# نظرية الأعداد

أحمد رامي رحمة وسامي رحمة

# المحتويات

# مقدمة في نظرية الأعداد

أهم مصطلح في نظرية الأعداد هو **قابلية القسمة** ويلفظ "يقسم" ورمزه $a|b$.

ومعناها أن $a$ يقسم $b$ أي أن $\frac{b}{a}$ يساوي عدد صحيح $k$.

وبمعنى آخر: يوجد عدد صحيح $k$ بحيث $b = ka$.

**بعض الامثلة والقواعد البسيطة في الامثلة:**

- يمكن اختصار عدد من الطرفيين مثلا $5|15$ **لو اختصرنا على 5 ستبقى محققة** $1|3$ (بالطبع لأنه بالنهاية يمكن تحويله لكسر).
- وايضا $3| -9$ تكافئ $3|9$ (لأن خارج القسمة سيبقى عدداً صحيحاً).
- وايضا $3|9$ تكافئ $3|9 \cdot n$ أي لو ضربنا القسم اليمين (البسط) بأي عدد سيبقى ناتج الكسر صحيحاً وهذه خاصية جميلة وبسيطة للاستخدام.
- وايضا $2|10-$ تكافئ $2|10$ (لأن خارج القسمة سيبقى عدداً صحيحاً).

**الخاصة الأهم هنا هي:**

إذا كان $a|b$ عندها $a|b - an$ (أي أن طرح **مضاعفات للمقسوم عليه** لا تؤثر على قابلية القسمة)

لأن:

$$\frac{b-an}{a} = \frac{b}{a} - n = \text{عدد صحيح} \quad (\text{حيث } \frac{b}{a} \text{ صحيح حسب } a|b)$$

كيف نستفيد من الخاصة السابقة؟

**فوائد هذه الخاصة:**

فمثلاً لدينا $5|y + 13$ فنستطيع تحسين شكلها ونحولها إلى $5| y + 3$.

طرحنا 10 أو 5 مرتين لأن الشكل الجديد مختزل ومريح.

أو حتى يمكن أن نحولها إلى $5|y - 2$ حيث طرحنا 5 إضافية فحصلنا على سالب 2 وهذه **هامة سنراها فيما بعد** ومريحة ايضة كالـ +3.

**مثال 1:**

أوجد $n \in \mathbb{Z}$ بحيث $n \mid n^2 + n + 1$

**الحل:**

يمكننا أن نطرح أي مضاعف لـ $n$ إذاً $n \mid 1$.

إذاً إما $n = 1$ أو $n = -1$.

((بمعنى آخر عند دراسة القسمة على $n$ نستطيع تجاهل أي حد يحوي $n$ ))

$$n \mid n^5 + 3n^4 + n + 6$$

$$n \mid 6$$

إذاً مجموعة الحلول هي قواسم العدد 6 ولا ننسى القيم السالبة.

**ولكن ماذا لو كان شكل المقسوم ليس بهذه البساطة $n$؟**

**مثال 2:**

أوجد كل الأعداد $n \in \mathbb{Z}$ بحيث:

$$n + 1 \mid n^3 + 2n^2 + 1 + (n + 1)^4 n$$

**الحل:**

نتجاهل أي حد يحوي على $n + 1$.

ومنه

$$n + 1 \mid n^3 + 2n^2 + 1$$

نتبع طريقة " **تخفيض المرتبة** " أيضاً هي بالاستفادة من الخاصية السابقة.

$$n + 1 \mid n^3 + 2n^2 + 1 - n^2(n + 1)$$

لاحظ اخترنا $n^2$ وذلك لنتخلص من $n^3$ (أكبر قوة) ونتابع على هذا المنوال حتى ننتهي من القوى واحدة فالأخرى فهدفنا الوصول إلى عدد ثابت على اليمين (أو أخفض مرتبة ممكن).

$$n+1|\, n^2+1$$

$$n+1|\, n^2+1-n(n+1)$$

$$n+1|1-n$$

هنا يمكن ضرب الطرف اليمين بـ $(-1)$ إذا كانت مريحة أكثر لنا لأن الإشارة في **قابلية القسمة** لا تؤثر على الحلول التي سنحصل عليها.

$$n+1|\, n-1$$

$$n+1|\, n-1-(n+1)$$

$$n+1|-2$$

إذاً مجموعة الحلول هي $n+1$ يساوي أحد قواسم 2 ولا ننسى أن يساوي القيم السالبة.

**تمرين:**

$$n \in \mathbb{Z}$$

$$n+2|n^5+n^3$$

## والآن

ماذا لو كان المقسوم عليه ليس ببساطة $n+1$ أو $n$ ماذا لو كان درجة ثانية مثل

$$n^2+1|n^4+n^3-5$$

$$n^2+1|n^4+n^3-5-n^2(n^2+1)$$

$$n^2+1|n^3-n^2-5$$

$$n^2+1|n^3-n^2-5-n(n^2+1)$$

$$n^2+1|-n^2-n-5$$

$$n^2+1|n^2+n+5$$

$$\Longrightarrow n^2+1|n+4$$

في هذه الحالة لم نصل إلى عدد ثابت لنأخذ قواسمه ولم نعد نستطيع تخفيض الدرجة لأن أي من مضاعفات $n^2+1$ سيكون درجة ثانية على الأقل وهذا لن يزيل الدرجة الأولى.

**إذاً سنلجأ إلى الخاصية التالية:**

إذا كان $a|b$ عندها $|a| \leq |b|$ أو $\boldsymbol{b=0}$

وهي خاصية اساسية جداً في القسمة وبديهية.

**ملاحظة:**

إن $0$ مضاعف لجميع الأعداد وإذا كان $b=0$ لا يتحقق $|a| \leq |b|$ وبالتالي هي حالة صغيرة يتوجب مناقشتها إذاً.

أما سبب القيمة المطلقة لأن $|-14| 7$

وكما قلنا إن الاشارة لا تؤثر في حل قابلية القسمة ولكن تؤثر في المتراجحة لذلك نحاول أن نعرف اشارة المقدار ونحولها لموجب قبل التطبيق ففي **المثال** أعلاه لو فرضنا أن $n$ موجب

إذاً اما $n-1=0$ أي $n=1$

أو $n^2+1 \leq n+4$

هذا المتراجحة تبدو أنها غير منطقية في عالم الأعداد الطبيعية (إذ أن الطرف الأصغر درجة ثانية والطرف الأكبر درجة أولى) فمثل هذه المتراجحة ستتحقق من أجل قيم قليلة فقط لـ $n$

هذا المنطق موجود **في نظرية الأعداد (أي في $\mathbb{Z}$) وليس في $\mathbb{R}$** فالمتراجحة السابقة ستعطي مجالاً يحوي عدد محدوداً من الأعداد الصحيحة (وليس الحقيقية) التي تحققها.

$$n^2+1 \leq n+4$$
$$n^2-n+3 \leq 0 \Leftrightarrow (2n-1)^2+11 \leq 0$$

وهي ليس لها حلول صحيحة.

□

**تمرين:** أوجد $n \in \mathbb{N}$ بحيث

$$n^3 + 2 \mid n^5 + n^4 + 3n + 1$$

**الحل:**

كالعادة نخفض المرتبة حتى تصبح مرتبة اليمين أقل من اليسار (أي لا يمكننا تخفيض المرتبة أكثر).

$$n^3 + 2 \mid 2n^2 - n - 1$$

الآن نبدأ بـ $n$ موجب (وحالة $n$ سالب ليست أصعب) قد يقول قائل: إن $n^3$ في حالة $n$ سالبة ستكون قيمة صغيرة $n^3 + 2$ $n^3 + 2$ عندها يجب تذكر أن ما يهمنا هو **القيمة المطلقة.**

إذاً كيف نتعامل مع حالة $n$ موجب مع أنها متراجحة صعبة في $\mathbb{R}$ ولكن لحسن الحظ في نظرية الأعداد الأمور أسهل وتتبع المنطق.

$$n^3 + 2 \leq 2n^2 - n - 1$$
$$n^3 - 2n^2 + n + 3 \leq 0$$

**حالة $n = 1$**: المتراجحة غير محققة.

**حالة $n = 2$ :** تنتج $5 \leq 0$ غير محققة أيضاً.

**حالة $n = 3$:** أيضاً غير محققة بل إن الفرق في تزايد مستمر.

إذاً يمكننا أن ننهيها بالاستقراء ونثبت أن $n^3 - 2n^2 + n + 3 \geq 0$ عندما $n \geq 3$.

أو **بطرق فنية** بما أن $n \geq 3$

(أي بعد أن أنهينا نقاش حالة 1 و2) في هذه الحالة يكون

$$n^3 - 2n^2 = n^2(n-2) \geq 0$$
$$n^3 - 2n^2 + n + 3 \geq 0$$

أي مجموع عددين موجبين يجب أن يكون موجباً.

□

## أما الآن سنبحث في طرق أسهل وأذكى لتخفيض المرتبة

**أولاً:** لنتعرف على المتطابقة التالية: (المتطابقة الأم)

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 \dots . y^{n-1})$$

حفظها ليس صعباً كما يبدو فلاحظ القوس الثاني يسير وفق نمط تبادل الأسس واحدا واحدا بين الـ $x$ والـ $y$

ماذا عن $x^n + y^n$ ؟

لاستنتاج صيغة متطابقتها نعوض $y$ بـ $-y$ **إذا كان $n$ فردي:**

$$x^n - (-y)^n = (x+y)(x^{n-1} + x^{n-2}(-y) + x^{n-3}(-y)^2 + (-y)^{n-1})$$
$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \dots + y^{n+1})$$

حالة خاصة عندما $y = 1$

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + x^{n-3} \dots . x + 1)$$
$$x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + x^{n-3} \dots . + 1)$$

نستفيد من هذه العلاقات أن:

$$x - y | x^n - y^n$$
$$x + y |\ x^n + y^n \quad n \text{ فردي}$$
$$x - 1 | x^n - 1$$
$$x + 1 | x^n + 1 \quad n \text{ فردي}$$

كيف يمكننا الاستفادة من هذه النظريات.؟! لاحظ كيف سنخفض الدرجة في هذا المثال:

$$n \in \mathbb{Z}$$

$$n - 2 | n^5 + 5n^4 - 3n^3 + n^2 + 2$$
$$n - 2 | \left(\boldsymbol{n^5} - \boldsymbol{2^5} + 2^5\right) + 5(\boldsymbol{n^4} - \boldsymbol{2^4} + 2^4) - 3(\boldsymbol{n^3} - \boldsymbol{2^3} + 2^3) + (\boldsymbol{n^2} - \boldsymbol{2^2} + 2^2) + 2$$

لاحظ انه كل المقادير بالخط العريض يمكن تحليلها والحصول على القوس $n - 2$

$$n - 2 |\ 2^5 + 5 \cdot 2^4 - 3 \cdot 2^3 + 2^2 + 2$$

**مثال:**

$$n \in \mathbb{Z}$$

$$n^3 - 3 \mid n^8 + 3n^7 + n^5 + 6n^4$$

**الحل:**

هنا قد لا نستطيع أن ننزل إلى رقم ثابت ولكن أيضاً يمكننا أن ننزل إلى درجة أقل

$$n^3 - 3 \mid n^2(n^6 - 3^2 + 3^2) + 3n(n^6 - 3^2 + 3^2) + n^2(n^3 - 3 + 3) + 6n(n^3 - 3 + 3)$$
$$n^3 - 3 \mid 12n^2 + 45n$$

هل لاحظت أنه في المثال الأول **وكأننا عوضنا بدل $n$ ب 2** في كل قوة وبالتالي الناتج كان تعويض 2 مكان $n$ في التركيب الجبري على اليمين (وهذه طريقة ستخدمها مستقبلاً في المسائل الصعبة عندما لا يكون لديك الوقت لتجري تخفيض المنزلة).وفي المثال الثاني كاننا عوضنا بدل $x^3$ ب 2

هذه الطريقة التي تختصر الطريق في تخفيض المرتبة ستكون إثبات لخاصة رئيسية من خواص الـ $mod$ سنأخذه قريباً.

الآن مع المزيد من التمارين:

- أوجد جميع $n \in \mathbb{Z}$ بحيث $n + 10 \mid n^3 + 100$
- أثبت أن:

$$2009 \mid 2010^k - 1$$
$$2011 \mid 2010^{2k} - 1$$

- إذا كان $x, y \in \mathbb{Z}$ ، $17 \mid 9x + 5y$ أثبت أن $17 \mid 2x + 3y$ من أجل أي عددين $x, y$ صحيحين.

التمرين الثالث تحدي، إبداع حاول حلها قبل قراءة الحل

**حل التمرين الثالث:** نلاحظ أن 9 لا تتحول لـ 2 بجمع أو طرح $17x$ (مضاعف لـ 17) لذا سيتوجب علينا الضرب بعدد ثم الطرح .... ولكن ماذا عن الـ $y$ ستتعرض ايضاً للضرب ☐

عندما نحصل على أمثل الـ $x$ فسنحصل تلقائياً على الأمثال المطلوبة لـ$y$ (وذلك بحسب المسألة)

ولكن ما هو الرقم الذي سنضرب به الـ 9 .....

بالتفكير نجد أنه الـ 4 ثم نطرح $34x + 17y$ وبالفعل نصل للمطلوب.

**الآن كملخص:**

- تعلمنا كيفية تخفيض المرتبة.
- استخدام متراجحات.
- ومتطابقة للتعامل بسرعة فقط.

**الآن تمارين من طراز جيد:**

- تخلّص من $k$ من الطرف الأيمن حيث $k, s \in \mathbb{Z}$

$$k^2 + 2 \mid (k^2 + s)^2 + 1$$

- أوجد $m, n$ أعداد صحيحة تحقق كل من الشرطيين

$n \mid 2m - 1 \qquad m \mid 2n - 1$ (جملة قسمتين!!)

- أوجد كل $n \in \mathbb{Z}$ بحيث

$$2n + 2 \mid 5n + 3$$

**خذ وقتك في المحاولة قبل القراءة:**

- $k^2 + 2 \mid k^4 + 2k^2s + s^2 + 1$ إما تخفيض المرتبة أو المتطابقة.

$$k^2 + 2 \mid k^4 - 4 + 4 + 25(k^2 + 2 - 2) + s^2 + 1$$
$$k^2 + 2 \mid s^2 - 45 + 5$$

طالما لا يوجد شرط آخر لربط $s$ , $k$ لا يمكننا مواصلة تخفيض المرتبة.

$n|2m-1$ $m|2n-1$ حيث $m,n$ صحيحان موجبان.

**الحل:**

الآن دائماً عند الآنطلاق بعدة علاقات قسمة يجب أن يكون في البال أن الطرف الأيمن دائماً أكبر من اليسار.

وفي العلاقتين السابقتين سيكون كل مجهول مرة في الطرف الأكبر والمرة الأخرى في الطرف الأصغر إذاً لابد هنا من تناقض.

$$2n-1 \geq m \qquad 2m-1 \geq n$$
$$m \geq \frac{n+1}{2}$$
$$2n-1 \geq m \geq \frac{n+1}{2}$$

لكن هذه المتراجحة ممكن أن تتحقق إذاً هاتان المتراجحتان غير كافيتان للحل.
لذلك يجب أن نستخدم المتراجحات بحيث تكون أقوى.

نعود إلى الأصل الذي جاءت منه المتراجحات السابقة (دائماً الإبداع كهذا... لذلك يجب أن نعرف إثبات كل النظريات).

$2m-1=kn$ $k$ صحيح إذاً هو أكبر أو يساوي 1 وهو أيضاً عدد فردي

لذلك قد يكون 3 ولكن في حالة $5 \geq$ لا نجد حلول لأنه عندها تصبح المتراجحتان

$$2n-1 \geq m \qquad 2m-1 \geq 5n$$
$$2n-1 \geq m \geq \frac{5}{2}n+\frac{1}{2}$$ هنا تناقض

إذاً إما واحد أو 3 لكليهما

- $2m-1=3n$ $2n-1=3m$ منقوضة مباشرة
- $2m-1=n$ $2n-1=m$ بالحل $1=m=n$

$2m-1=3n \qquad 2n-1=m$

(5,3) والحل المقابل (3,5)

$$\boldsymbol{2n+2 \mid 2n^2+7n+3}$$
$$2n+2 \mid 2n^2+7n+3-(2n+3)n$$
$$2n+2 \mid 5n+3$$

هنا نريد تخفيض المرتبة ولكن لا يوجد شيء نضربه بـ $2n$ ليصبح $5n$

ماذا سنفعل ..."ما في شي عظيم".

أول فكرة تخطر في بالنا هي أن نضرب الطرف اليمين بـ 2 وهذا ممكن وفق الخاصية:

إذا كان $a|b$ عندها $a|bc$ "**خاصية الضرب**".

أو إذا كان $ab|c$ عندها $a|c$ وهذه معناها منطقي جداً وهو أنّ $c$ حتى تكون مضاعفة لـ$ab$ يجب أن يقبل القسمة على $a$ وحدها حتى يقبل القسمة على لـ$a$ والـ$b$ معاً. "**خاصية الاختزال**"

فلنعد للمسألة:

إما أن نضرب بـ 2

$2n+2 \mid 2(5n+3)$ ثم تختصر 2 مع الـ 2

$n+1 \mid 5n+3$ "حسب الضرب"

أو أن نقول إن شرط المسألة $2(n+1) \mid 5n+3$ يقتضي حتما أنّ $n+1 \mid 5n+3$ "حسب الاختزال"

**لكن هنا ملاحظة أنه عند الضرب أو الاختزال أنت تختزل من شروط المسألة** فمثلاً هنا الحلول $n$ التي تحقق $n+1 \mid 5n+3$ قد لا تحقق
$2(n+1) \mid 5n+3$

لا بد وأن تكون وضحت الفكرة.

لذا ما علينا سوى حل $n+1 \mid 5n+3$ **والتحقق بعدها**

**مثال لك:**

أوجد قيم $n$ الحقيقية التي تحقق $2n+1 \mid 5n+3$

# $(mod)$ Modulo operation

هو مفهوم جديد ندخله إلى نظرية الأعداد يعني **الباقي** (باقي القسمة).

ربما لاحظت خلال حلك للتمارين السابقة في الكتاب بوجود طراز أو نمط يجعل التعامل مع القسمة ونظرية الأعداد بشكل عام أسهل وهذه الأنماط والنظريات تُجمع في مفهوم الـ $mod$.

