$n = \prod_k p_k^{\alpha_k}$ ← $n \in \mathbb{N}^*$ ليكن نتيجة

$$\varphi(n) = \prod \varphi(p_k^{\alpha_k})$$

$$n = 50 = 5^2 \times 2$$

$$\varphi(50) = \varphi(5^2) \cdot \varphi(2)$$

ضربي لكن ليس ضربي تام لأن $\varphi(5^2)$ ويمكن تبسيطه أكثر.

12 م 2016/5/4

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = n$$

وإذا كان $n = 7$ عدد أولي فإن.

$$|\mathbb{Z}/n\mathbb{Z}| = n - 1$$

برهنة: ليكن n عدد صحيح موجب، $a \in \mathbb{Z}$ حيث $\gcd(n, a) = 1$

عندها $a^{\varphi(n)} \equiv 1 \pmod n$

تمرين: أوجد باقي القسمة:

$n \in \mathbb{Z}^*$ على 91 حيث 10^{72n^2+3}

أعداد أولية ← بالتحليل

$$\varphi(91) = \varphi(13 \times 7) = \varphi(13)\,\varphi(7) = 12 \times 6 = 72$$

$$10^{\varphi(91)} \equiv 1 \pmod{91}$$

91 ← $10^{72} \equiv 1 \pmod{91}$

$$\Rightarrow (10^{72})^{n^2} \equiv 1 \pmod{91}$$

$$10^{72n^2+3} = 10^{72n^2} \times 10^3 \equiv 1 \cdot 90 \pmod{91}$$

10^{72n^2} ← باقي قسمة على 91 يساوي 1

10^3 ← $10^3 = 91 \times 10 + 90$ ← باقي قسمة على 91

$$\equiv 90 \pmod{91}$$

وظيفة: أوجد باقي قسمة 3^{100000} على 35

$\varphi(35) = \varphi(5 \cdot 7) = \varphi(5)\varphi(7) = 4 \cdot 6 = 24$

$3^{100000} = 3^{24 \times 4166 + 16}$ نقسم 100000 على 24 فيكون

$3^{100000} = (3^{24})^{4166} \times (3)^{16}$

حسب مبرهنة أويلر: $3^{24} = 3^{\varphi(35)} \equiv 1 \pmod{35}$

$(3^{24})^{4166} \equiv 1 \pmod{35}$

باقي قسمة 3^{16} على 35:

$3^{100000} \equiv 1 \times 3^{16} \pmod{35} \equiv 11 \pmod{35}$

ملاحظة: باقي قسمة x على 5 هي $r \in \{0,1,2,3,4\}$

باقي قسمة x^2 على 5 هي $r \in \{0,1,4,9 \equiv 4,16 \equiv 1\}$

تعريف: تابع مجموع قواسم عدد وليكن σ وتابع عدد قواسم عدد وليكن τ

$\sigma(n)$: مجموع قواسم العدد n.

$\tau(n)$ عدد " " n.

$\sigma(n) = \sum_{d \mid n} d$ ، $\tau(n) = \sum_{d \mid n} 1$

n	1	2	3	4	5	...
$\sigma(n)$	1	3	4	7	6	
$\tau(n)$	1	2	2	3	2	

1 قاسم وحيد

2 قاسم 1 و 2

3 قاسم 1 و 3

4 قاسم 1 و 2 و 4

5 قاسم 1 و 5

برهنة: بما أن σ و τ توابع ضربية

بفرض: $n \in \mathbb{N}$ حلل إلى عواملة الأولية

$$n = \prod_k p_k^{n_k}$$

$$\sigma(n) = \prod_k \sigma(p_k^{n_k})$$

$$\sigma(n) = \prod_k \frac{p_k^{n_k+1} - 1}{p_k - 1}$$

$$\tau(n) = \prod_k \tau(p_k^{n_k})$$

$$\tau(n) = \prod_k (n_k + 1)$$

مثال تطبيقي:

$$6 = 2 \times 3 = p_1^1 \times p_2^1$$

$$\sigma(6) = \frac{2^{1+1} - 1}{2 - 1} \times \frac{2^{2+1} - 1}{3 - 1}$$

$$= \frac{2^2 - 1}{1} \times \frac{7^3 - 1}{2} = \frac{3}{1} \times \frac{8}{2} = 3 \times 4 = 12$$

$$\sigma(49) = \sigma(7^2) = \frac{7^{2+1} - 1}{7 - 1} = \frac{7^3 - 1}{6}$$

$$= 57$$

تعريف: نقول $n \in \mathbb{Z}$ $n > 1$ أنه طالي التربيع إذا لم يكن له قاسم تربيع (لم يكن له قاسم مغايرة 1 أكبر من 1)

