphi(14)$ (إما 2 أو 3 أو 6).

$$5^2 \equiv 11 \pmod{14}$$

$$5^3 \equiv 13 \pmod{14}$$

وبالتالي لا داعي لحساب 5^4 أو 5^5 والرتبة: $\operatorname{ord}_{14}(5)=6$.

ندرس الآن إذا كان هناك علاقة بين رتبة ab ورتبة كل من العددين a و b.

مبرهنة٣,١٠ ليكن $(ab,n)=1$. إذا كان $(\operatorname{ord}_n(a),\operatorname{ord}_n(b))=1$ فإن $\operatorname{ord}_n(ab)=\operatorname{ord}_n(a)\cdot\operatorname{ord}_n(b)$.

البرهان. لاحظ أولا أن

$$(ab)^{\operatorname{ord}_n(a)\cdot\operatorname{ord}_n(b)}=a^{\operatorname{ord}_n(a)}\cdot b^{\operatorname{ord}_n(b)}\equiv 1\cdot 1\equiv 1 \pmod n$$

لأن رتبة العدد ab هي $\operatorname{ord}_n(ab)$، من الخاصية الأولى لدينا $\operatorname{ord}_n(ab)\mid\operatorname{ord}_n(a)\cdot\operatorname{ord}_n(b)$. لإثبات المساواة نعرف أولا التطبيق

$$\left\{ab,(ab)^2,(ab)^3,\ldots,(ab)^{\operatorname{ord}_n(ab)}\right\}\longrightarrow\left\{a,a^2,a^3,\ldots,a^{\operatorname{ord}_n(a)}\right\}\times\left\{b,b^2,b^3,\ldots,b^{\operatorname{ord}_n(b)}\right\}$$

$$x\longmapsto\left(x^{\operatorname{ord}_n(b)},x^{\operatorname{ord}_n(a)}\right)\qquad\pmod n$$

يكفي إثبات أن هذا التطبيق غامر:

ليكن $\left(a^i,b^j\right)$ زوجا مرتبا من المجال المقابل، نحتاج لحل النظام

$$x\equiv i\pmod{[\operatorname{ord}_n(a)]}$$

$$x\equiv j\pmod{[\operatorname{ord}_n(b)]}$$

بما أن $(\operatorname{ord}_n(a),\operatorname{ord}_n(b))=1$ فمن الباقي الصينية يوجد حل وحيد $x=k$ قياس $\operatorname{ord}_n(a)\cdot\operatorname{ord}_n(b)$.

من خواص الرتبة لدينا

$$a^k\equiv a^i\pmod n$$

$$b^k\equiv b^j\pmod n$$

من تعريف التطبيق فإن صورة العنصر $(ab)^k$ هي الزوج المرتب $\left(a^i,b^j\right)$. إذن فالتطبيق غامر وبالتالي فعناصر المجال أكثر من المجال المقابل.

مبرهنة١١,٣ ليكن $n \in \mathbb{Z}^+$. إذا وجد عدد $a \in \mathbb{Z}$ بحيث يتحقق

❶ $a^{n-1} \equiv 1 \pmod{n}$.

❷ $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$ لكل عدد أولي p يقسم $n-1$.

فإن n أولي.

البرهان. بما أن $a^{n-1} \equiv 1 \pmod{n}$ فإن $(a,n)=1$. من المبرهنة السابقة $\operatorname{ord}_n(a) \mid n-1$ وسنبرهن الآن أن $\operatorname{ord}_n(a) = n-1$. لنفرض لغرض التناقض أن $\operatorname{ord}_n(a) \neq n-1$، من $\operatorname{ord}_n(a) \mid n-1$ فهذا يعني وجود عدد $x > 1$ حيث

$$n-1 = x \cdot \operatorname{ord}_n(a)$$

إذا كان q قاسما أوليا لـ x نجد أن

$$a^{\frac{n-1}{q}} = a^{\frac{x \cdot \operatorname{ord}_n(a)}{q}} = \left(a^{\operatorname{ord}_n(a)}\right)^{\frac{x}{q}} \equiv 1 \pmod{n}$$

وذلك يتناقض مع الفقرة الثانية من الفرضيات.

ملاحظة:

تسمى المبرهنة السابقة باختبار لوكا والجدير بالذكر أنه غير مجد في الحسابات العادية فهو يتطلب تحليل العدد $n-1$ وهذا في الحالة العامة ليس بأقل سوء من تحليل n. تظهر فائدة هذا الاختبار عند دراسة أعداد بصيغ معينة كأعداد فيرما ومرسين وفيما يلي مثال على ذلك.

مثال١٤ أثبت أن العدد $F_3 = 2^{2^3}+1 = 257$ هو عدد أولي.

الحل لاحظ أن $F_3 - 1 = 2^{2^3}$ سهل التحليل حيث لا يوجد سوى القاسم الأولي 2. نختبر باستخدام $a = 3$.