الشكل العام للعلاقة الـ $mod$ ية هو

$$a \equiv b \ mod \ n$$

وتعني $a$ لها نفس باقي $b$ عند القسمة على $n$

- **الآن الآنتقال من القسمة إلى الـ $mod$**

**إذا كان $b|a$ عندها $b$ باقي قسمته على $a$ هو $0$ وبالتالي $b \equiv 0 \ mod \ a$**

- المقسوم عليه على يمين الـ$mod$ ويبقى ثابتاً غالباً
- **أهم القواعد هي:** إذا كان $a \equiv b \ mod \ n$ عندها $a^k \equiv b^k \ mod \ n$

**الإثبات:**

لابد وكما كل قواعد الـ $mod$ أن يتم استنتاجها من قواعد القسمة بطبيعة الحال.

$$a \equiv b \ mod \ n$$

كالمساواة $a - b \equiv 0 \ mod \ n$

$$n| \ a - b$$

من المتطابقة نجد:

$$\Rightarrow n| \ a^k - b^k$$
$$a^k - b^k \equiv 0 \ mod \ n$$
$$a^k \equiv b^k \ mod \ n$$

■

**الفائدة / المعنى: معناها أنه يمكننا أن نعوض باقي العدد ضمن الأس مهما كبر الأس.**

لنرَ بعض التطبيقات عنها:

ولكن أولاً لننظر لبعض العلاقات الجوهرية.

$$n+2 \equiv -1 \; mod \; n+1$$
$$5(n+1)+3 \equiv 3 \; mod \; n+1$$
$$n \equiv -1 \; mod \; n+1$$

هي العلاقات بديهية يجب ألا تُذكر ولكن ذُكرت هنا لكي تتذكر أن تستخدمها عندما تكون $n$ داخل أس كبير وتتذكر تعويضها مباشرة بـ $-1$ عندما يتم أخذ $mod \; (n+1)$

**تمرين1:**

$$n \in \mathbb{Z}$$
$$n+1 | \; n^3+2n^2+1$$

**الحل:**

$$n^3+2n^2+1 \equiv 0 \; mod \; n+1$$
$$(-1)^3+2(-1)^2+1 \equiv 0 \; mod \; n+1$$
$$2 \equiv 0 \; mod \; n+1$$

إما أن تكتب $n+1 \; | \; 2$ أو نجريها ذهنياً ونستنتج الحلول الـ 4

**تمرين 2:**

$$n \in \mathbb{Z}$$

$$n-2 | \; n^5+5n^4-3n^3+n^2+2$$

**الحل:**

بتطبيق الـ $mod$

$$n-2 | \; 2^5+5 \cdot 2^4-3 \cdot 2^3+2^2+2$$

$$n-2 | 94$$

ومنه

$$n-2 = \{-94,-47,-2,-1,1,2,47,94\}$$

$$n = \{-94,-45,0,1,3,4,49,96\}$$

**تمرين 3:**

$$n \in \mathbb{Z}, \qquad n^2+1 \mid n^4+n^3-5$$

**الحل:**

العلاقة $n^2 \equiv -1 \ mod \ n^2$ في ذهننا

$$\begin{aligned} n^4+n^3-5 &\equiv 0 \ mod \ n^2+1 \\ (-1)^2+n(-1)-5 &\equiv 0 \ mod \ n^2+1 \\ -n-4 &\equiv 0 \ mod \ n^2+1 \end{aligned}$$

بضرب الطرفين بـ $-1$ لا تؤثر وذلك كما القسمة تماماً.

$$n+4 \equiv 0 \ mod \ n^2+1$$

طبعاً العلاقة هنا أيضاً غير قابلة للتبسيط وسنلجأ للتراجح للوصول إلى حلول معدودة لهذا التطابق

القيم التي تحقق المتراجحة هي $\{-1,0,1,2\}$ بالتجريب نجد أنّه قيمة واحدة تحقق القسمة وهي 0

إذاً الحل هو $n=0$.

**تمرين 4:**

$$n \in \mathbb{Z}, \qquad n \mid (n+1)^5+(n+2)^3+1$$

**الحل:**

لا يوجد داعٍ لفك الأقواس وتجاهل كل حد يحوي $n$ كما كنا نفعل سابقاً فبتطبيق قاعدة الـ $mod$:

$$\begin{aligned} n &\mid 1^5+2^3+1 \\ n &\mid 10 \end{aligned}$$

**تمرين 5:**

$$n \in \mathbb{Z}, \qquad n^2+1 \mid n^7+n^3+5$$

**الحل:**

$$n^7+n^3+5 \equiv 0 \ mod \ n^2+1$$

لدينا $n^2 \equiv -1 \ mod \ n^2+1$

$$\rightarrow \text{بالتعويض } (-1)^3 n + (-1)n + 5 \equiv 0 \; mod \; n^2 + 1$$

$$-2n + 5 \equiv 0 \; mod \; n^2$$

**تمرين 6:**

$$n \in \mathbb{Z}$$
$$8n \equiv 16 \; mod \; 2t + 1$$
$$n \equiv \; 2 \; mod \; 2t + 1$$

**الحل:**

لاحظ اننا أكدنا على كون ما داخل الـ $mod$ فردي لنختصر دون تغيير شروط المسألة (التطابق) حسب **الاختزال** ولكن لن نذكر الاختزال بعد الآن فهي سنبدأ بتطبيقها بكل سلاسة

**تمرين 7:**

$$n \in \mathbb{Z}$$
$$4n \equiv 20 \; mod \; 4t + 4$$
$$n \equiv 5 \; mod \; t + 1$$

**الحل:**

هنا لاحظ أنّ ما داخل الـ $mod$ ليس فردي بل فيه 4 وضوحاً، ما فعلناه هو أننا عملياً قسمنا البسط والمقام على 4،فلو شككت بأي خاصية للـ $mod$ خذ الطرف اليمين إلى اليسار بحيث يصبح اليمين 0 ثم حولها إلى قسمة وتأكد هل ما فعلته منطقي

إذاً تقسيم الأرقام الثلاث هو نفس تقسيم البسط والمقام 👌

**تمرين 8:** بمساعدة قواعد الـ $mod$

$$2011 | \; 2010^{2k} - 1$$

لم يعد تمريناً بعد الآن.

## القاسم المشترك الأكبر:

**القاسم المشترك الأكبر للعددين $a, b$ يرمز له $\gcd(a,b)$ أو $(a,b)$. حيث $a, b \in \mathbb{Z}$**

هو أكبر عدد يقسم $a, b$ معاً.

الآن الخاصية الأعم التي تمكننا من التعامل مع القاسم المشترك الأكبر:

$$(a,b) = (a, b-an)$$

حيث $a, b, n \in \mathbb{Z}$

**الإثبات:** إذا كان $d = (a,b)$ فإن $d|a$ و $d|b$

$d|\ b-an$ وأيضاً $d|a$ إذاً $d$ هو قاسم ل $(a, b-an)$

بالعكس أي عدد صحيح $m$

$$m \mid a \quad \text{و} \quad m \mid b-an$$
$$m|\ (n)a + (1)(b-an)$$

بما أن $m$ يقسم أي تركيب خطي لـ $a$ و $b-an$ وهذا يؤدي إلى $m|\ b$

$$m|\ a \ , \ m|\ b$$

إذاً أي عدد يقسم الثنائي $a, b$ معاً يقسم الثنائي $a, b-an$

وبالعكس أي عدد يقسم الثنائي $a, b-an$ يقسم الثنائي $a, b$ إذاً $(a,b) = (a, b-an)$.

**ملاحظة:** لو لم نثبت العكس كان

$$(a,b)|(a, b-an)$$

فكل عامل موجود في الثنائي $a, b$ موجود في الثنائي $a, b-an$ ولكن الثنائي $a, b-an$ قد يحوي عوامل أكثر. فيجب علينا إثبات العكس أيضاً.

## التطبيق العملي:

$$(a, b) = (a, b - an)$$

**في كل خطوة أحد الأطراف يبقى ثابتاً** أما الطرف الآخر نطبق عليه خاصة القسمة نفسها تماماً لذلك يمكننا تطبيق ما نشاء وبالتالي نذهب إلى أفضل طريقة وهي الـ $mod$.

**مثال:**

$$\boldsymbol{n} \in \mathbb{Z}$$

$$(n^3 + n^2 + 1, n) = (1, n) = 1$$

$$(n^3 + 2n^2 + 1, n + 1) = (2, n + 1)$$

هذا أبسط شكل للقاسم المشترك الأكبر (حيث أحد طرفيه على الأقل عدد ثابت).

القاسم المشترك الأكبر هنا يمكن أن يكون أي من قواسم الـ 2 أي 2 أو 1 وذلك حسب $n + 1$ فإذا كان فيها 2 (أي $n + 1$ زوجي) يكون القاسم المشترك الأكبر 2.

إذا لم يكن فيها 2 يكون عندها الـ ق.م.أ (القاسم المشترك الأكبر) 1.

**مثال أصعب:**

$$\boldsymbol{n} \in \mathbb{Z}$$

$$(n^4 + n^3 + n + 1, n^2 + 2)$$
$$= ((-2)^2 - 2n + n + 1, n^2 + 2)$$

لاحظ أننا ثبتنا الطرف الأيمن وطبقنا $mod\ n^2 + 1$ على الطرف الأيسر.

$$= (5 - n, n^2 + 2)$$
$$= (n - 5, n^2 + 2)$$

وهنا بالعكس نثبت الطرف الأيسر ونطبق مودّه على الطرف الأيمن.

$$= (n - 5, 27)$$

أيضاً إما $1, 3, 9, 27$

**أوجد القيم الممكنة لـ**$(n^4 + 3, n^2 + 5n + 1)$ حيث $\boldsymbol{n} \in \mathbb{Z}$

**والآن النظرية الواضحة التالية:**

إذا كان $a|bc$ وكان $(a,c)=1 \Leftarrow a|b$

معناها واضح بأنه إذا $c$ ليس لديه أي عامل مشترك مع $a$ يمكن لـ $b$ الاستغناء عنه (وهذه الخاصية ليس لها علاقة **بخاصية الاختزال** الأكثر وضوحاً من هذه) (والتي يتم الاختزال فيها من البسط والمقام -القاسم والمقسوم- أما هنا الاختزال من البسط وتحت شرط).

لذلك إذا كان لدينا $a|b$ يمكننا أن نضرب بـ $c$ أولي مع $a$ دون أن نغير أي شيء في المسألة وبعد أن نخرج الحلول **لا يوجد داعي لأن نتحقق** منها وذلك لأن هذا العدد يمكننا أن نستغني عنه كما في الخاصّة السابقة.

$$2n-1|\ 5n+3 \quad (2n-1 \text{ أولي مع } 2 \text{ الـ})$$
$$2n-1|\ 2\cdot(5n+3)$$
$$2n-1|\ 10n+6$$
$$2n-1|\ 11$$

أو باعتبار تعرفنا على الـ $\boldsymbol{mod}$ فلابد أن يخطر لك وجود طريقة أسهل لحل هكذا تمارين...وبالفعل طريقة نسترقها مما سنتعلمه قريبا:

$$n \equiv \frac{1}{2}\ mod\ 2n-1 \quad \text{لدينا}$$
$$5n+3 \equiv 0\ mod\ 2n-1$$
$$\frac{5}{2}+3\ \equiv 0\ mod\ 2n-1$$
$$\frac{11}{2} \equiv 0\ mod\ 2n-1$$

أيضاً ممكن هنا أن نضرب بـ 2 بسبب النظرية في الأعلى

$$11 \equiv 0\ mod\ \ 2n-1$$

**تمرين:**

$$k \in \mathbb{Z} \text{ حيث } (6k+5,7k+6)$$

$7k+6$ أولي مع الـ7 لذلك

$$=(7\cdot(6k+5),7k+6)$$

$$= (42k + 35{,}7k + 6)$$
$$= (-1, 7k + 6)$$
$$= 1$$

طبعنا حللنا بهذه الطريقة فقط لنستخدم النظرية بينما هنالك طريقة البسيطة ذاتها دون استخدام أي نظرية وهو أنّ نطرح اليسار من اليمين فيبقى $k + 1$ ونتابع بسهولة.

أو نعوض $k = \frac{-6}{7}$ في $6k + 5$ ونثبت $7k + 6$ كما نفعل في تطبيق الـ $mod$ في إيجاد القاسم المشترك الأكبر.

الآن أحد **الحركات** المنطقية والتي يمكن أن يؤديها محترف نظرية الأعداد.

$$d = \left(n^4 - n^3 + n + 1\ , n(n+1)\right)$$

يمكننا أن نلاحظ أن $n$ أولية مع اليسار مباشرة (فقط إذا كانت أولية ممكن زوالها ...فلو وجدت إمكانية وجود 2 كقاسم مشترك بين الـ $n$ والحد الأيسر ما استطعنا تعويضها بـ 2 ...لأن قيمة $n + 1$ هي من تحدد إذا القاسم المشترك بينهما هو 1 أو 2.

**ملاحظة:** عندها نتعامل مع المسألة بشكل عادي كأنها درجة ثانية مقابل رابعة:

$$\Rightarrow d = (n^4 - n^3 + n + 1\ , n + 1)$$

ثم بتطبيق الـ $mod$ فوراً.

$$d = (2, n + 1)$$

لو حُلّت بالطريقة التقليدية لاستغرقت وقتاً أطول.

$$n^2 \equiv -n\ mod\ n^2 + n \quad \text{لدينا}$$

$$(n^4 - n^3 + n + 1, n^2 + n)$$
$$= (-n^3 + n^2 + n + 1, n^2 + n)$$
$$= (+n^2 - n + n + 1, n^2 + n)$$
$$= (1 - n\ , n^2 + n)$$
$$= (1 - n\ , 1^2 + 1)$$
$$= (n - 1, 2)$$

**لقد** أزلنا الـ $n$ في التمرين أعلاه لأنها أولية مع الطرف الأيسر أما إذا كانت موجودة في **كلا الطرفيين** نخرجها من الطرفيين عاملاً مشتركاً وبالتالي ستدخل في القيمة النهائية ل ق.م.أ دائماً.

**كمثال:**

$$n \in \mathbb{Z}$$

$$(n^4 - n^3 + n, n^2 + n)$$

$$= n \cdot (n^3 - n^2 + 1, n + 1)$$

$$= n \cdot (-1^3 - (-1)^2 + 1, n + 1)$$

$$= n \cdot (1, n + 1) = n$$

**ملخص:**

$$a|b \Rightarrow a|b - an$$
$$|a| \leq |b|$$

الـ $mod$ ونظريات ثانوية (غير هامة) (أو هامة للكماليات فقط – متى أستطيع أن أضرب أو أقسم معادلة بالـ $mod$ )

$$\begin{cases} a|bc \Leftarrow a|b & (1) \\ a|b \Leftarrow ac|b & (2) \end{cases}$$

$$a|b \Leftarrow a|bc \quad (a,c) = 1 \quad (3)$$

$$a|bc \Leftarrow a|b \, , (a,c) = 1 \quad (4)$$ وهي لا تقلل شروط المسألة هذا فرق الوحيد عن (1)

(أي لا نحتاج إلى التحقق بعدها)

ماذا لو قمنا ببعض التمارين الرقمية عما تعلمناه هل يا ترى أضعنا التعريف والإحساس بمعنى الـ ق.م.أ من هذه النظريات ...لا طبعاً.

**مثال ١:** أوجد $(6,6k + 5)$

**الحل:**

بالفعل يمكن طرح مضاعفات الـ 6 من الطرف الأيمن ولكن من الأفضل ملاحظة أن باقي قسمة $6k + 5$ على 6 هو 5 أي غير مضاعفة لـ 6 وبالتالي الـ ق.م.أ =1

$$X = (12k + 9,120)$$

أولاً نخرج 3 مباشرة عاملاً مشتركاً

$3 \cdot (4k + 3,40)$ طبعاً نلاحظ أنّ 4 أولية مع اليسار فنزيلها من اليمين.

$3 \cdot (4k + 3,10)$ الـ 2 أيضاً أولية مع $4k + 3$ لذلك تزال.

$3 \cdot (4k + 3,5)$ الطرف الأيسر ليس لديه أي مشكلة مع الـ 5 حيث أمثال $k$ لا تحد الـ 5 وسنفهم هذا الأمر بتفصيل رائع قريباً.

إذاً ممكن أن يحوي القاسم المشترك الأكبر على 5 أو لا يحويها إذاً ق.م.أ إما 3 أو 15.

**أما الآن نظرية هامة تقول:**

$$\boldsymbol{a, b, c} \in \mathbb{Z}$$

$$lcm\ (a, b) | c \Leftarrow \text{عندها } b|c\ ،\ a|c \text{ إذا كان}$$

**هذه النظرية مميزة إذ تحول معادلتي قسمة إلى واحدة شرط أن يكون البسط (المقسوم) ذاته.**

**الإثبات:** إذا كان $d = gcd(a, b)$ عندها يمكن أن نكتب

$$lcm\ (a, b) = \frac{ab}{gcd(a, b)} \quad b = b_1 d \quad a = a_1 d$$

حيث: $(a_1, b_1) = 1$

إذاً لدينا $b_1 d | c\ ,\ a_1 d | c$

إذاً $a_1, b_1$ مختلفان تماماً لا يوجد أي عامل مشترك بينهما لذلك كلاهما يجب أن يكون في $c$ ولكن $d$ مشترك بينهما لا يجب أن يتكرر أو ليس من الضرورة أن يتكرر في $c$

إذاً $a_1 b_1 d | c$

$$lcm(a, b) | c$$

**حالة خاصة:**

إذا كان $(a, b) = 1$ عندها $lcm\ (a, b) = ab$

لذا إذا كان $a|c \quad b|c \quad (a, b) = 1 \Leftarrow ab|c$

**تمرين 1:** حل جملة المعادلتين:

$$n+2009 \mid n^2+2009 \qquad n+2008 \mid n^2+2008$$

**الحل:**

من الواضح أنها ليست بالمتراجحات وهي بمجهول واحد إذاً هي سهلة يمكن أن نبسطه كل واحدة ونقاطع بين حلولها:

$$n+2009 \mid 2009^2+2009 \qquad n+2008 \mid 2008^2+2008$$
$$n+2009 \mid 2009 \cdot 2010 \qquad n+2008 \mid 2008 \cdot 2009$$

نجرب الحالات (قاسمين متتاليين لـ $2018 \cdot 2019$ ونجد الحلول $n=0 \quad n=1$.