مثال: $n = 6$ طالي التربيع ($6 = 2 \times 3$)

$n = 4 = 2^2$) ليس خالي تربيع $n = 4$

$n = 4 \times 2 = 2^2 \times 2$) ~ ~ ~ $n = 8$

تابع Mobius:

$$\mu : \mathbb{N} \longrightarrow \{0, 1, -1\}$$

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{إذا كان ليس خالي من تربيع} \\ (-1)^r & n = p_1 p_2 \cdots p_r \end{cases}$$

حيث p_i أعداد أولية متمايزة. 3 × 2 عددين

مثال:

$\mu(6) = (-1)^2 = 1$

$\mu(49) = 0$

ليس خالي من تربيع.

برهنة: ليكن $1 < n \in \mathbb{Z}$ فإن

$$\sum_{d|n} \mu(d) = 0$$

مثال: بين أن $\sum_{d|n} \mu(d) = 0$ من أجل $n = 12$.

قواسم $n = 12$

$$\sum \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)$$

$$= 1 + (-1)^1 + (-1)^1 + 0 + (-1)^2 + 0$$

$$= 0$$

الأعداد من الشكل: $\underbrace{111\ldots1}_{n\ \text{مرة}}$

$= 1 + 10 + 100 + \cdots + 10^{n-1}$

نعوض من الشكل:

$1 + x + x^2 + \cdots + x^m = \dfrac{x^{m+1}-1}{x-1}$ $(m = (n-1)+1 = n)$

فإن: $\underbrace{111\ldots1}_{n\ \text{مرة}} = \dfrac{10^n - 1}{9}$

حالة خاصة: في حال $n = \alpha k$ يمكن أن نكتب

$\underbrace{111\ldots1}_{n=\alpha k\ \text{مرة}} = \underbrace{11\ldots1}_{\alpha\ \text{مرة}} \times \underbrace{1\,00\ldots0\,1\,00\ldots0\ldots}$ ($\alpha - 1$ مرة)

$\underbrace{100\ldots0\ (1)}$ $k-1$ مرة.

مثال: $\underbrace{111111}_{6\ \text{مرات}} = \underbrace{111}_{\alpha=3\ \text{مرة}} \times 1\underbrace{00}1$

$6 = 3 \times 2$ مرات (α, k)

$\alpha - 1 = 3 - 1 = 2$ مرة

مكرر $k - 1 = 2 - 1 = 1$ مرة.

$\underbrace{111111}_{6 = 3\times 2\ \text{مرات}} = \underbrace{11}_{\alpha = 2\ \text{مرة}} \times 1\underbrace{0}1\underbrace{0}1$ ($k = 3$, $\alpha = 2$)

$\alpha - 1 = 2 - 1 = 1$ مرة

$2 = 3 - 1 = k - 1$ مرة

مسألة: إذا كان $\underbrace{1\_\_\_111}_{3 \text{ مرة } t}$ أولي ⟸ t أولي
العكس غير صحيح.

الإثبات: يجب إثبات أن t أولي.
نفرض جدلاً أن t ليس أولي فإنه يوجد $n, m > 1$
$t = m.n$

$$\underbrace{1\_\_\_111}_{3 \text{ مرة } t} = \underbrace{1\_\_\_111}_{3 \text{ مرة } m} \times \underbrace{1\_\_\_1001\_\_\_001}_{3 \text{ مرة } m-1}$$

كتب العدد كجداء عددين وهذا تناقض ⟸ t أولي.

مثال عن العكس
$111 = 3 \times 37$ (3 مرات)
3 عدد أولي ولكن 111 غير أولي.

أمكن تقسيم 111 على 3 لكن ليس دائماً

مسألة: هل $\underbrace{1\_\_\_11}_{81 \text{ مرة}}$ يقبل القسمة على 81؟
$81 = 9 \times 9$

$$\underbrace{1\_\_\_11}_{81 \text{ مرة}} = \underbrace{1\_\_\_11}_{9 \text{ مرات}} \times \underbrace{1\_\_\_01\_\_\_01\_\_\_001}_{8 \text{ مرات}}$$

مجموع خاناته = 9 يقبل القسمة على 9

مجموع خاناته 9 يقبل القسمة على 9.