أو يوجد طريقة أسهل إن خطرت بالبال واستشعرت النمط المشترك في المعادلتين:

$$n+2009 \mid n^2+2009 \qquad n+2008 \mid n^2+2008$$
$$n+2009 \mid n^2-n \qquad n+2008 \mid n^2-n$$

$$(n+2009, n+2008)=1$$
$$(n+2008)(n+2009) \mid n^2-n$$

نلاحظ أن اليسار أكبر من اليمين إذاً

$$n^2-n=0$$

■

**ملاحظة:**

إذا كنا نريد إثبات $ab \mid c$ حيث $(a,b)=1$ عندها يجب أن نثبت أنّ $a \mid c$ , $b \mid c$ وإذا تحقق الشرطان يتحقق المطلوب مباشرةً أي هذان الشرطان **يكافئان** الشرط الأساسي بالضبط (**قاعدة التجزئة**).

نتساءل لماذا قد نقوم بتحويل شرط واحد إلى شرطين؟!

**الإجابة:** هو أن هذه الطريقة هي الأفضل في تمارين **إثبات** القسمة، وتمارين إثبات القسمة عادةً تأتي **والمقسوم عليه رقم** حيث نعلم عوامله الأولية ونحولها إلى قسمة على ارقام صغيرة أولية.

**تمارين على الأرقام لتعلم طرق التعامل معها**

**التمرين 2:**

$$n \in \mathbb{Z}$$

أثبت أن:

$$14 \mid 3^{4n+2} + 5^{2n+1}$$

**الحل:**

أولاً العدد $3^{4n+2} + 5^{2n+1}$ زوجي وضوحاً إذاً ننتهي من حالة الـ 2 إذاً بقي:

$$7 \mid 3^{4n+2} + 5^{2n+1}$$

الآن صغر الرقم لذا أصبح التعامل أسهل:

$$3^{4n+2} + 5^{2n+1} \equiv 9^{2n+1} + 5^{2n+1} \equiv 0 \ mod\ 7$$

ربما لم نستفد منها هنا ولكن علينا أن نعرف أنه بإمكاننا أن نفصل في العمل بين $mod$(أي أنّ مود الـ 2 منفصل عن مود الـ 7).

**تمرين 3**

اذا كان لدينا $35 \mid 12^n + 10^{2n+1} + 1$

اثبت ان

$$5 \mid 2^n + 1$$

الحل :

من العلاقة المعطاة نجد على الطرف الايسر ان $35 = 5 * 7$ وبالتالي سننظر الى هذه العلاقة على انها قسمة على 7 وقسمة على 5

ناخذ منها فقط شرط القسمة على 5 لنر كيف يتصرف المقدار الايمن في شرط قسمة ال5

$$5 \mid 12^n + 10^{2n+1} + 1$$

نختصر ال $10^{2n+1}$ لانها مضاعفة ل 5 وال $12$ ببساطة نعوضها 2

.

**تمرين 5: أثبت** أنّ:

$$n \in \mathbb{Z}$$

$$9|n^3 + (n+1)^3 + (n+2)^3$$

**الحل:**

هنا لا يمكننا الاستفادة من القانون السابق

$$n^3 + (n+1)^3 + (n+2)^3$$

$$= 3n^3 + 9n^2 + 15n + 9$$

$$= 3(n^3 + 3n^2 + 5n + 3)$$

إذاً كل ما علينا إثبات أن

$$3|n^3 + 3n^2 + 5n + 3$$

$$3|n^3 + 5n$$

لو كنا نعرف فيرما $a^p \equiv a \ mod \ p$ حيث $p$ أولي لكان $n^3 + 5n \equiv n + 5n \equiv 0 \ mod \ 3$.

■

لو لم نكن نعرفها، $3|n^3 + 5n$ وكنا نعرف أنه يكفي تعويض $n = 0,1,2$ والتأكد من تحققها سنحلها قريباً جداً (ونعم صحيح يمكننا تعويض $n = 0,1, \dots ,8$ في الأصلية) ولكن أيضاً لو لم نعرفها؟!

لم لا نحلّل $3n^3 + 5n \equiv n^3 + 2n \equiv n^3 - n \ mod \ 3$

$$\equiv n(n^2 - 1) \equiv n(n-1)(n+1) \equiv 0 \ mod \ 3$$

لأنه جداء ثلاثة أعداد متتالية لابد وأن حداها من مضاعفات الـ 3.

■

**تمرين 6:** أوجد

$$d = (2002 + 2, 2002^2 + 2, 2002^3 + 2, \dots \dots)$$

**تمرين 7:** أثبت أن

$$11^2 \nmid (n-7)(n+4)+33$$

**الحل:**

لنفرض أن $11^2 \mid (n-7)(n+4)+33$

(هنا التجزئة غير ممكنة لأن 11 ليس أولي مع 11 أي لا يمكن أن نحول المسألة لـ 11 يقسم كذا و11 أيضاً يقسم كذا)

ما نقوم به هو ما يشبه البناء نبدأ بأول قوة لـ 11 ثم على أساس المعطيات نلاحق القوة الثانية:

الآن لتسوية وضع 11 الأولى $11 \mid (n-7)(n+4)+33$

$$11 \mid (n-7)(n+4)$$

إذاً 11 يجب أن تدخل في أحد القوسين على الأقل وهي أهم وأوضح خواص العدد الأولي سنناقشه في الصفحة التالية

إذاً إما: $11 \mid n+4$

أو $11 \mid n-7$

ولكن $n+4=(n-7)+11$

لذلك إذا قسمت الـ 11 أحد القوسين ستقسم كلا القوسين اجباري لذا في حالتها

$$11^2 \mid (n-7)(n+4)$$

ولكن بالعودة للبناء والقوة الثانية إذا كان $11^2 \mid (n-7)(n+4)+33$ عندها

$$\Rightarrow 11^2 \mid 33$$

وهذا تناقض.

تعقيب: سنحصل على نفس المسألة لو وضعت لك $(n-3)^2$ وجمعت لها أي عدد مضاعف للـ 11 وغير مضاعف لـ $11^2$

بهذا نكون قد تعلمنا استراتيجيات متقدمة نوعاً ما في إثبات أو نقض القسمة.

## الفكرة الاخيرة في الـ ق.م.أ

**القاسم المشترك بمجهولين والاستفادة من فكرة العامل الأولي الأبسط**

$(x\ ,y)=1$ نقض هذه العلاقة هي وجود $p$ اولي بحيث $p|x\ ,p|y$ فهي أبسط علاقتين لنتعامل معهم

لنرى تطبيقاً عليها إذا كان $(a\ ,b)=1$

أثبت أن $(ab,a+b)=1$

لنفرض العكس عندها يوجد $p$ بحيث $p|ab\quad ,\quad p|a+b$

من العلاقة الأولى نجد أن $p$ يقسم أحد العددين $a$ أو $b$

من العلاقة الثانية نجد أن $p$ يقسم الآخر، وبالتالي $p|\ b\quad ,\quad p|a$ هذا تناقض

**تمرين 1: أوجد** $(a+b\ ,b)$ حيث $a,b\in\mathbb{Z}$

إنه حقيقة ليس مثال إذا كان $(a\ ,b)=1$ عندها

$$(a+b\ ,b)=(a\ ,b)=1$$

**تمرين 2:** أوجد $A=(a+b\ ,a-b)$ حيث $a,b\in\mathbb{Z}$

$$A=(a+b\ ,2a)$$

$a+b\ ,a$ أوليان فيما بينهما حسب التمرين السابق

$$A=(a+b\ ,2)$$

وهذا أبسط شكل إذا 2 أو $A=1$ أو يمكن حله بدائياً كما في التمرين السابق.

**تمرين 3:**

$$a,b\in\mathbb{Z}$$

$$A=(a^2+b^2\ ,ab)$$

أوجد بدلالة $d = (a\,,b)$

**الحل:**

من صياغة المسألة وكأنه يوجهنا أن نعوض $(a,b) = d$ ، $a = da_1$ , $b = db_1$

$$A = \left(d^2\left({a_1}^2 + {b_1}^2\right), d^2a_1b_1\right) = d^2\left({a_1}^2 + {b_1}^2, a_1b_1\right) = d^2$$

القاسم الأكبر لـ ${a_1}^2 + {b_1}^2, a_1b_1$ يساوي 1 (إثباته تماماً كما المثال الأول في الفقرة)

عندما يكون الشرط $(a_1\,, b_1) = 1$ محقق فكّر في كون القاسم المشترك الأكبر واحد أو رقم ثابت.

يستفاد من هذه العملية - أي إخراج القاسم المشترك الأكبر $d$ من $b$ و $a$ وتحويلهما إلى $a_1, b_1$ - في حل علاقات قسمة أو معادلات ديوفانتية

إذاً غالباً يكون $d$ بأسّ (بدرجة) متساوي في كل الحدود فيتم اختصاره بسهولة.

ونستفيد من العلاقة $1 = \left(\text{تركيب}\,,\,\text{تركيب}\right)$ باختصار حدود من الطرف الأيمن للقسمة.

**مثال: أوجد ثنائية الأعداد الصحيحة $(a, b)$ التي تحقق**

$$a, b \in \mathbb{Z}$$

$$ab|a^2 - b^2$$

**الحل:**

نختصر $d$ فيتبقى ${a_1}^2 - {b_1}^2|a_1b_1$

ولكن كما سبق نثبت أن $\left(a_1b_1\,,{a_1}^2 - {b_1}^2\right) = 1$

$$a_1b_1|1$$

وتنتهي حينها المسألة ■

## الأعداد الأولية:

**تعريف:** الأعداد الأولية هي البنية الأولى للأعداد الصحيحة لا يمكن تقسيمها إلى جزأين لذلك لدينا هذه الخواص حيث $p$ أولي:

- $p \mid ab \Leftarrow p \mid a$ إما $p \mid b$ أو

وذلك لأن $p$ لا يتجزأ (له فقط عامل واحد) فلو كانت العلاقة $m \mid ab$ عندها يمكن لجزء من $m$ أن يدخل في $a$ والآخر في $b$

- $n \mid p \Leftarrow n = p$ إما $n = 1$ أو

وضوحاً أصلاً.. إنه تعريف العدد الأولي.

- كل عدد يحلل إلى جداء عوامل اولية $n = p_1^{a_1}.p_2^{a_2}.p_3^{a_3} \dots \dots .p_m^{a_m}$

وأيضاً نستنتج أن العدد $n$ يحوي $m$ مجموعة أولية فيما بينهما وهي $p_1^{a_1}, p_2^{a_2}, p_3^{a_3}, p_4^{a_4}, \dots, p_m^{a_m}$ كل واحدة منها تُعامل باستقلال عند تطبيق الـ $mod$ كما ورد في النظرية
(المقصود إذا كنا نتعامل مع أثبت أن كذا $n \mid$ ).

**مثلاً:**

إذا كان $\boldsymbol{n = 360 = 2^3 \cdot 3^2 \cdot 5}$ عندها لدينا 3 مجموعات أولية فيما بينها واحدة لـ 2 وأخرى لـ 3 وأخرى لـ 5 فعند مناقشة القسمة على $\boldsymbol{n}$ نناقش القسمة على $\boldsymbol{5}$و$\boldsymbol{3^2}$و$\boldsymbol{2^3}$ كلٍ على حدا فتتحقق على إثر ذلك القسمة على$\boldsymbol{360}$.

## الآن تمارين عن الأعداد الأولية

**تمرين 1:** $A = p^2 + 2^p$ أوجد العدد الأولي $p$ بحيث يكون $A$ أولي.

**الحل:**

ترى ما الذي يمنع المقدار السابق أن يكون أولياً لكثير من قيم $p$؟!!

نجرب اولاً مؤكد لن نجرب 2 لأنها تجعله عدداً زوجياً.

عندما $p = 3$ $A = 17$ اذاً محققة

$$A = 57 = 3 \times 19 \quad p = 5$$

$$A = 2169 = 3 \times 733 \quad p = 11$$

اذاً نلاحظ أنه دائماً $A$ يحوي 3 لربما هذا سبب عدم كونه أولياً عندما $p \neq 3$ اذاً لنثبت أن

$$3|p^2 + 2^p \quad p \neq 3$$

$$p^2 + 2^p \equiv p^2 + (-1)^p \equiv p^2 - 1 \; mod\; 3$$

$$\equiv (p-1)(p+1) \equiv 0 \; mod\; 3$$

الأخيرة يمكننا أن نثبتها إذا كنّا نعرف فيرما $a^{p-1} \equiv 0 \; mod\; 3$ ، $p$ أولي $(a, p) = 1$

أو عندها مباشرة $p^2 - 1 \equiv 0 \; mod\; 3$

((حيث $p$ مكان $a$ و 3 مكان $p$ ))

- أو بدونها اذ أن باقي قسمة العدد الغير مضاعف لـ 3 على 3 (لأن $p$ هنا لا يقبل القسمة على 3) إما 1 أو $-1$.
- أو إيجاد البواقي التربيعية $mod\; 3$ طريقة سنستعملها قريباً اذاً انتهى الإثبات.

**تمرين 2:**

أوجد $n$ بحيث $3n-4$ و $4n-5$ و $5n-3$ جميعها أولية

**الحل:**

لنبدأ من الصفر في الأعداد التي يمكن مناقشتها

لنرى الـ 2 $4n-5$ فردي وضوحاً اذاً لا يشكل تناقض

ماذا عن $3n-4$ و $5n-3$ أحدهما زوجي وذلك لأن

- إما لأن مجموعهما فردي
- أو الطريقة الثابتة

$$3n-4 \equiv n \ mod\ 2$$

$$5n-3 \equiv n-1 \ mod\ 2$$

بالتالي أحدهما فردي

اذاً **إما** $3n-4=2 \Longleftarrow n=2$ نعوض فتكون الأعداد هي 2,3,7.

**أو** $5n-3=2 \Longleftarrow n=1$ مرفوض.

**التمرين 3:** أوجد $p, q$ بحيث $p^2 + pq + q^2$ مربع كامل و $p, q$ عددان أوليان.

**الحل:**

علينا في حل المعادلات الديوفانتية (الصحيحة) أن نحول أحد الأطراف إلى جداء قوسين والآخر إلى جداء عدد محدود من الأعداد الأولية أو عدد ثابت.

$$p^2 + pq + q^2 = k^2$$

بعد محاولات عديدة التحليل يخطر لنا

$$(p+q)^2 - pq = k^2$$

$$(p+q)^2 - k^2 = pq$$

$$(p+q-k) \cdot (p+q+k) = pq$$

الآن لماذا انتهت المسألة؟؟ لأن $p, q$ كما أشرنا أعداد أولية لا تتجزأ لذلك هناك أربع حالات للتوزيع على الأقواس كما يلي

$$1 \qquad p \cdot q$$

بقية الحالات $\begin{cases} q & p \\ p & q \\ p, q & 1 \end{cases}$ ترفض فوراً لأن العامل الأيمن يجب أن يكون $\geq (p+q+k)$

$$(p+q-k) = 1$$
$$(p+q+k) = pq$$

الآن نعزل $k$ لأن العددين $p, q$ أهم من $k$ فهما أوليان أما $k$ فلا شروط عليه، إذاً نجمع المعادلتين

$$2p + 2q = pq + 1$$

$$pq - 2p - 2q + 1 = 0$$

الآن نأتي إلى هذا الصنف من المعادلات الديوفانتية

نحول المعادلة إلى قوسين ناتج نشرهما $pq - 2p - 2q$ إضافةً لعدد ثابت (لا يشكل عبئاً علينا)

$$pq - 2p - 2q + 1 = 0$$

$$(p-2)(q-2) - 4 + 1 = 0$$

$$(p-2)(q-2) = 3$$

ويوجد تمارين اخرى تعتمد على هذه الفكرة "**فكرة التحليل**"

**مثال:**

$$n^5 + n^4 + 1 = p$$

$$n^4 + 4 = p$$

**لذلك يجب تعلم ابعض أسس التحليل لتساعدك على حل مثل هذه المسائل**

**والآن مع المزيد من التمارين:**

**تمرين 1:**

$$\frac{1}{x} + \frac{2}{y} = \frac{1}{5}$$

**الحل:**

بالفك $xy = 10x + 5y$

$$xy - 10x - 5y = 0$$

$$(x - 5)(y - 10) = 50$$

**تمرين 2:** ماذا عن المعادلة التالية

$$3xy - 5x - 2y + 1 = 0$$

لنجرب التحليل لأنه الطريقة

$$(3x \quad )(y \quad )$$

ولكن ماذا سنضع هنا حتى نضربه بـ 3 ويصبح 5 ؟!! هذا غير ممكن..

نريد أن نجعل أمثال $x$ في المعادلة الأصلية مضاعفاً لـ 3

ونريد أن نحدث عدل بين $x$ و $y$ لذا نضرب المعادلة بـ 3

$$9xy - 15x - 6y + 3 = 0$$

$$(3x - 2)(3y - 5) - 10 + 3 = 0$$

$$(3x - 2)(3y - 5) = 7$$

**تمرين 3:**

أوجد حل لمشكلة هذه المعادلة

$$9xy - 5x - 7y + 1 = 0$$

**تمرين 4:**

أوجد الأعداد الأولية $p, q, r$ التي تحقق

$$7p$$

**تمرين 5:**

## الـ $Mod$

الـ $mod$ أقوى استراتيجية وأهمها في نظرية الأعداد.