ومنه $\underbrace{1\_\_\_11}_{81 \text{ مرة}}$ يقبل القسمة على 81.

1111 لا يقبل القسمة على 4

Scanned by CamScanner

مسألة: برهن أن $\underbrace{1\ldots11}_{n \text{ مرة}}$ يقبل القسمة على 41 إذا وفقط إذا كان n يقبل القسمة على 5.

لدينا $n=5k+r$ حيث $r\in\{0,1,2,3,4\}$

$$\underbrace{1\ldots111}_{n \text{ مرة}} = \underbrace{1\ldots11}_{5k \text{ مرة}}\underbrace{0\ldots00}_{r \text{ مرة}} + \underbrace{1\ldots11}_{r \text{ مرة}}$$

$$111 = 100 + 11$$

$$\underbrace{1\ldots111}_{5k \text{ مرة}} = \underbrace{11111}_{5 \text{ مرة}} \times 1\underbrace{0000}_{5-1=4 \text{ مرة}}1\ldots\underbrace{10000}_{5k-1 \text{ مرة}}1$$

$$11111 = 41 \times 271$$

وعليه فالعدد $\underbrace{1\ldots11}_{5k \text{ مرة}}$ يقبل القسمة على 41

وبالتالي العدد $\underbrace{1\ldots11}_{r \text{ مرة}}$ يجب أن يقبل القسمة على 41

لكن في حال $r=1,2,3,4$ لا يتحقق هذا الشرط ومنه $r=0$

وبالتالي العدد $\underbrace{1\ldots11}_{n \text{ مرة}}$ يقبل القسمة على 41.

العكس: n يقبل قسمة على 5 وبالتالي $n=5k$ نبرهن أن $\underbrace{1\ldots11}_{n \text{ مرة}}$ يقبل القسمة على 41.

تمرين: بين أن الأعداد: $\frac{1078111}{3}$ ، $\frac{1107788111}{3}$

$x \in \mathbb{Z}$ حيث x^3 ، $\frac{1111077788811111}{3}$

هي مكعبات من أعداد صحيحة

$\underbrace{11\ldots1}_{\text{n مرة}}0\underbrace{77\ldots7}_{\text{n مرة}}\underbrace{88\ldots8}_{\text{n مرة}}\underbrace{11\ldots1}_{\text{n+1 مرة}}$

سنستخدم الخاصة الآتية

$$\underbrace{111\ldots1}_{\text{n مرة}} = \frac{10^n - 1}{9}$$

تمرين: برهن أن:

$$\underbrace{11\ldots1}_{\text{2n مرة}} - \underbrace{2.2\ldots2}_{\text{n مرة}} + (3-3)^2$$

14 - م 2016/5/11

برهنة:

برهنة Wilson: إذا كان p عدد أولي فإن:

$$(p-1)! \equiv -1 \pmod{p}$$

$$\frac{10!}{(11-1)!} \equiv 1 \pmod{11}$$

برهنة: إذا كان $(n-1)! \equiv -1 \pmod{n} \Leftarrow n$ أولي.

نتيجة: إذا كان p أولي فردي فإن:

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 = (-1)(-1)^{\frac{p-1}{2}} \pmod{p}$$

$$\left(\left(\frac{7-1}{2}\right)!\right)^2 \equiv (-1)(-1)^{\frac{7-1}{2}} \pmod{7}$$

$$(3!)^2 = +1 \pmod{7}$$

برهنة: Fermatlittle:

إذا كان p أولي و a عدد صحيح موجب: و a لا يقسم p فإن

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

قد يأتي الامتحان ذكر نص برهنة ما وقد يأتي على تمرين الاستعانة بالبرهنة

مبرهنة: إذا كان p عدد أولي عندها $(Z/pZ)^*$ زمرة دارية من المرتبة p-1 أي يوجد g بحيث:

$$(Z/pZ)^* = \langle g \rangle$$

مثال $(Z/19Z)^* = \langle [13] \rangle$

المعادلة من الشكل $x^2 \equiv a \pmod p$ (p أولي):

تعريف: البواقي التربيعي $\pmod p$: هو عدد صحيح a بحيث $x^2 \equiv a \pmod p$ حل لها و $p \nmid a$.

تعريف رمز Legendre ليجاندر: يرمز له بـ $\left(\frac{a}{p}\right)$ بشرط $p \nmid a$ و p عدد أولي فردي.