- هي أعمق من القسمة التي تعني فقط $0\ mod\ n$
- فلو لم نتعمق في الـ $mod$ لن يخطر لنا أخذ باقي طرفي المعادلة على عدد معين ما لم يكن موجوداً بذاته في أحد الأطراف (وحده آلية للقسمة)، هذه الفائدة ستتعرف عليها تفصيلاً في هذا البحث.
- كما تعلمنا أن التعامل مع الـ $mod$ سهل وهو كالتعامل مع المعادلة أي التعويض ممكن على السطر مهما وجد أس أو أي شيء مثلاً.

$$(p-n)^5 \equiv (-n)^5 \equiv -n^5\ mod\ p$$

أو نكتب

$$(p-n)^5 \equiv (1-n)^5\ mod\ p-1$$

## نتأمل الان التمارين التالية مع الأرقام

### المثال الأول

احسب باقي قسمة المقدار $2^{2000}$ على 11

الحل

ننزل قوى من الأس الى الأساس ولاحظ الرقم 2000 يساعد على ذلك فهو مليء بال 5 وال 2

$$2^{2000} \equiv 16^{500} \equiv 5^{500} \ mod\ 11$$
$$5^{500} \equiv 25^{250} \equiv 4^{250} \ mod\ 11$$
$$4^{250} \equiv 16^{125} \equiv 5^{125} \ mod 11$$
$$5^{125} \equiv (5^5)^{25} \equiv (25 * 125)^{25} \equiv (3 * 4)^{25} \equiv 1^{25} \equiv 1 \ mod\ 11$$

**المثال الثاني :**

احسب باقي قسمة $257^{37}$ على 50

الحل :

نلاحظ هذه المرة أن 37 غعدد اولي وبالتالي لا نستطيع ان ننزل قوى الى الأساس

لنر كيف ندبرها برايك ماهي الفكرة

$$257^{37} \equiv 7^{37} \equiv \mathbf{7} * \mathbf{7^{36}} \equiv 7(7^2)^{16} \equiv 7(49)^{16}$$
$$\equiv 7(-1)^{16} \equiv 7(-1) \equiv -\mathbf{7} \equiv \mathbf{4} \quad mod\ 11$$

طبعا لاحظ عندما حصلت على $-7$ في الباقي 11 استبدلنا ب 4 وهما نفس الباقي ،،حيث ببساطة اضفت 11 لكي اتخلص من السالب

احيانا نقوم بالعكس فلو لدي $10 \ mod\ 11$ساجعلها $-1$ لان ال$-1$ اسهل جدا في التعامل ،،وهما نفس الباقي تماما حيث طرحت 11فقط

وبشكل عام كلما راينا باقي كبير مثل $30 \ mod\ 37$ نجعله $-7$مباشرة وستصبح من حركاتك البديهية

ولكن هذه الطريقة لها تطويرات لتسهيل التعامل والسرعة وهي مهارات لابد من اكتسابها في عالم نظرية الأعداد لذا فلنناقشها في المسائل التالية

**المثال الأول:**

أوجد $2^{1049} \ mod\ 29$

**الحل:**

أولاً عليك أن تعرف أنّ مثل هذه المسائل لا تخيفنا أبداً، لأننا نعلم لها حلاً طويلاً جاهزاً وهو حساب هذه القوة بالتدريج من $2, 2^2, 2^3 \dots, 2^{1049}$.

وطبعاً الـــ $mod$ لا يسـمح للأعداد بأن تصـبح أكبر من 25 وبالتالي ليسـت بالمهمة الصـعبة ،ولكننا دوماً نبحث عن حل أســهل ... وهذا هو طريقنا في نظرية الأعداد: أن نؤمَّن الطريق الطويل ثم نبحث عن الأقصر والأذكى.

لو لجئنا لطريقتنا السـابقة ربما سـنخرج $2^9$ خارج الجداء لنرفع الـــ 2 لقوة 10 قوة149ونبسـط $2^{10}$ ولكن هذه ما زالت معقدة قليلاً وخصوصاً مع الرقم 149.

لذا ما سنفعله هو أننا **سندرس قوى ال2في الـ $mod\ 29$** ولكن ليس كلها حتى اللانهاية **فعند محاولة أول29قوة** وخاصة ان 29 يعتبر **ليس كبيرا** بل مقبول لدراسة القوى ...ستضمن أنك ستحصل على قوة قيمتها 1 وهي ما سنستفيد منه.

$$2^5 \equiv 32 \equiv 3\ mod\ 29$$

حسبت قوة 5مباشرة لانها اول قوة ل 2 بعد ال29 وبالتالي يمكن اختصار 29 منها

$$2^{15} \equiv (2^5)^3 \equiv 3^3 = 27 \equiv -2\ mod\ 29$$
$$\Rightarrow 2^{14} \equiv -1\ mod\ 29$$

ولان ال 1 اسهل حتى من ال$-1$ عند رفعه للاسس:

$$2^{28} \equiv 1\ mod\ 29$$

بالفعل درست قوى الـ2وأوجدت الـ 1 المنشود

والآن كيف نستفيد من ذلك؟

لدينا $1149 = 28 \cdot 41 + 1$

$$2^{1149} \equiv 2^{28 \cdot 41+1} \equiv 2(1)^{41} \equiv 2\ mod\ 29$$

وهو المطلوب.

**تمارين:** أوجد آخر منزلتين من $A \equiv 7^{2010}$ (المطلوب هو $mod\ 100$ )

**الحل:**

$$A \equiv 7^{2010} = 49^{1005}$$

ربما 100 **كبير نوعاً ما** ....فالفكرة القوية هذه المرة التي سنقوم بها هي

لنناقشه على خطوتين $4 \times 25$

$$A \equiv 7^{2010} \equiv (-1)^{2010} \equiv 1 \ mod\ 4$$
$$A \equiv 7^{2010} \equiv (49)^{1005} \equiv (-1)^{1005} \equiv -1 \ mod\ 25$$

الآن كيف نجمع $mod\ 4$ و $mod\ 25$ إلى $mod\ 100$

هنا لمحة عن ذلك

بما أننا نبحث عن $mod\ 100$

$$A \equiv -1 + 25k \ mod\ 100$$

بهذه الحركة يكون قد حافظنا على خاصية $A \equiv -1\ mod\ 25$ ولكن بقي أن نختار $k$ بحيث يكون

$-1 + 25k$ يكافئ 1 بالـ $mod\ 4$

نجرب $k$ من $1 \leftarrow 4$ واحدة منهم ستحقق ذلك أو من $0 \leftarrow 3$ (لأنها تشكل كل الاحتمالات الممكنة)

$49\ ,24$

إذاً: $A \equiv 49\ mod\ 100$

عندما نتعود على اللمحة ستصبح هذه طريقة أسهل ولكن حالياً هناك طريقة على 0100 مباشر

$$7^{2010} = 49^{1005} = 49 \cdot 49^{1004}$$
$$= 49 \cdot (49^2)^{502}$$
$$= 49 \cdot (2401)^{502}$$
$$\equiv 49 \cdot (1)^{502} \equiv 49\ mod\ 100$$

**تمرين 4:** أوجد آخر منزلتين لـ $2^{999}$

**الحل:**

لندرس $mod\ 25$

أي من قوى الـ 2 أقرب مايمكن إلى مضاعفات الـ 25 سنرى أنها بعد التجريب

$$1024 = 2^{10} \equiv -1\ mod\ 25$$

لاحظ الباقي هنا هو $-1$ وهو باق رائع عندما يرفع لأي أس

سنحاول الاستفادة منها:

$$2^{999} = 2^9 \cdot 2^{990}$$

$$= 2^9 \cdot (2^{10})^{99}$$

$$= 512 \cdot (1024)^{99}$$

$$\equiv 512 \cdot (24)^{99}$$

كلما وصلنا لعدد قريب جداً لـ 25 **نحوله إلى مكافئه السالب** لأنه أسهل لحساب الأس:

$$\equiv 512 \cdot (-1)^{99}$$

$$\equiv -12\ mod\ 25$$

$$\equiv 13\ mod\ 25$$

$$\Longrightarrow 2^{999} \equiv 13 + 25k\ mod\ 100$$

يجب أن يكون $4\ mod\ 0$ نجرب فنجد $k = 1$

$$\equiv 28\ mod\ 100$$

وبالتالي 28هما منزلتيه الأخيرتين

**تمرين 5:**

احسب باقي $14^{14^{14}}$ على 25

طبعا هنا يوجد اس كبير ولدينا 25 ليست كبيرة للغاية فلنوجد نقطة ضعفها (اي نناقش قوى ال 14 الصغيرة حتى نصل الى ال1

$$14^2 \equiv 21 \equiv -4\ mod 25$$

$$14^4 \equiv (-4)^2 \equiv 16$$

$$14^5 \equiv 224 \equiv -1\ mod25$$

ممتاز

$$14^{10} \equiv (-1)^2 \equiv 1\ mod25$$

الان كيف نستفيد من هذه المعلومة في اس الاس ..دعنا لانعقد الامور ونرجع لمعنى اس الاس

$$14^{14^{14}} = 14^{14*14*14*14.....14}$$

حيث ذكرت 14 ... 14مرة في الأس

وبما ان $14^{10}$ يمكن تعويضها ب 1 ..فيكون كاننا أزلنا 10 من الأس ....**اذا ببساطة اينما نجد 10 نزيلها**

وذلك ببساطة لأن $14^{\mathbf{10}} \equiv 1 mod25$

وبالتالي

$$14^{14^{14}} \equiv 14^{4*4*4.....4} \equiv 14^{4^{14}} mod25$$

**اذا وكاننا نحسب الان باقي $4^{14}$ على** 10

$$14^{4^{14}} \equiv 14^{16^7} \equiv 14^{6^7} mod25$$

ولكن $6^7$ او ال 6 مرفوعة لاي أس تعطي 6 في الباقي 10

اذا

$$14^{6^7} \equiv 14^6\ mod25$$

الان الامور بسيطة نكمل الحساب

$$14^6 \equiv -14 \equiv 11\ mod25$$

**المثال الثاني** أوجد أصغر مكعب ينتهي بـ 888

**الحل:**

وهو ليس كما اعتدنا، هنا لدينا حالة عكسية حيث علينا أن نحل المعادلة:

1 $$x^3 \equiv 888 \; mod \; 1000$$

الطريقة الأكثر تقليدية لحل معادلات الـ $mod$ هي التجريب ولكن التجريب على الـ 1000 ليس بالفكرة المبتكرة

إذا لو استخدمنا طريقة التجزئة في الـ $mod$ ثم إعادة الدمج

قد نأخذ 8 أولاً ثم 125 ثانياً ولكن أيضاً 125 كبيرة لذا سنأخذ 10 حالياً (ولكن ليس 10 ثم 100 لأنهما ليسا أوليان فيما بينهما).

سنأخذ $mod10$ فقط (أي سآخذ جزءاً من الشروط لأرى جزء من حقيقة $x$ ثم أدخله في الصورة الأكبر).

$$x^3 \equiv 888 \; mod \; 10$$

$$x^3 \equiv \; 8 \quad mod \; 10$$

$$x^3 \equiv \; 8 \quad mod \; 10$$

$$x^3 \equiv \; 2 \quad mod 10$$

**لا يجوز الجذر مباشرة سنرى لاحقاً الشروط لذلك نكتفي الآن بالتجريب**

$x = 10k + 2$ نعوضها في المود الأكبر (الأصلي) $600k^2 + 120k \equiv 880 \; mod \; 1000$

2 $$60k^2 + 12k \equiv 88 \; mod \; 100$$

أيضاً بنفس الخطة نأخذ $60k^2 + 12k \equiv 88 \; mod \; 100$

$$2k \equiv 8 \; mod \; 10$$

$$k = 4 \; mod \; 5$$

وهنا تنتج لدينا حالتين: (سنترك التفاصيل الحسابية للقارئ)

أما $k = 10t + 4$ نعوض في 2 ونختصر

$$12t \equiv 8 \ mod\ 10$$
$$6t \equiv 4 \ mod\ 5$$
$$3t \equiv 2 \ mod\ 5$$
$$t \equiv 4 \ mod\ 5$$

أو $k = 10t + 9$ نعوض في 2 ونختصر

$$60 \cdot 81 + 20\ t + 8 \equiv 88 \ mod\ 100$$
$$60 \cdot 81 + 20\ t \equiv 80 \ mod\ 100$$
$$3 \cdot 81 + \ t \equiv \ 4 \ \ mod\ 5$$
$$t \equiv \ 1 \ \ mod\ 5$$

**هنا استنتجناها بتجريب الأعداد**

**من 1 إلى 5 في المعادلة أعلاها**

**واحد منها فقط سيحقق وهو كان الـ 4**

الان نريد الـ$t$ بالمود 10 :

إذاً $t = 10m + 4$

أو $t = 10m + 9$

إذاً $t = 10m + 1$

أو $t = 10m + 6$

نعوض في $k$ ومنه في $x$

$$x = 1000m + 442$$
$$x = 1000m + 692$$
$$x = 1000m + 942$$
$$x = 1000m + 192$$

هكذا وجدنا جميع الاعداد التي مكعبها ينتهي بـ888

ولكن أصغرها هو 192

### المثال الثالث:

$$\binom{99}{19} = (10719667408076193 6xyz)_{10}$$

أوجد $x, y, z$ (بدون استخدام الآلة الحاسبة).

**الحل:**

ليست فكرة عملية أن نحسب المقدار فالمطلوب هو ثلاث خانات فقط.

أول فكرة قد تكون حساب $1000\ mod$ ولكنه صعب أيضاً يمكننا حساب $10\ mod$ سيعطي فكرة عن $z$ ولكننا نريد معلومات أكثر.

ما هي البواقي غير 2, 5 يسهل حساب العدد فيها إذا عرفنا الخانات ما عدا أول 3 ؟؟

الجواب هو 9, 11 وهناك الـ 7 أيضاً ولكن أصعب قليلاً.

لنتأمل أن التوافيق مضاعف لـ 9, 11 لأن إيجاد $mod$ كبير في غير هذه الحالة له شروط (سنتعرف عليها لاحقاً)

يكون الكسر مضاعفاً لعدد ما إذا وجد بالبسط أكثر تماماً من المقام (مستحيل المقام يكون فيو أكبر لأن هذا الكسر (التوافيق) في النهاية عدد صحيح) وهذا يعني أنّ الحالة الأُخرى هي البسط نفس المقام.

الآن كيف نشعر أن كسر التوافيق مضاعف لـ 3 مثلاً؟ غالباً يوجد في البسط عدد مميز للـ 3 في مثالنا 81 ونتأكد من ذلك بالعد الفعلي لقوى 3 أما للـ 11 يوجد 88 و 99 في البسط و 11 في المقام وللـ 7 يوجد 98 في البسط (دون مقابل في المقام) إذاً الطرف الأيمن يجب أن يكون مضاعفاً للأعداد 7,9,11 لذا سنتعامل مع اليمين الآن فقط

نأخذ له $7,9,11\ mod$

$$x + y + z \equiv 0\ mod\ 9$$
$$z - y + x - 6 + 3 - 9 + 1 - 6 + 7 \ldots - 0 + 1 \equiv 0\ mod\ 11$$
$$z + 2y + 4x + 6 + 2(3) + 4(9) + 1 + 2(6) + 4(7) + \cdots + 7 + 2(0) + 4(1) \equiv 0\ mod\ 7$$

بالحساب

$$x + y + z \equiv 0\ mod\ \ 9$$

$$z - y + x \equiv 0\ mod\ 11$$

$$z + 2y + 4x \equiv 3 \; mod \;\; 7$$

(طبعاً اســتخدمنا قوانين حســاب باقي الأعداد على 9,11,7 والتي لم تســتنتج من العدم بل اعتماداً على بواقي الـ 10على هذه الأعداد -فمثلاً العدد 123 يكتب بالشكل: $1 + 2 \cdot 10 + 3 \cdot 10^2$

والآن كما يلي:

من العلاقة الثانية نستنتج أنّ المقدار $z - y + x = 0,11$ لأننا دائماً في نظرية الأعداد لا ننسى حجم المجاهيل فهذا المجهول هو رقم منزلة لذا المقدار لا يساوي 22 أو غيرها من مضاعفات الـ 11 نأخذ حالتين ونعوض في كل منهما في التكافئين المتبقيين والباقي تحصيل حاصل👌

وجب الذكر هنا أن التوافيق دائماً عدد صحيح لأنه يمثل عدد طرق ولذلك جداء أي $n$ عدد متتالي مضاعف لـ $n!$ هام جداً جداً. الحل هو $(x, y, z) = (6,9,3)$

**المثال الرابع:** $p + q = (p - q)^3$ أوجد $p, q$ حيث $p, q$ أوليان

**الحل:**

$$p + q \equiv 0 \; mod \; p - q$$
$$2q \equiv 0 \; mod \; p - q$$

هذا يعطي 4 حالات ناقشهم ببساطة

# القوى في الـ $mod$

**البواقي التربيعية:**

أكثر ما يفيدنا في الأعداد المربعة أنها لا تعطي كل البواقي $(mod)$ أي عدد.

فمثلاً لا يوجد مربع باقيه على 4 2 أو 3، الباقي ممكن أن يكون 1او 0 فقط.

كيف عرفنا ذلك؟ أو كيف نعرف البواقي التي يمكن يأخذها المربع والتي لا يمكن؟؟!!

≡ كما يلي: نجرب كل الأعداد

$$0^2 \equiv 0 \quad 1^2 \equiv 1 \quad 2^2 \equiv 0 \quad 3^2 \equiv 1$$

نتوقف هنا لأن تجريب 4 مثل تجريب الـ 0 في $(mod\ 4)$

≡ ماذا عن 9؟!!

$$0^2 \equiv 0 \quad 1^2 \equiv 1 \quad 2^2 \equiv 4 \quad 3^2 \equiv 0 \quad 4^2 \equiv 7 \quad 5^2 \equiv 7 \quad 6^2 \equiv 0 \quad 7^2 \equiv 4 \quad 8^2 \equiv 1$$

إذاً البواقي التربيعية و $mod$ هي $\equiv 0, 1, 4, 7$ وغيرها من الأعداد جرب الـ 16 و 7 و...

**مثال 1:** هل يمكن أن يكون $\underbrace{1111111111}_{n \text{ مرة}}$ حيث $n \geq 2$ مربع كامل

**الحل:**

الفكرة فقط أن تأخذ الـــ $mod\ 4$ تخيل نعرف اننا لو اخذنا الجذر لن يكون عدد صــحيح فقط من خلال باقي بسيط على 4

**مثال 2:** 24680 هل يمكن إذا بدلنا منازل هذا العدد بأي طريقة أن يصبح مربع كامل

التفكير الصحيح ما الذي يبقى ثابتاً عند تبديل مواقع الأرقام

نعم إنه مجموع أرقام العدد وبالتالي $mod\ 9$

في الرقم المعطى مجموع الارقام $2 mod\ 9$...وبايجاد جدول بواقي مربعات الاعداد في $mod\ 9$ نجد 0,1,4,7

ولانجد 2وبالتالي مهما بدلنا الأرقام لن نحصل على مربع كامل

. **مثال 3:** اثبت ان مربع اي عدد اولي اكبر من 3 هو يكافىء $1 \ mod \ 12$

**الحل :**

نلاحظ طبعا ان 12 هي $4 \times 3$ اذا نثبت ان مربع اي عدد اولي فردي هو $1mod3$و$1mod4$

باخذ جدول مربعات بواقي اي عدد بال$mod3$ نجد انه اما $0,1$ ويكون 0 فقط اذا كان العدد بالاساس $0mod3$

مثل هذا الجدول لن تضطر لكتابته كل مرة بل ستحفظه تلقائيا عندما تحتاجه المرة القادمة

ولكن بما اننا ناخذ عدد اولي اكبر من 3 اذا مستحيل ان يكون مضاعف لل3

والان جدول مربعات بواقي الاعداد بال$mod4$ ايضا نجد انه اذا كان العدد زوجي اي $0,2mod4$ يكون مربعه $0mod$ واذا كان فردي اي $1,3mod4$سيكون مربعه $1mod$ وبما اننا لدينا عدد اولي اكبر من 2 سيكون مربعه

حتماً $1mod4$ بوبالتالي من المناقشتيين نجد ببساطة انه $1mod12$

**ملاحظة**: لاحظ انه ليس شرط ان يكون عددا اوليا ،،يكفي ان يكون غير مضاعف ل 3 او2

**مثال 4:** هل يمكن أن يكون $\{13d-1\ ,5d-1\ ,2d-1\}$ مربعات كاملة في ان واحد حيث $d$ عدد صحيح

لا يبدو أننا نستطيع أن نثبت عدم وجود $d$ يحقق الخاصة تراجحياً، فالمربعات لا تتأثر ببعضها ضرباً برقم كالـ 2 أو 5 أو 13

فالعدد $x^2$ وضعفه $2x^2$ يوجد مربع بينهما قد يكون عند $2x^2-1$ مثلاً

لذا أين يكمن التناقض لابد أنه في باقي $d$ لأحد الأعداد لو جربنا $mod\ 4$ لأخفقنا لأن $d \equiv 1 \ mod \ 4$ تفي بالغرض للثلاث مقادير

صراحة الاختيار 4 ضعيف لأن $13d-1 \equiv 5d-1 \ mod4$ وهذا يعطي فرص أقل للتناقض والـ 8 أيضاً لا تزال ضعيفة لنفس السبب ،لذا سنأخذ حتماً mod16 لنجد اختلاف بين المقدارين السابقين وسنلاحظ ان بواقي 16 التربيعية ستنهي المسألة.

طبعاً لا تقلق فسوف تجرب الـ $mod$ البواقي بالترتيب التصاعدي أخذ $mod5$ ستخسر $5d-1$وأخذ باقي الـ 3 سيجعل $2d-1 \equiv 5d-1$ وتجرب طبعاً $mod7$ ولكن الباقي 6 $mod7$ يجعل الثلاث مقادير مقبولة كمربعات في $mod\ 7$ .ستصل بالنهاية الى $mod16$لأنك ببساطة تستبعد المودات الاخرى بسرعة جدا مع الخبرة...الآن

البواقي التربيعية في $mod16$هي $0,1,4,9,$

لكي يكون $2d-1$ مربعاً كاملاً على $d$ أن ياخذ احد القيم التالية 1,5 ....حيث لاحظ ان $2d-1$ لا يمكن أإن يكافىء 0,4في $mod\ 16$

ولكن عندما $d \equiv 1\ mod16$ عندها $13\mathrm{d}-1 \equiv 12\ \mathrm{mod}16$ الذي هو ليس مربعاً كاملاً في $mod\ 16$

وعندما $d \equiv 5\ mod\ 16$ عندها $5d-1 \equiv 8\ mod16$ والذي هو أيضاً ليس مربعاً كاملاً في $mod\ 16$

إذاً في هذه المسـألة كان توقعنا الأكبر هو أنها لتنتهي يجب أن يقضيـ عليها $mod$ معين ولكن كان علينا أن نعرفه

**تمرين 5:**

لدينا عدد من الأعداد الصحيحة ( قد يكون البعض منها متساوي ) بحيث يكون مجموعها مساوياً لـ *1492* .
حدد إذا ما كان المجموع القوى السابعة لهذه الأعداد ( أي .... $a^7, b^7,$ ) يمكن أن يكون *1998*

الحل :

بفرض الأعداد هي $a_1, a_2, a_3, \dots, a_n$ عندها :

$$a_1 + a_2 + a_3 + \cdots + a_n = 1492 \ \dots (1)$$
$$a_1^7 + a_2^7 + a_3^7 + \cdots + a_n^7 = ???? \ \dots (2)$$

الآن سنفكر كيف سنحدد ما اذا كان هذا المجموع يمكن ان يكون مساويا ل *1998* .... يجب أن نستفيد من العلاقة (*1*) لكن بالتأكيد إنّها لا تكفي لحساب (*2*) كقي إذأ كيف سأستفيد من (*1*) هنا يتدخل ال *mod*... ماشي هلق بقا ولكن اي مود ساختار هلق بلاحظ ب (*2*) الأعداد مرفوعة للقوة *7* فأول ما بخطر لي انه اجرب *mod 7* بسبب فيرماا ببساطة اتمكن من ربط $a$ ب $a^7$ ((يمكن لفيرما ايضا ان ترتبط $a^{13}$ مع $a$ ببساطة لان فيرما تجعل كل $a^6 \equiv 1 mod 7$.... فكل $a^6$ تتحول الى 1..

نلاحظ اذا ان $a^7 = a \ mod 7$ ... هذه هي العلاقة الجوهريّة الّتي ستنهي المسألة ..

$$a_1^7 + a_2^7 + a_3^7 + \cdots + a_n^7 \equiv a_1 + a_2 + a_3 + \cdots + a_n \equiv 1492 \ mod \ 7 \ \equiv 1 \ mod \ 7$$

**تمرين 6**

لدينا $a_1 = 19 , a_2 = 98$ ، من أجل $n \geq 1$ نعرف $a_{n+2}$ هو باقي قسمة العدد $a_n + a_{n+1}$ على 100 . أوجد باقي قسمة العدد

$a_1^2 + a_2^2 + \cdots + a_{1998}^2$ على 8 .

**الحل :**

عندما طلب مني الباقي على 8 اوحى لي بفكرة ان ال 5 الموجودة ضمن ال100 لاقيمة لها...اذا ببساطة نأخذ $a_n (mod\ 4)$ كجزء من معلومة باقي قسمته على 100 ...تذكر متى فعلنا ذلك من قبل

الان بعد ان قررنا ان ناخذ من متتاليتنا فقط باقيها على 4 ،،نحسب اول عدة حدود بالباقي 4 كما تعلمنا لنبحث عن نوع من الدورية

فينتج بالفعل لدينا سلسلة البواقي الستة التالية 3 , 0 , 3 , 1 , 2 , 3 و التي تتكرر دوريا 333 مرة .

الان كيف نعرف باقي مربعاتها بال $mod8$ .... هنااا سنستخدم فكرة بسيطة ولكن رائعة

ان تربيع باقي عدد بال mod4 يعطي باقي المربع بال mod8،،، واكثر من ذلك ..اذا ربعنا عدد بالmod8 يعطي باقي المربع بال mod16 وهكذا(فقط على قوى ال2 سنرى لماذا ...وذلك لانه لو عدنا للاصل وقلنا ان

عندها $x = 4k + 3$

$$x^2 = \mathbf{16}k^2 + \mathbf{24}k + 9$$

هل لاحظت ..ان مربع ال4 حتما مضاعف لل 16..وان $3 \times 4 \times 2$حتما مضاعف لل8 فقط لان ال4 استفادت من ال2 الاتية من المتطابقة وبالتالي الرقميين مضاعفيين لل8 وبالتالي فعلا التربيع ينقلنا الى $mod 8$

$$a_1^2 + a_2^2 + \cdots + a_{1998}^2 \equiv 333(1+4+1+1+0+1) \equiv 0 mod\ 8$$

و منه الباقي هو 0 .

.

**ليست فقط التربيعي فالتكعيبي وأي قوة يمكن أن تعامل بنفس الطريقة**

الآن ماذا عن الأسية حيث يكون الأساس ثابت والأس هو المتغير.

فمثلاً $5^a$ ما هي البواقي التي يعطيها $mod\ 7$

سنجرب كل الأعداد

$$5^0 \equiv 1 \quad 5^1 \equiv 5 \quad 5^2 \equiv 4 \quad 5^3 \equiv 6 \equiv -1 \quad 5^4 \equiv 2 \quad 5^5 \equiv 3 \quad 5^6 \equiv 1$$

نتوقف عن التجريب لأننا وصلنا لواحد هذا يعني أن السلسلة ستعيد نفسها كل 6 حدود

**مسألة :**

ماهي قيمة التي يأخذها آحاد العدد ( $7^{7^{7^{\cdots^{7}}}}$.....) . اذا علمت ان هناك *1001* من ال*7* في الصيغة السابقة.

**الحل :**

إن القيمة التي ياخذها آحاد العدد هو باقي هذا العدد في مود ال*10* .

لدينا نحســب اول اســس ال *7* لنجد اجمل نتيجة والتي هي قد تكون $1, -1$ لاننا نعرف رفع ال1 للاس كم هو مريح

وبالفعل بسرعة هذه المرة نجد

$$7^2 = 49 \equiv -1 \; mod \; 10$$

و منه $7^7 = (7^2)^3 \times 7 \equiv -7 \; mod \; 10$..... ربما هذه المرة الاستفادة من ال$-1$ ليست خارقة لانه ببساطة تم رفعها للقوة ال3فقط والتي كان من الممكن حسابها بسهولة ...ولكن في ارقام اكبر .. ستكون ال$-1, 1$هي ملاذك التي تلجا لها لتشعر بارتياح ...اذا

$(7^7)^7 \equiv (-7)^7 \equiv -(7^7) \equiv -(-7) \equiv 7 \; mod \; 10 \Leftarrow$ لاحظ انه بعد كل رفعة للقوة 7تظهر سالب جديدة نخرجها خارج القوس

و بنفس الطريقة نستنتج أن $((7^7)^7)^7 \equiv 7 \; mod \; 10$

و بشكل عام $(\ldots(((7^7)^7)^7)\ldots^7) \equiv \pm 7 \; mod \; 10$

بحيث تكون الإشارة + في حال كان هناك عدد فردي من مرات الرفع للقوة *7* في الصيغة ، و تكون الإشارة – في حال كان هناك عدد زوجي من مرات الرفع للقوة ال*7* في الصيغة .

العدد *1001* هو عدد فردي و منه القيمة التي يأخذها آحاد العدد هي *7* .

سنأخذ العديد من النظريات عن هذه البواقي الأسية والدور ولكن سنحتاج إلى هذه النظرية شديدة الأهمية وتدخلنا في عمق الـ $mod$.

سنسميها **النظرية العظيمة**:

| | |
|---|---|
| **الصيغة الأولى** | لدينا جميع البواقي بـ $mod \; p$ حيث $p$ عدد **أولي** $\{0,1,2,3,4, \ldots p-1\}$ إذا ضربنا كل حد منهم بعدد ما (نضرب بنفس العدد للكل وهو أولي مع $p$). سنحصل من جديد على **جميع البواقي بـ $mod \; p$** |
| **الصيغة الثانية** | لدينا جميع البواقي $mod \; n$ **الأولية مع $n$** إذا ضربناهم جميعاً بعدد ما أولي مع $n$ سنحصل على جميع البواقي الأولية مع $n$ مجدداً. |

نلاحظ أن الصيغة الثانية هي المعممة من الصيغة الأولى

**الإثبات:**

لنفرض أن $i, j$ باقيان مختلفان بالمود $p$ بعدما ضربناها بـ $a$ فأصبح لهما نفس القيمة

$$aj \equiv ai \ \ mod\ p$$

ولكن $a$ أولية مع $p$

$$\Rightarrow j \equiv i \ \ mod\ p$$

وهذا تناقض لأن $i, j$ باقيان مختلفان في $mod\ p$

أو نقول $ai - ai \equiv 0\ mod\ p$

$$a(j - i) \equiv 0\ mod\ p$$

اذا $p$ يجب أن يقسم اليسار ولكن لا يمكن أن يدخل في $a$ لذا أيضاً تناقض

وبالمثل افرض من أجل $n$

$$(a, n) = 1$$

وجود باقيان $i, j$ مختلفان يحققان

$$aj \equiv ai\ mod\ n$$

$i \equiv j\ mod\ n$ تناقض

نختصر على $a$ لأنها أولية مع $n$ وكأنها تقول أنا لا أستطيع أن أفيد $n$ بشيء فاختصروني من الطرفيين

هذه النظريات هامة جداً والفكرة في الإثبات هامة للغاية في عالم نظرية الأعداد ويجب أن تبقى في ذهنك طوال فترة حلك للمسائل.

**مسالة 1:**

اذا كان لديك عدد اولي $p$ ولديك $a$ عدد طبيعي اولي مع $p$

اثبت ان التطابق التالي $an \equiv 1\ mod\ p$ له حل $n$ ....واستنتج منها انه يمكننا استخدام **المقلوب في ال مود** $\frac{1}{a} mod p$

الان لو اخذنا المجموعة $\{an\}_0^{p-1}$ كما ناقشنا قبل قليل انها تعطي كل البواقي في $mod\ p$ بوالواحد هو احد البواقي لذا سناخذ ببساطة ال $n$ التي تعطي ان$an \equiv 1$ كحل المطلوب للتطابق

الان ننتقل الى النقطة التي اسعى للوصول لها

هو مشروعية استخدام المقلوب في ال *mod* ...الان بفضل ما اثبتناه نقر مشروعيته لانه $\frac{1}{a} mod p$

قيمته موجودة دائما وهي ال *n* التي اوجدناها ..وبالتالي لم نعد نخاف من حالة عدم تعريف او عدم تحديد للمقلوب

اومن وجود عملية لا يمكن اجرائها للمقلوب ..فكل ما ينطبق على *n* ينطبق على $\frac{1}{a}$

## مسألة 2

لدينا متتالية حسابية غير منتهية .... $a_1, a_2, a_3 \dots a_n$ هل يمكن ان تكون مجموعة الاعداد الاولية التي تقسم احد عناصر المتتالية ..مجموعة محدودة؟؟

**الحل**

بما انها متتالية حسابية عندها $a_n = an + b$ حيث *a* هي الفرق المشترك و *b* هو الحد الاول كما تعلمت في مقدمة الجبر

الان الشكل الخطي هذا ..لقد ناقشناه للتو..ماذا يخطر لك الان بخصوص طلب المسالة

بالتاكيد خذ اي عدد اولي *p* غير موجود في *a* عندها *an* تعطي كل البواقي في ال *mod p* لو جربنا ل *n* كل القيم من *1* الى *p-1* .....ولكن من بين هذه البواقي سنحصل على ال *b-* اذا وبالتالي يمكن ايجاد *n* بحيث $a_n = an + b$

مضاعف ل p فقط ببساطة ان لايكون p موجود في a اذا مجموعة الاعداد الاولية التي تقسم اي عنصر من عناصر المتتالية هو غيييير منتهي

ملاحظة :طبعا يمكن ان تعبر الان عما سبق :

ان التطابق $an + b \equiv 0 \ modp$ له حل n

وهو

$$n \equiv \frac{b}{a} mod p$$

...وفي المستقبل هذه المناقشة ستصبح من بديهياتك ..الخطي يعطي كل شيء

## مسالة 3:

### مسألة 4:

من أجل عدد صحيح $n > 6$ لتكن $\{a_i\}_1^t$ مجموعة الأعداد الأصغر من $n$ والأولية مع $n$ إذا كانت تحقق:
$a_2 - a_1 = a_3 - a_2 \dots = a_k - a_{k-1} > 0$، أثبت عندها أن $n$ إما عدد أولي أو قوة للـ 2:

**الحل:** الآن نفرض أن 1 هو أول هذه الأعداد، أي $a_1 = 1$ والأخير $a_k = n - 1$، الآن نريد المزيد من الحدود، $a_2$ مثلاً ما هي؟ هل هي 2؟ نعم إذا كان $n$ فردياً، وعندها الفرق المشترك هو 1 وبالتالي العدد أولي حصراً ... إذاً نفرض $n$ زوجي.

إذاً ما قيمة $a_2$؟ إياك أن تتركها وشأنها حتى تعجز بها، إن لم يوجد 3 في $n$ عندها الفرق المشترك هو 2 وبالتالي $n$ قوة الـ 2.

إذاً نعود لـ $a_2$ طبعاً بعد أن نفرض $n$ مضاعف لـ 3 أيضاً ... لكي ننهي قضية $a_2$، نلاحظ أن $a_2$ هي أصغر عدد أولي $P$ غير موجود في $n$، فالفرق المشترك هو $P - 1$، وبعد أن عرفنا الفرق، ما هو الحد الذي نعرف قيمة ولم نستفد منه؟ نعم إنه: $a_k$

$$a_k = (P-1)(k-1) + a_1$$

$$\Leftarrow n - 2 = (P-1)(k-1) \dots (*)$$

الآن ما قمنا به هو عمل روتيني، الان نريد فكرة صغيرة وظريفة (وهذه المسألة أضعها خصيصاً بعد كل ما تعلمناه لأؤكد على دور $mod$ الأعداد الصغيرة الذي يخدم في كثير من الحالات) (لا يحل المسألة بالكامل أبداً ولكن يستثني حالات نتمنى لو أنها غير موجودة أثناء عملنا)

جرب عدة أرقام، ما الذي يمنع تحقق ذلك بعد فرضنا للـ $P$؟ مثلاً $n = 2 \times 3 \times 5 \times 7$ لكي نجعل الـ $P = 11$

$$1 \quad 11 \quad 21 \quad 31$$

يحوي الحد 21 3، لكن ما دخل الفرق $P-1=10$ بهذه الظاهرة؟ ولاحظ من علاقة * أن $P-1$ غير مضاعف لـ 3 لأن $n-2$ غير مضاعف لـ 3، إذاً $P \equiv 2 \ mod 3$ و$P-1 \equiv 1 \ mod 3$ كما في $P-1=10$ ولكن ما المشكلة التي يولدها كون الفرق $1 \ mod 3$؟ بالطبع سيتولد حتماً $2P-1$ المضاعف لـ 3 ... عملياً حتى لو لم يكن مباشرة الحد الذي يليه مضاعف للـ 3 حتماً فيما بعد سيتولد مضاعف للـ 3 وهذه هي الفكرة دائماً مع الفرق الثابت.