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a,\ x^2 \equiv a \pmod p \text{ حل لها} \\ -1 & p \nmid a \text{ ليس لها حل} \end{cases}$$

رمز مجرد

مبرهنة: إن العلاقات التالية صحيحة: (ليس بالضرورة أن يكون a أولي)

1) إذا كان $a \equiv b \pmod p$ فإن $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

2) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$

نكمل

مثلا لو لدينا معادلة من الشكل:

$$f(x) \equiv 0 \pmod{n}$$

$n = p_1 \times p_2 \times p_3$ عواملها أولية. ثم نحل كل واحدة على حدة

$$f(x) \equiv 0 \pmod{p_1} \Rightarrow x \equiv \text{الحل} \pmod{p_1}$$

$$f(x) \equiv 0 \pmod{p_2} \xRightarrow{\text{مرفوع}} f(x) \equiv 0 \pmod{p_2^2} \rightarrow x \equiv \text{الحل} \pmod{p_2}$$

$$f(x) \equiv 0 \pmod{p_3} \Rightarrow x \equiv \text{الحل} \pmod{p_3}$$

لكن في المحاضرة هذه سنأخذ دوال تربيعية.

سنحصل على 3 معادلات من شكل خطي نحل ① و ② ثم نحل مع ③

4) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

مبرهنة:

1) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \mp 1 \pmod{8} \\ -1 & p \equiv \mp 3 \pmod{8} \end{cases}$

2) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = \begin{cases} 1 & p \equiv 1 \pmod{4} \text{ أو } q \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \text{ و } q \equiv 3 \pmod{4} \end{cases}$

تمرين:

هل $x^2 \equiv 44 \pmod{47}$ لها حل ولماذا؟

$$\left(\frac{a}{n}\right) = \left(\frac{44}{47}\right) = \left(\frac{4\times 11}{47}\right) \overset{\text{ص ب ٤}}{=} \left(\frac{4}{47}\right)\left(\frac{11}{47}\right)$$

$$= \left(\frac{2}{47}\right)\left(\frac{2}{47}\right)\left(\frac{11}{47}\right)$$

أي ١- أو ١ وبالتالي ضربهما ١

$$= \left(\frac{11}{47}\right)$$

باستخدام ٢

$$\left(\frac{11}{47}\right)\left(\frac{47}{11}\right) = (-1)^{\left(\frac{11-1}{2}\right)\left(\frac{47-1}{2}\right)} = -1$$

$$\Rightarrow \left(\frac{11}{47}\right) = -1\left(\frac{47}{11}\right)$$

$$= -1\left(\frac{47}{11}\right)$$

ص ب (١) باقي قسمة 47 على 11 هو 3 أي

$47 \equiv 3 \pmod{11}$

$$= -1\left(\frac{3}{11}\right)$$

ص ب ٢

$$= \underbrace{(-1)(-1)}_{(1)} \cdot \left(\frac{11}{3}\right)$$

ص ب (١) باقي قسمة 11 على 3 هي 2

$11 \equiv 2 \pmod{3}$

$$= \left(\frac{2}{3}\right)$$

ص ب ١١

$$= (-1)^{\frac{3^2-1}{8}} = -1$$

بما أن $\left(\frac{44}{47}\right) = -1$ فإن ليس للمعادلة حل.

أوجد: لكل p عدد أولي أوجد:

$$\left(\frac{-2143018}{p}\right) \text{ حيث } = \left(\frac{-1 \times 2 \times 101 \times (103)^2}{p}\right)$$

حسب (4)

$$= \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{101}{p}\right) \times \left(\frac{103}{p}\right)^2$$

حسب (3) — حسب (2) — كونه تربيع ← نوعا 1- أو 1 يرجع جوابها 1

لنسبة من أجل $p = 7$ حسب (1)

$$= (-1)^{\frac{7-1}{2}} (-1)^{\frac{7^2-1}{8}} \left(\frac{101}{7}\right)$$

$$= (-1)\left(\frac{3}{7}\right) \quad \text{حسب (2)}$$

$$= (-1)(-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}} \left(\frac{7}{3}\right)$$

$$= \frac{7}{3} \quad \text{حسب (1)} \quad \frac{1}{3} = +1$$

لا يوجد حلول بر هنه بتساوي 1

حسب تعريف لوجاندر،

$$x^2 \equiv 1 \pmod 3$$

بالتجريب فقط نجد حلول

حلولها $[1]$ و $[2]$