إذاً نصل لتناقض في حالتي $P \equiv 1$ و$P \equiv 2$ في $P=3 \Leftarrow mod 3$ وهذا يفيدنا لحالة $a_2-a_1=2$، إذاً حتماً $n$ عدد أولي أو قوة لـ 2.

تقودنا هذه النتيجة أو النظرية السابقة إلى العديد من النظريات الهامة جداً عن الأسية.

## نظرية فيرما الصغرى:

**في حالة $p$ أولي، لدينا $a^{P-1} \equiv 1 \ mod \ p$ أياً كان $a$ أولي مع $p$ (أي $p$ لايقسم $a$)**

**الإثبات:** لدينا مجموعة البواقي $\{a, 2a, 3a, 4a, \dots (p-1)a\}$ تعطي جميع البواقي إذاً هذا المجموعة تساوي (بالـ $mod \ p$ طبعاً) المجموعة $\{1,2,3, \dots . p-1\}$

إذاً جداء عناصر المجموعتين لابد أنه سيكون متساوي

$$a \cdot 2a \cdot 3a \cdots (p-1)a \ \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \ \ mod \ p$$

نختصر على $(p-1)!$ لأنها أولية مع $p$

$$a^{p-1} \equiv 1 \ mod \ p \Leftarrow$$

إنها تسمى **نظرية $ferma$** سنرى التطبيقات العملية عليها.

النظرية الأخرى هي **نظرية Euler** وهي أعم وبرهانها ليس مخيفاً وهو نفس فكرة إثبات فيرما بالضبط ولكن مع احترام ال $n$ ستعتاد على هذا المبدأ في التعميم كثيراً في نظرية الأعداد: تنص المبرهنة

$$(a,n)=1 \quad \text{حيث} \quad a^{\emptyset(n)} \equiv 1 \ \ mod \ n$$

وحيث $\emptyset(n)$ عدد الأعداد الأولية مع $n$ وأصغر من $n$ (مثلاً $\emptyset(6) = 2$ لأنها الـ 6 أولية مع 1 و5 فقط).

**الإثبات:**

لدينا مجموعة البواقي **الأولية مع** $\boldsymbol{n}$ $\{b_1, b_2, b_3 \dots, b_{\emptyset(n)}\}$ لو ضربناها بـ $a$ لأعطت **جميع البواقي الأولية مع** $\boldsymbol{n}$ إذاً

$$\{ab_1, ab_2, ab_3 \dots . ab_{\emptyset(n)}\} = \{b_1, b_2 \dots . . b_{\emptyset(n)}\}$$

وايضاً نقول هنا أنّ جداء عناصر المجموعتين متساوي

$$a^{\emptyset(n)} \equiv 1 \mod n \Leftarrow$$

وطبعاً قسمنا على $\dots b_1 b_2$ لأنهم أعداد أوليّة مع $n$

ولكن قد تسألني كيف لي أن أحسب قيمة تابع أويلر من أجل أي عدد $n$ ؟؟

تم إيجاد صيغة لحسابه مباشرة وفعلاً الاستفادة منه في الـ $mod$

إذا كتبنا العدد $n$ على شكل جداء أعداده الأولية كما يلي:

$$n = \prod_{i=1}^{m} p_i^{e_i} = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

يكون

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_m})$$

عملياً ليس صعب الحساب فلو دققت بالصيغة فأنت تستبدل أي عدد موجود في $n$ بالعدد الأولي مطروحاً منه 1

**مثال:**

لدينا $\phi(3^3.5^2.7) = 2 \cdot 3^2 \cdot 4 \cdot 5^1 \cdot 6 \cdot 7^0 = 2160$

**تمرين 1: أوجد $a \in \mathbb{Z}$ بحيث و**

$$(a, 35) = 1: \quad 35 | (a^4 - 1)(a^4 + 15a^2 + 1)$$

**ملاحظة:** النقطتين تعني "حيث"

**الحل:**

الآن نناقش العامل 5 أولاً ثم ننتقل إلى العامل 7 حسب نظرية سابقة والتي أصبحت من البديهيات.

لدينا $5 | (a^4 - 1)$ حسب فيرما فانتهينا من العامل 5 فلننتقل إلى العامل 7:

$$(a^4 - 1)(a^4 + 15a^2 + 1) \equiv (a^4 - 1)(a^4 + a^2 + 1) \mod 7$$
$$\equiv (a^4 - 1)\frac{a^6 - 1}{a^2 - 1} \mod 7$$

يبدو أننا اقتربنا من ***Fermat***.

ولكن هناك مقام، نعلم أن $a^6 - 1$ تقبل القسمة على 7 ولكن نخشى أن تقبل $a^2 - 1$ أيضاً القسمة على 7من أجل بعض قيم $a$.

الحقيقة هذه القيم لـ $a$ هي 1 و $-1$ استنتجناه من

$$a^2 - 1 \equiv 0 \mod p$$
$$(a - 1)(a + 1) \equiv 0 \mod p$$

$p$ يدخل(يقسم) إلى واحد من القوسين إذاً إما $a \equiv 1 \mod p$ أو $a \equiv -1$ .

إذاً لنتخلص من المقام

$$(a^4 - 1)(a^4 + 15s^2 + 1)$$
$$\equiv \frac{(a^2 - 1)(a^2 + 1)(a^6 - 1)}{a^2 - 1}$$
$$\equiv (a^2 + 1)(a^6 - 1) \equiv 0 \mod p$$

حسب فيرما حيث $(a, 7) = 1$

**تمرين 2: اوجد جميع الأزواج $(x, y)$ الصحيحة التي تحقق ان:**

$$y^2 = x^5 - 4$$

لدينا قوة من المرتبة الخامسة، ما هو المود الذي قد ينفعنا

ماذا لو وجدنا مود قوي جدا للاس عشرة قد ينفعنا في حالتنا

بالتأكيد انه $mod11$ ...لانه حسب فيرما ..

$$x^{10} \equiv 1 mod(11)$$

اي انه لايوجد داعي لوضع جدول للقوة عشرة في $mod11$ فكل الاعداد ستعطي 1 ببساطة ....وابعد من ذلك من اجل $x^5$ لدينااا

$$(x^5 - 1)(x^5 + 1) \equiv 0 mod(11)$$

اذن $x^5$ اما 1 او -1 بالمود 11 وولكن البواقي التربيعية اي من اجل $y^2$ بالمود 11 هي $\{1,3,4,5,9\}$

بالبحث من هذه البواقي على بواقي تحقق المعادلة المعطاة لانجد اذا هذا ممتاز وبالتالي المعادلة لاحلول لها بفضل $mod\ 11$

**تمرين 3 : أثبت أنه يوجد عدد طبيعي $n$ : $2^n + 3^n + 6^n - 1$ مضاعف لأي عدد أولي $p$ كان**

**الحل:**

**نحاول إيجاد عدد متعلق بـ$p$ نضعه بدل إن فيصبح المقدار** $2^n + 3^n + 6^n \equiv 1\ mod\ p$

$n = p - 1$ لا تجدي، ستعطي الطرف الايسر قيمة 3

الارقام 2,3,6 تذكرنا بأن $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$

ماذا إذاً؟

- لايمكننا ان نعوض $n = -1$ لانه عدد طبيعي ...ماالحل اذا هل نستطيع ان نستفيد من المعلومة السابقة القوية التي وكانها مفصلة تفصيلا للمسالة

هنا تخطر عبالنا فكرة الدورية وتكرار البواقي عدة مرات ...

وبالفعل اهم الدورات التي نعلمها هي عند ال $p-1$

ماهي ال$-1$ بعد دورة كاملة .....بالضبط هي $-1$ من $p-1$

اي نعوض $n=p-2$ ....وهنا تظهر اهمية شرعية وصحة المقاليب في ال $mod\ p$

**تمرين 4**

ليكن m و $n$ عددين طبيعيين حيث $1 \leq m < n$ ، في النظام العشـري للعدد $1978^m$ آخر ثلاث خانات مســاوية لآخر ثلاث خانات في النظام العشـري للعدد $1978^n$ بالترتيب، أوجد $m.n$ بحيث يكون $m+n$ أصغر ما يمكن.

الحل: لكي يكون للمقدارين نفس اخر ثلاث خانات ببساطة يجب ان يتحقق

$$1978^m \equiv 1978^n \ mod\ 1000$$

$$1978^m(1978^{n-m}-1) \equiv 0\ mod\ 1000$$

نجد أن ال$2^3$ الموجودة في العدد 1000 يجب ان تكون موجودة في $1978^m$ لذلك مبدايا نوجد شرط على $m$ ان أصغر قيمة ممكنة لm هي 3 ويتبقى من الشرط المطلوب

$$1978^{n-m}-1 \equiv 0\ \ mod\ 125$$

$$1978^{n-m} \equiv 1\ \ mod\ 125$$

$$1 \equiv 1978^{n-m} \equiv (1978-15\times 125)^{n-m} \equiv 103^{n-m}\ mod\ 125$$

$$103^{\varphi(125)} = 103^{100} \equiv 1\ mod 125$$

وبالتالي لايجاد اصغر عدد $n-m$ يحقق التكافىء السابق $1 \equiv 103^{n-m}\ mod\ 125$

سيكون هذا العدد من قواسم ال100 لنبحث عنه ..

من الممكن التجريب واحدا واحدا حتى نصل فعلا لهذا العدد ولكن تعلمنا خبرات تفيدنا لنختصر الوقت

فمثلا سابدا ب $mod 5$ لاستنتج انه ان $n-m=4k$ مضاعف لل4

اذا العدد الاصغر لايستطيع التخلي عن ال4 الموجودة في ال100 الان لنرى عم قد يتخلى من ال25

اي ان الجواب سيكون اما $4,20,100$ اي $k = 1,5,25$

نلاحظ أن $103^{4k} \equiv 22^{4k} \equiv 6^k \ mod\ 125$

$$6^1 \equiv 6\ mod 125$$

اذا $k \neq 1$

الان فعلا ناتي الى القسم الذي نحسب فييه ...سنحسب الى $6^5 \equiv 26$

اذا $k \neq 5$

اذا حتماا $k = 25$ ولكي يطمئن قلبك

$$6^{25} \equiv 26^5 \equiv 1\ mod 125$$

$$n - m = 4k = 100$$

وال $m$ لايوجد عليها اي شرط اخر وبالتالي بالتاكيد سنختارها تساوي3 اذاااا

$$m + n = 106 \Leftarrow$$

هل لاحظت كمية الخبرة التي تتمتع بها الان ،، وما اجمل كل ما استخدمناه لكي نوفر الوقت والجهد

## مثال1: على الـ $mod$ بشكل عام:

أثبت أن $7^p - 6^p - 1 \equiv 0\ mod\ 43$ حيث $p$ عدد أولي اكبر من 3

**الحل:**

نعلم أن $6^p$ تفيدنا عند أخذ $mod\ p$ ب فيرما ..ولكن هنا فخ ..المطلوب ليس $modp$ .. فيا ترى ما المطلوب من العدد الأولي في $mod\ 43$ ربما أنه فردي أو أنه غير مضاعف للـ 3 لذا قد تكون الإجابة أسهل من المتوقع.

الان ماذا نفعل في مثل هذه المسائل ..حاول تذكر مسائل ابسط تشبه هذه المسالة ...فمثلا مسائل اوجد باقي العدد التالي في $modp$ او اوجد احاد وعشرات

نعم نجرب كالعادة من $1 \leftarrow 42$ عندها نلاحظ أن $6^p$ لحسن الحظ (او لان صاحب المسالة لا يطلب التعقيد ) ستتكرر عند الـ $p = 3$ و $7^p$ تتكرر عند الـ 6 لذا ككل يتكرر قيمة التركيب عند الـ 6 والان ماذا سنفعل احتفالاً بهذه المعلومة؟

حتماً سنجرب قيم من $0$ الى $5$ في المعادلة المطلوبة وهذا كافي بسبب المعلومة المكتشفة حديثاً

وبما ان $p$ عدد اولي القيم الوحيدة التي يتوجب علينا تجربتها هي $1,5$ فقط لانه مثلا $3mod6$ عدد مضاعف ل3

و $4mod6$ مضاعف ل2 .

**مثال 2:** أثبت أنه من أجل أي عدد $n$ يوجد عدد $m$ مؤلف من $n$ خانة فردية بحيث $5^n|m$

**الحل:**

اولا كما نرتاح ونحب ..نجرب امثلة لاول عدة $n$ ليطمئن قلبنا ونحاول تحسس بعض المعلومات من هذه الامثلة

$$3125\ ,125, 25, 5$$

هل نستفيد من العدد السابق أم نؤلف عدد جديد كليا لكل $n$

بالفعل يمكن ان نكتفي بالعدد السابق وفقا للامثلة (ولكن لو حاولت بالامثلة ووجدت ان اضافة خانة واحدة على يسار العدد السابق لا تفي بالغرض اتراجع عن هذه الفكرة..وابحث عن فكرة اخرى ..فانا لم اثبت ان المسالة خاطئة خاطئة ) ولكن كيف الان اثبت ان اضافة خانة تكفي

بأن نضيف خانة في أقصى اليسار ولكن أرى أن الخانات حصراً فردية قد تصعّب الأمر قليلاً

لذا ناخذ $m$ مكونا من $n$ رقماً و $5^n|m$

ساكتب $\mathrm{m} = 5^{\mathrm{n}} \cdot \mathrm{k}$

الان عند اضافة منزلة ستكون الخيارات بالكتابة العشرية

$$(am)_{10} \in \{9m\ ,7m\ ,5m\ ,3m\ ,1m\}$$

$((1m)_{10} = 1234 \Leftarrow m = 234$ نعني بهذه الكتابة لو أن)

$$(xm)_{10} = x10^n + 5^n k$$
$$5^n(x \cdot 2^n + k)$$

نريد $5^{n+1}$ أن يقسم الحد الاخير أي نختصر على $5^n$ فنجد

$$5|x \cdot 2^n + k$$

الان اخذ نفسا لانني قريب من الحل ..فانا الان اتعامل مع $mod5$ فقط

ولكن $x$ لو تاملنا كل قيمها الممكنة فيها سر ..نعم انها تعطي كل البواقي الممكنة بالمود $5$ و $2^n$ أولي مع 5 إذاً

$x \cdot 2^n$ تعطي كل شي ...اي تعطي $k$ –مهما كانت قيمة الأخير وبالتالي يوجد $x$ يحقق المطلوب.

**مثال3**: (نمط متكرر من المعادلات)

أوجد $(a, b)$ بحيث

$$3^a + 7^b \quad \text{مربع كامل}$$
$$3^a + 7^b = k^2$$

**الحل:**

هذه المسألة جميلة ومتكاملة

سنستفيد من خواص المربع في الـ $mod$ وأن الأسس تتحول إلى مربعات سهولة

أخذ $mod\ 3$ لا ينفع

بأخذ $mod\ 4$ $(-1)^a + (-1)^b \equiv 0, 1$ لذا اما $a$ أو $b$ زوجي لذلك نحن أمام حالتين، لنرَ قبل ان نفصل بالحالتين إن كان هناك شيء آخر يساعدنا ويخلصنا من احد الحالتين

نريد شيء يعطي دور 2أي أن $7^b$ يتكرر عند دور 2 (حتى نطبق المتطابقة $a^2 - b^2$) اي بالكتابة الرياضــية اريييد

$$7^2 \equiv 1\ mod \quad \text{(عدد نريده)}$$

$$48 \equiv 0\ mod \text{ (عدد نريده)} \Leftarrow$$

(بـالنسـبـة لـــ $3^a$ أيضـــاً لا شيء جـديـد فلو اردنـا ان تتكرر بـدور 2 لـدينـاا $8 \equiv (8 = 3^2 - 1$ $0 \bmod$ (عدد نريده)

لا جدييد .. حتى تجرب $mod7$ ...نلاحظ من انشـاء جدول البواقي ..ان $a$ يعطي بواقي مقبولة فقط عندما $a \equiv 0,2,4\ mod6$

اي ان $a$ حصرا زوجي ..وال $b$ هو الفردي

والان نسارع استثمار أن $a$ زوجي

حصرا $a = 2r$

$$7^b = (k - 3^r)(k + 3^r)$$

لكن القاسم المشترك الأكبر لهما $(k - 3^r)$ $2.3^r = k + 3^r$ لا يحوي 7 إذاً لايمكن ان يشترك القوسيين باي 7

$$k + 3^r = 7^b \qquad k - 3^r = 1$$

$2.3^r + 1 = 7^b$ تخلصنا من التربيع حالياً الآن لا يزال مسألة جديدة

من الواضح هنا ان $mod3$ محققة دوماا.. غالبا تترافق هذه الحالة بانه يجب ...ان تاخذ $mod9$ واكتب الجدول

لكن فقط تذكر انه قبل اخذ هذا الموود ناقش حالة $r = 1$ التي للعجب هي التي تعطي الحل

..الان بعد كتابة الجدول نلاحظ ان $b$ مضاعف ل3 ..اذا نكتب $b = 3c$ الان بالطبع نحلل

$$2.3^r + 1 = 7^{3c}$$

$$2.3^r = 7^{3c} - 1$$

$$2.3^r = (7^c - 1)(7^{2c} + 7^c + 1)$$

الان القاسم المشترك الاكبر للقوسيين نحسبه بتنويل المرتبة او اخذ القوس الايمن بموود الطرف الايسر ..نلاحظ انه يساوي 3 ... هذا اكثر من رائع اي ان القوسيين لا يمكن ان يشتركا باكثر من ثلاثة واحدة لا يجوز ان يتشاركا بـ9 وبالتالي احد القوسيين لن يحتوي اكثر من 6 ...اذا $c \leq 1$

وفي حال $c = 1$ نجد ان

$$2.3^r \neq 342$$

**مثال مشابه4:** أوجد $(x, y)$ تحقق المعادلة $7^x = 3^y + 4$

نفس المبدأ

## المقلوب في الـ $mod$

إذا كان $a$ باقي قسمة عدد على $n$ $(a \bmod n)$ و $(a,n) = 1$ عندها يوجد لـ $a$ مقلوب هو $\frac{1}{a}$ وهو يساوي $b$ (باقي صحيح آخر $b \bmod n$ )ويحقق

$$\frac{1}{a} = b \mod n$$

نضرب بـ $a$

$$ab \equiv 1 \mod n$$

ما هو إثبات وجود مثل هذا العدد $b$ ؟؟

إثباته يعتمد على **النظرية العظيمة** فلو أعطينا لـ $b$ كل البواقي الأولية $mod\ n$ عندها $ab$ من أجل $a$ معين وثابت ستعطي كل البواقي الأولية $mod\ n$ ومنها الـ 1 وبالتالي فهو موجود.

وأفضل ما في الأمر أن المقاليب تحقق الخاصية التجميعية والطرحية والضربية ...أي يمكننا أن نضربها ونرفعها للأس كما اعتدنا أن نعامل المقاليب في المساواة.

ما هو مقلوب 2 $(mod\ 7)$ وكيف نوجده

نبحث عن عدد $b$ يحقق

$$2b \equiv 1 \mod 7$$

بالتجريب نجد أنه 4 وبالتالي

$$\frac{1}{2} \equiv 4 \mod 7$$

وأيضاً:

$$\frac{1}{4} \equiv 2 \ mod \ 7$$

ما يهمنا من المقلوب هو أكثر من إيجاد قيمة المقلوب هو أنه يسهل العمل أيضاً في الـ $mod$.

**فمثلاً:**

$$a^{p-2} \equiv \frac{1}{a} \ mod \ p$$

مجرد إمكانية وجود المقلوب تساعد

فمثلاً إذا كان لدينا $(a,p) = 1$ و $p$ أولي

$$2a^2 \equiv 1 \ mod \ p$$

$$2 \equiv \frac{1}{a^2} \ mod \ p$$

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

$$b^2 \equiv 2 \ mod \ p$$

ما أثبتناه هو أن 2 هو باقي تربيعي $mod \ p$

فمثلاً إذا كان لدينا $(a,p) = 1$ و $p$ أولي

$$c^2 \equiv 3a^2 \ mod \ p$$
$$c^2 \left(\frac{1}{a}\right)^2 \equiv 3 \ mod \ p$$
$$(cb)^2 \equiv 3 \ mod \ p$$
$$k^2 \equiv 3 \ mod \ p$$

3 هو باقي تربيعي $mod \ p$

هذه الأمثلة ستواجهنا كثيراً في التمرينات لذلك يجب أن تصبح من البديهيات.

**مثال 1:**

أثبت وجود عدد غير صفري $n$ يحقق

$$a^n \equiv 1 \ mod \ p$$

من أجل أي عدد أولي $p$ و $(a,p) = 1$

بالطبع انه $n = p - 1$ وبالتالي هي تذكير اكثر من مسالة

**مثال 2:** أثبت أنه يوجد عدد طبيعي $n$ : $2^n + 3^n + 6^n - 1$ مضاعف لأي عدد أولي $p$ كان

**الحل:**

**نحاول إيجاد عدد متعلق بـ$p$ نضعه بدل إن فيصبح المقدار** $2^n + 3^n + 6^n \equiv 1 \ mod \ p$

$n = p - 1$ لا تجدي، ستعطي الطرف الايسر قيمة 3

الارقام 2,3,6 تذكرنا بأن $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$

ماذا إذاً؟

- لايمكننا ان نعوض $n = -1$ لانه عدد طبيعي ...ماالحل اذا هل نستطيع ان نستفيد من المعلومة السابقة القوية التي وكانها مفصلة تفصيلا للمسالة

هنا تخطر عبالنا فكرة الدورية وتكرار البواقي عدة مرات ...

وبالفعل اهم الدورات التي نعلمها هي عند ال $p - 1$

ماهي ال$-1$ بعد دورة كاملة .....بالضبط هي $-1$ من $p - 1$

اي نعوض $n = p - 2$ ....وهنا تظهر اهمية شرعية وصحة المقاليب في ال $mod \ p$

**مثال3:** إذا كانت $S$ مجموعة الأعداد $x > n$ التي تحقق أن

$$(x,n) = 1 \quad (x+1,n) = 1$$

أثبت:

$$\prod_{x\in S} x \equiv 1 \; mod \; n$$

**الحل:** بما أننا نريد الجداء 1 لذلك لابد لكل عدد من $S$ يرتبط بعنصر اخر من نفس المجموعة ..بحيث هذا الزوج يعطي نتائج جميلة في الجدااء الكبير...الان لندخل في صلب الحل

إذا كان $(x,n) = 1 \quad (x+1,n) = 1$

نعم لابد أن نفكر بالمقلوب بالـ $mod$

سنتوجه اذا مباشرة لاخذ b الذي يحقق $xb \equiv 1 \; mod \; n$ وأيضاً $(b,n) = 1$

ولكن هل نضمن ان هذا ال $b$ المنقذ ينتمي الى $S$ ...يجب ان يتحقق$(b+1,n) = 1$

اذا ماذا عن $b + 1$ ..

.تتذكر انك الى الان لم تستفد من كون $(x+1,n) = 1$ لكي تتوجه بتصرفاتك وتحول $b + 1$ بدلالة $x$

إن $b \equiv \frac{1}{x} \; mod \; n \leftarrow$

$$b + 1 = \frac{1}{x} + 1 = \frac{x+1}{x} \; mod \; n$$

ولكن $(x+1,n) = 1 \quad 1$ ....اذا $\left(\frac{1}{x} = b \; , n\right) = 1$ $(b+1,n) = 1$

إذاً إذا كان $x$ يحقق الخاصية عندها $b = \frac{1}{x}$ يحقق الخاصية أيضاً

وبالتالي في الجداء سيختصرون معا ونحصل على الجداء يكافئ 1.

**مثال 4:** أثبت وجود عدد $n \in \mathbb{Z}$ يحقق من أجل **أي** عدد أولي $p$

$$a^n \equiv n \; mod \; p$$

**الحل:**

سنستغل هذه المسألة لنعرض هذه الفكرة الخارقة:

يتعرض الأس في $mod\ p$ لـ $mod\ p-1$ بشكل صريح ودون لبس (فيرما) أي أننا نأخذ باقي الأس على $p-1$ ثم نعوضه مكان الاس القديم

لذا في هذه المسألة، $n$ ،مرة يخضع لـ $mod\ p$ على الطرف الأيمن للتكافئ

ومرة أخرى لـ $mod\ p-1$ في الاس على الطرف الايسر

وهذان مستقلان عن بعضهما لان $p, p-1$ اوليان فيما بينهما أي يمكن التحكم بالأثنين على مزاجك (يوجد $n$ يعطي أي باقي لـ $p$ مقابل أي باقي لـ $p-1$ لذا المسألة أصبحت سهلة )(تذكر عندما كنا ناخذ عدد ما بال $mod25$ و$mod4$ ومن ثم بكل ثقة نركبهم الى عدد يحقق كلا التكافئيين اي $mod100$

والان بالطبع سنختار $n$ بحيث يتحقق

$$n \equiv 1\ mod p$$

$$n \equiv 0\ mod\ p-1$$

وبالتالي الطرف اليسار سيكافىء $1 mod p$ بفضل فيرما ... والطرف الايمن ايضا يكافىء 1 وذلك بفضل اختيارنا لل $n$

المثال السابق محفز أو مدخل أو مثال عن النظرية المشهورة "**البواقي الصينية**"

**مثال 5:** لنتأمل المتتالية $a_0 = m$ حيث $m \in \mathbb{N}$

$$\forall\ k \in \{0, 1, 2 \dots\}\ a_{k+1} = na_k + 1$$

أثبت أن أول $m$ حد من المتتالية بعد $a_0$ لا يمكن أن تكون أولية كلها.

**الحل:**

أولاً نستنتج الصيغة العامة للمتتالية بخبرة جبرية من خلال اول بضعة حدود فنجد

$$mn^{m-1} + \frac{n^m - 1}{n-1}, \dots, \quad mn^3 + n^2 + n + 1, \quad mn^2 + n + 1, \quad mn + 1, \quad m$$

نريد عدد أولي $p$ يقسم على الأقل أحد هذه الحدود، ما هو هذا العدد يا ترى؟!!

دائماً نبدأ بالحالة الأســـهل: الأســـهل هو أن يكون هذا العدد الأولي $p$ يقســـم كلاً من جزئي العدد أي ($mn^{k-1}$ و $\frac{n^k-1}{n-1}$ ) لكي يقســـم الجزء $mn^{m-1}$ يجب أن يقســـم $m$ أو $n$ إذا قســـم $p$ $n$ فإنه عندها لن يقسم $\frac{n^m-1}{n-1}$ لذلك نفترض أنّ $p|m$.

الآن يجب أن نثبت وجود $k$ أصغر من $m$ بحيث $p|\frac{n^k-1}{n-1}$

نعم إنه $p-1$ وببساطة هو أصغر من $m$.

### مسألة عما سبق

أوجـد جميع الأعـداد الصـــحيحـة $n>1$ بحيـث أن أي عـدد أولي يقســـم $n^6-1$ يكون قـاســـماً لـ $(n^2-1)(n^3-1)$

**الحل:** هذه مسألة قوية وتحتاج إلى تفكير جيد وتركيز

نلاحظ أن $n^3-1$ هي موجودة ضـــمن $n^6-1$ وكذلك $n^2-1$ لذلك لا خوف من قواســـم الأولية لهما إذاً ممّا الخوف؟!! الخوف من $n^6-1$ وبـالضـــبط القســـم $n^3+1$ منهـا نلاحظ أن $n+1$ موجودة في $n^2-1$

ماذا عن $n^2-n+1$ أين ستكون أعدادها الأولية في $(n^2-1)(n^3-1)$

ماهي الطريقة الأفضل لمعرفة العوامل المشتركة بين عددين؟ نعم إنه القاسم المشترك الأكبر

$$(n^2-n+1,n^2-1)=(-n+2\ ,n^2-1)=(n-2,2n-1)=(n-2,3)$$

إذاً إن وجد عدد أولي مشترك بين $n^2-1$ و $n^2-n+1$ سيكون الـ 3

طريقة أخرى لحساب القاسم المشترك تكون ربما أقصر

نأخذ أولاً $d=(n^2-n+1,n-1)$ مباشرة نعوض $n=1$ كما تعودنا $d=(1,n-1)=1$

$$d=(3,n+1)\Leftrightarrow\ d=(n^2-n+1,n+1)$$ ثم

ماذا عن $n^3-1$ , مع $n^2-n+1$ إما أن نحســـب القاســـم بنفس الطريقة أو نتذكر أن $n^2-n+1$ كأن أصله $n^3+1$ وبالتالي القاسم هو 2 أو 1.

ولكن $n^2-n+1$ فردي بوضوح لذا القاسم المشترك الأكبر هو 1 (الـ 2 جاءت من $((n^3+1,n^3-1)$

إذا المهرب الوحيد لـ $n^2-n+1$ هو أن تكون تحوي فقط 3

كيف سنحل هذه المعادلة؟ ما هو أملنا الأول بالوصول إلى تناقض؟ $n^2-n+1=3^k$

ناخذ اولا $mod\ 3$ ...ولكن نلاحظ ان قيمة $-1$ وحدها تحقق التكافىء...اذا لضـعف $mod3$ ماذا سـنفعل بعدها

بالفعل $mod\ 9$ ومن اقوى دوافع التحوول لل$mod\ 9$ هو انه في $mod3$ وجدنا حلا وحيدا

وبالتجرييبب نهاية نجد ان $n^2-n+1$ لا تعطي 0 . ■

**ملاحظة:** يكفي تجريب $8,5,2$ لأنه حتى يكون $n^2-n+1$ مضـاعف للـــ 3 فقط يجب أن يكون $(n\equiv -1\ mod\ 3$.

الان لدينا مثال نستفيد ايضا من فكرة الخطي يعطي ولكن بطريقة خطيرة وجميلة

■

❖ مثال : أثبت أن من أجل أي أعداد $a,b,c$ صحيحة أكبر أو تساوي الصفر فإنه من أجل أي عدد صحيح أكبر من $2abc-bc-ca-ab$ يمكن كتابته بالشكل: $bcx+acy+abz$ حيث $x,y,z$ أعداد صحيحة غير سالبة:

الآن لنلاحظ الشكل الذي سيعطي الأعداد، ربما هو مخيف نوعاً ما، لكن هل يمكن تبسيطه؟ ... دائماً سنفكر أنه إذا لم أعرف ماذا يعطي مجهولان، كيف سأعرف ما يعطيه ثلاثة؟ ولكن كيف سأربط بين شكل الثلاث مجاهيل مع شكل المجهولين؟ فهنالك مربوط بـ $x,y$ كل من $a,b,c$، ولكن بالفعل:

$$bcx+acy+abz=c(bx+ay)+abz$$

نعم إنه شكل ظريف ، $bx+ay$ لابد $100\%$ أن نعرف عنه، ما هي القيم التي يعطيها يا ترى؟

بوضوح: $bx+ay=n$، الصعوبة في إيجاد الـ $x,y$، أو ما يصعب على $x,y$ أخذ أي قيمة ما هي قسمة $b$ أو $a$ طبعاً لنقل $b$:

$$y\equiv {}^{n}/_{a}\ modb \iff ay\equiv n\ modb$$

بإيجاد $^{n}/_{a}$ ستكون قيمة بين $0 \to b-1$، بالتأكيد سنجعل $y$ يأخذ هذه القيمة لمن نضيف أو نطرح $b$، إذاً أسوأ الحالات سيضطر $y$ أن يأخذ قيمة $b-1$ أي $y \le b-1$ لكي يحقق قسمة $b$.

إذاً إذا كان $n > ab-a$ فحتماً سنجد $y$ بحيث $n-ay$ موجب ومضاعف لـ $b$ وبالتالي نوجد $x$.

- لكن $ab-a$ غير متناظر، يدفعنا للفضول هل يمكننا تحسينه؟
- متى نخاف من أن يكون $n-ay$ سالب؟ ... عندما يضطر $y$ ليكون $b-1$،

ولكن $ay \equiv n \; mod b$ $\quad$ $a(b-1) \equiv n \; mod b$

$$\Longrightarrow n \equiv -a \; mod b$$

أي $n = ab-a$، في هذه الحالة مقبولة لأن $x$ سيأخذ $x=0$.

ننزل الـ $n$ الذي تحته $ab-a-b$ $100\%$ مرفوض لأن $x=-1$، وأما عن الأعداد $ab-a \leftarrow ab-a-b$ سيكون $y \le n-2$ وبالتالي لن تضطر $x$ أن تساوي $-1$.

إذاً يمكن لـ $ax+by$ أن يعطي كل الأعداد أكبر من $ab-a-b$.

الآن نعود لمسألتنا: $c(bx+ay)+abz$

هل خسرنا مجهولين بما فعلناه سابقاً؟ ... أم أننا خسرنا واحداً؟ ... نعم خسرنا اثنين وكسبنا واحداً ... ما هو؟ وما هي شروطه؟ (ما هو مقدار كيفيته؟)

إنه $ay+bx=t$، $t$ مجهول يعطي كل القيم أكبر من $ab-a-b$، لذا نجعل $t = ab-a-b+1+m$، والآن $m \ge 0$ ويعطي كل القيم.

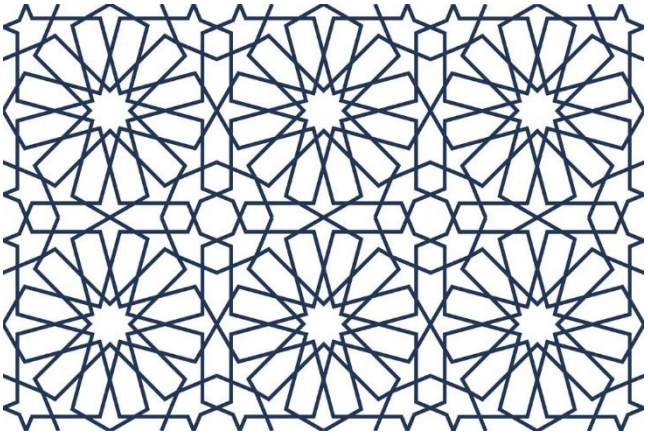
$$X = abc-ac-bc+c+\underbrace{mc+zab}$$

بالتأكيد سنطبق على المجهولين تماماً ما طبقناه، إذاً $X$ يعطي كل القيم الأكبر من

$$abc-ac-bc+c+abc-ab-c$$

$$= 2abc-ac-bc-ab$$

إذاً حصلنا على القيمة بالملي.



## نظرية البواقي الصينية

تخبرنا هذه النظرية بأنه يوجد عدد $x$ يحقق جميع المتطابقات (التالية)

$$x \equiv a_1 \ mod \ b_1$$
$$x \equiv a_2 \ mod \ b_2$$
$$\vdots \equiv \quad \vdots$$
$$x \equiv a_n \ mod \ b_n$$

بشرط أن تكون $b_1, b_2, \dots, b_n$ أولية مثنى مثنى.

بمعنى آخر أنه إذا كان العدد يكافئ 1 بالـــ $mod\ 3$ لا يمنع ذلك أن يأخذ أي باقي $mod\ 5$ ولا يؤثر منطقياً على باقي العدد $mod\ 7$

لـذلـك إن كنـا نـنـاقش $mod\ 30$ مثلاً فيمكننـا أن نـنـاقش $mod\ 3, mod\ 5, mod\ 2$ كلاً على حـدى إن اضطررنا لذلك، لأنه إذا وجدت الحلول لتلك المتطابقات يوجد حل لـ $mod\ 30$ .

تذكر كيف كنا نحســب باقي عدد ما على 100 من خلال باقيه على 25 و 4 وكلّنا على يقين من وجود عدد سيحقق كلا التطابقين ...هذه الثقة منشؤها هو نظرية البواقي الصينية.

**مثال:** أوجد عدد حلول المتطابقة:

$$(x-1)(x+1) \equiv 0 \; mod \; (n = p_1^{a_1} p_2^{a_2} \dots . p_k^{a_k} 2^r)$$

**الحل:**

هنا الحل متطابقة من الشـكل هذا: $mod$ كذا $x \equiv$ فالمعادلة في الأعلى هي تربيعية نريد حلولها كما في المعادلات النظامية.

$$p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} 2^r \mid (x-1)(x+1)$$

القوسان أوليان فيما بينهما إلا على 2 لذا كل قوة لعدد أولي فردي إما أن تدخل كاملاً إلى الأول أو الثاني

وكذلك الـ $2^r$ ولكن الفرق أن 2 ستدخل أحد القوسين و $2^{r-1}$ في القوس الآخر أيضاً حالتين، وبالتالي يوجد $2^{k+1}$ حالة.

ولكل من هذه التوزيعة ...**نظرية البواقي الصـينية** تضـمن لي $x$تكافئ 1 للجزء الأول وتكافئ -1 للجزء الثاني الأوليان فيما بينهما ماعدا الـــ 2 التي نضـمنها عندما يكون أحد $x+1, x-1$ مضـاعف ل $2^{r-1}$ سيكون العدد الآخر زوجي حتماً.

**برهان نظرية البواقي الصينية:**

1 $$x = b_1 k + a_1 \;\Leftrightarrow\; x \equiv a_1 \; mod \; b_1$$

نعوض في المعادلة الثانية المطلوبة

$$b_1 k \equiv a_2 - a_1 \; mod \; b_2 \Leftrightarrow \; b_1 k + a_1 \equiv a_2 \; mod \; b_2$$

بما أن $b_1$ أولي مع $b_2$ لذا يوجد حل $k$ $k = t b_2 + m$ نعوض في 1

$$x \equiv m b_1 + a_1 \; mod \; b_1 b_2 \;\Leftarrow\; x = t(b_1 b_2) + m b_1 + a_1$$

بتكرار ذلك $n$ مرة يتم المطلوب أو بالاســتقراء فقد أصــبح لدينا نظرية البواقي ولكن على $n-1$ عدد $\{\dots b_4, b_3, b_1 b_2\}$ نبرهنها على $n$ عدد.

ما زلنا سنستفيد كثيراً من هذه النظرية أو هذه الفكرة لاحقاً.

**والآن مسألة عامة عن كل ما تعلمته واكتسبته من خبرة**

أوجد جميع الأعداد $m , n$ بحيث أنه لأي $a \in \{1,2, \dots , n\}$ يتحقق

$$m|a^n - 1$$

**الحل:**

أول فكرة ستخطر هي أن $m$ أكبر من $n$ وإلا $a$ تمكن من أخذ $m$ فتصبح $m|m^n - 1$ وهذا مرفوض وضوحاً، بل أكثر من ذلك، يجب ألا يوجد أي شيء مشترك بين $m , a$ أذاً أي قاسم أولي $p$ لـ $m$ هو أكبر من $n$.

كما تعودنا الآن أننا أقوى في التعامل مع العدد الأولي وهو البنية الأساسية لـ $m$ لذا نناقش كل الـ $p$ $n \leq p$

نلاحظ أنه في المعادلة $a^n - 1 \equiv 0 \ mod \ p$ يوجد لدينا عدد من الحلول يساوي الأس فما دلالة ذلك

سنستخدم فكرة استخدمناها في مسألة إثبات أن عدد البواقي التربيعية هي $\frac{p-1}{2}$ .

- نعم هي نظرية أنه لكثير حدود من الدرجة $n , n$ جذراً على الأكثر ولكن كيف سنستخدمها؟!!
- كثير الحدود $P(a) = a^n - 1$ من الدرجة $n$ وله $n$ جذر إذاً المقاعد كلها محجوزة ولا يمكن لأي $a$ جديد أن يكون جذراً له لذلك بالضد سنبحث عن واحد.

أي الـ $a$ يمكن توقع ما سنختاره بسهولة، بالطبع هو $p - 1$ خارج $\{1,2, \dots , n\}$ (ماعدا حالة $p = n + 1$ نتركها حالياً)

$$(-1)^n - 1 \equiv 0 \ mod \ p$$

نجد أنه إذا كان $n$ زوجي أوجدنا الحل الجديد للمعادلة وهذا تناقض.

ولكن في حالة $n$ فردي يجب أن نبحث عن مناقشة جديدة

- الآن لو كنا أكثر تيقظاً للاحظنا أنه لو كان $n$ زوجي لكان $p - 1$ ليس وحده حلاً بل $p - 2$ و $p - 3$ ..... (علل)

وبماذا يوحي ذلك؟؟

يوحي قدرتنا على الانتقال من $x$ إلى $x-$ بفضل $1-$ غالباً على إمكانية أنه أي عددين عندها جداءهما هو حل (كيف نثبت ذلك؟).

الآن من المستحيل حصر جداءات العناصر $\{1,2, \dots n\}$ في المجموعة نفسها وذلك بسبب مناقشة بسيطة (لا تعقّد مناقشاتك في مثل هذه الحالات).

نعم إنها $\frac{n+1}{2}$ مع 2 حيث $n$ فردي، إذاً جداؤهما $(n+1)$ لذلك هو حل وبالتالي تناقض من جديد وبالتالي المهرب الوحيد هو أن تكون $n+1$ هي الـ $p$ (أي الحالة الخاصة التي تركناها).

إذاً $p = n + 1$

الآن استنتجنا أن أي عدد أولي في $m$ يجب أن يكون $p = n + 1$ هل أثبتنا أن $m$ عدد أولي الآن؟!!

لا كالعادة هو قوة لعدد أولي حيث $m = p^t , n = p - 1$

الآن من أجل $r = 1$ أي أولي واضح تحقق ذلك

$$p | a^{p-1} - 1$$

ولكن لو صعدنا بالدرجة قليلاً هل سيبقى ذلك صحيحاً.

- دون أن نتحمل عبئ $t$ كاملاً لنرى حالة $t = 2$ أولاً.

هل ممكن وجود $p$ بحيث $p^2 | \ a^{p-1} - 1$ لأي $a$ من 1 إلى $p - 1$

بالطبع نحاول بـ $p - 1$

$$p^2 | \ (p-1)^{p-1} - 1$$

علينا بمنشور نيوتن لأن هناك حدود ستطير لأنها تحمل $p^2$.

$$p^2 \underbrace{| \ 1 - (p-1)p}_{\text{ماتبقى من المنشور}} - 1$$

$$p^2 | \ (p-1)p$$

وبوضوح الآن حالة $t$ أكبر من 2 أيضا تناقض بنفس الطريقة.

إذاً $m = p \quad n = p - 1$

## المربعات والمكعبات

يمكننا الاستفادة كثيراً من المربعات والمكعبات غير تطبيق الـ $mod$ في حل معادلات نظرية الأعداد فمثلاً

- إذا كان $a^2 > n^2 \Leftarrow a^2 \geq (n+1)^2$

يعني إذا أردنا مربعاً أكبر من $n^2$ فهو أكبر أو يساوي المربع التالي

لو كان لدينا عدد عادي $b > n^2$ لا يمكننا القفز إلى المتراجحة القوية $b \geq (n+1)^2$

- المربع إذا أعطيته $p$ (عدد أولي) يعطيك $p^2$ أي إذا كان

$$pk = a^2$$

$p|a^2 \Leftarrow p|a$ لأنه $p$ موجود في البنية الأولية لـ $a$

$$\begin{aligned} a &= bp \\ \Rightarrow pk &= p^2b^2 \\ k &= pb^2 \end{aligned}$$

لنتدرب على هذه الأفكار بالأمثلة.

**مثال1**: أثبت أنه إذا كان $n$ عدد صحيح موجب وكان

$$2 + 2\sqrt{28n^2 + 1}$$

عدد صحيح فهو عندها مربع كامل.

**الحل:**

لكي يكون عدد صحيح عندها $28n^2 + 1$ يجب أن يكون مربع كامل.

$28n^2 + 1 = k^2$ والعدد المطلوب يصبح $2(k + 1)$ أي يجب إثبات $k + 1 = 2s^2$ من أجل عدد $s$ صحيح

قد يقول أحدهم $28n^2 = (k - 1)(k + 1)$

القوسان أوليان فيما بينهما وبالتالي الـ $n^2$ بشكل كامل في أحد القوسين فقط ولكن هذا هو عين الخطأ.

هذا الخطأ مشـهور لذا انتبه و $n$ فيها كثيرٌ من الأعداد الأولية كل منها يتوزع على أيٍّ من القوسـين ولذا كيف الحل ؟

وفقاً لما قلناه من قبل، جزء من أعداد $n$ الأولية في الأحد القوسين $a$ والباقي $b$

$$28a^2b^2 = (k - 1)(k + 1)$$

إذاً $a^2$ مربع كلها في $k + 1$ و $b^2$ كلها في $k - 1$ وهذه قاعدة هامة (إذا كان جداء قوسـين أوليين فيما بينهما مربع كامل عندها كل بينهما مربع كامل) تابع في الصفحة التالية (بعد المثال ٢)

**تمهيدية:** لو لم يكن القوسين أوليان فيما بينهما

$$ab = n^2$$

$$a = a'd, b = b'd \quad \leftarrow (a, b) = d \text{ ليكن}$$

$$a'b'd^2 = n^2 \quad \Leftarrow$$

$$\boldsymbol{d|n \Leftarrow d^2|n^2 \text{ عندما}}$$

**وهي نظرية هامة** أيضاً لاسـتنتاج صحتها نناقش الأعداد الأولية داخل العددين فـــ $d$ يحوي $p^{2a}$ و $n$ يحوي $p^{2b}$ يجب أن يكون $2a \leq 2b \Leftarrow a \leq b$ على كل الأعداد الأولية في $d$ مما يؤدي $d|n$.

$$n = n'd$$

$$a'b' = n'^2$$
$$a' = c^2 \quad b' = t^2$$
$$\Rightarrow a = dc^2 \quad b = dt^2$$

■

إذاً الـ 4 في 28، 2 في $k+1$ و 2 في $k-1$ أما الـ 7 لها حالتين نناقشهما:

الحالة الأولى:

$$k-1 = 2b^2 \quad k+1 = 14a^2$$
$$14a^2 - 2b^2 = 2$$
$$7a^2 - b^2 = 1$$

نلاحظ أن هذه الحالة لا تحقق الشرط المطلوب الذي يجب أن نبقي عيننا عليها، لذا علينا نقض هذه الحالة غالباً طريقة النقض هي الـ $mod$ وبالفعل هنا الحالة الـ 7 $mod$ تنقض.

أما الحالة الثانية:

■ $k-1 = 14b^2, \quad k+1 = 2a^2$ عندها يتحقق المطلوب.

**تمهيدية:** أثبت أنه إذا كانت كتابة العدد الصحيح $n$ بعوامله الأولية كما ياتي

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

عندها يكون

$$T(n) = (a_1+1)(a_2+1)\dots(a_k+1) \Leftarrow$$

حيث $T(n)$ هو عدد قواسم العدد $n$.

**الإثبات:** لكي يكون العدد قاسماً لـ $n$ يجب أن تكون قوى جميع أعداده الأولية أصغر أو تساوي قوى العدد $n$ لذا فالعدد الأولي $p_i$ لقوته $a_i + 1$ احتمالاً لأننا نعد القوة صـفر أيضـاً ...وحسـب المبدأ الأسـاسي في العدد فان عدد طرق تشكيل قاسم لـ $n$ هي

$$(a_1+1)(a_2+1)\dots(a_k+1)$$

وهو المطلوب.

**مثال2**: أوجد جميع الأعداد الطبيعية $n$ بحيث

$$T(n)^4 = n$$

$T(n)$ هو عدد قواسم وله قانون وسنتعمق به لاحقاً.

**الحل:**

إذا كان:

$$T(n) = (a_1 + 1)(a_2 + 1) \dots (a_k + 1) \Leftarrow n = p_1^{a_1} p_2^{a_2} \dots . p_k^{a_k}$$

الآن إلى المسألة بتطبيق القانون طبعاً

$$(a_1 + 1)^4 (a_2 + 1)^4 \dots (a_n + 1)^4 = p_1^{a_1} \dots . p_k^{a_k}$$

الطرف الأيسر قوة لـ 4 لذا 4 تقسم $a_k$ كلها ونضع $a_i = 4b_i$

$$(4b_1 + 1)(4b_2 + 1) \dots (4b_k + 1) = p_1^{b_1} \dots . p_k^{b_k}$$

كما تعلمنا في الجبر أن** . . . . $4b_i + 1 < p_i^{b_i}$ ستحقق قريباً جداً (لأن الزعيم هو الحد الذي فيه المجهول في الأس أكبر من الحد الذي فيه المجهول كأساس).

من أجل $p_i > 5$ تتحقق دائماً، $p = 3$ تتحقق بدءاً من عند $b_1 = 3$ $p = 5,,,,,,$ تتحقق بدءاً من عند $b_1 = 2$.

البرهان بسهولة استقراء والآن يبدو أن المسألة أصبحت سهلة ولكن كيف نختمها؟!!

أولاً لا يمكن أن يوجد $p = 2$ لأن الطرف الأيسر فردي، هذه الملاحظة قاضية ... نرتب الأعداد الأولية وفقاً لدليلها( نرتبها بحيث العدد الاولي ذو الدليل الاكبر هو العدد الاكبر. الآن إذا كان:

ليكن$p_1 = 3$ إذا وضعت $b_1 = 2$ لا نستطيع وضع إلا $p_2 = 5$ $b_2 = 1$ وإلا رجحت الكفة تماماً للطرف الأيمن ....ولكن ايضا في هذه الحالة لا تتحقق المساواة

وإذا وضعت $b_1 = 1 \Leftarrow 4b_1 + 1 = 5$ لذا $p_2 = 5$

إذا كان $b_2 = 1$ عندها $4b_2 + 1 = 5$ وتختصر مع $p_2 = 5$ وتبقى $4b_1 + 1 = 5$ على الطرف الأيمن لا تصريف لها لذا $b_2 \geq 2$ نبرهن بالاستقراء أن $5(4b_2 + 1) < 3.5^{b_2}$

بالدمج مع ** للأعداد الأولية $p_i$ من أجل $i \geq 3$ نجد أن الكفة ترجح تماما للطرف الأيمن

اذا نجعل $p_1 = 5$ وتكون $b_1 = 1$ وهذا يكون الحل الوحيد

**مثال 3:** أوجد جميع الثلاثيات $(a, b, c)$ أعداد صحيحة موجبة بحيث:

$$a^2 + b + c \qquad b^2 + a + c \qquad c^2 + a + b$$

جميعها مربعات كاملة.

**الحل:**

$$a + b \geq 2c + 1 \Leftrightarrow c^2 + a + b \geq (c + 1)^2 \text{ لذا } c^2 + a + b > c^2$$

وبالمثل $b + c \geq 2a + 1, c + a \geq 2b + 1$

بالجمع نصل للتناقض.

**مثال 4:** أوجد $(x, y)$ أعداد **صحيحة** بحيث

$$x^2 + 3y \quad , \quad y^2 + 3x$$

مربعات كاملة

نفس الفكرة حاول فيها

**مثال 5:** ربما هذا المثال **أقل علاقة بالمربعات والمكعبات** لكن له صـــلة كبيرة بتوزيع **القوة** – هنا قوة العدد 2

هل يوجد للمعادلة التالية حل

$$(36a + b)(36b + a) = 2^k$$

حيث $a, b$ أعداد صحيحة موجبة

**الحل:**

(جداء قوسين قوة لـ 2 إذاً كل منهما قوة لل 2)

**(لنعرف قوة الـــ 2 في مجموع حدين، هي قوة الحد الأصغر وأما إذا تساوت القوتين عندها لا تستطيع معرفة قوة المجموع لأنه بعد إخراج القوة المشتركة سيكون هناك مجموع حدين لا نعرف كم قوة للـــ 2 ستعطي)** (لذا إذا أردت لمجموع حدين أن يكون قوة لـ 2 يجب أن **تتساوى** القوة في الحدين).

لا بد أن المسألة انتهت. الآن فكر بحل بطرق أخرى بطريقة خاصة بك.

## مسائل قسمة متطورة

هذه المسائل أصعب من المسائل التي استعرضناها في المقدمة بالتأكيد سيكون فيها أكثر من مجهول فهي خليط ذكي من المتراجحات وبعض التقنيات في المقدمة وبعض التناظر وبعض شـــؤون القاســـم المشترك الأكبر وقد يوجد حركة خاصة بكل مسألة.

تنتج المتراجحة $b \geq a$، من $a|b$ إذا كان $a, b$ موجبان أو $|b| \geq |a|$ بشكل عام.

$$x|y$$
$$x|ay - bx$$

ملحوظة عند ضرب $y$ بعدد $a$ ربما يضعف ذلك من قوة (القسم) إذا كان $a$ غير أولي مع $x$.

بمعنى آخر يجب أن يكون $a$ ضرورياً جداً لنضرب به حيث سيتوجب التأكد في النهاية لأنه ربما يحقق الحل $(x, y)$ العلاقة $x|ay$ ولكن ليس $x|y$.

ربما ناقشنا هذا الأمر تفصيلاً من قبل والآن أكدنا عليه.

ويمكن الاستفادة من التناظر بفرض $x \geq y$ والاستفادة من ذلك في المتراجحات أما القاسم المشترك الأكبر فهي إذا كان $(c, b) = 1\ ,\ c|ab$ عندها $c|a$ أي نتخلص من $b$ إذا كان لا يشترك بشيء مع $c$ وبالتالي نقلل حجم المتراجحة.

**مثال 1:** أوجد $a, b$ أعداد صحيحة موجبة بحيث

$$\frac{a^2+b}{b^2-a} \ , \ \frac{b^2+a}{a^2-b} \text{ أعداد صحيحة}$$

**الحل:**

بدون المس بعمومية المسألة نفرض أن $a \geq b$

يجب أن يكون من الكسر الأيمن:

$$b^2+a \geq a^2-b \Leftrightarrow b^2+b \geq a^2-a \Leftrightarrow (a-b)(a-b-1) \geq 0$$

إما $a=b$ أو $a \geq b+1$ في هذه الحالة وبما أن $x^2-x$ متزايدة عالموجب بديهياً ومنه

$$b^2+b \geq a^2-a \geq (b+1)^2-(b+1)$$

نلاحظ المساواة في هذه الحالة إذا $a=b+1$ أي أول كسر يساوي 1 مقبول ولكن ماذا عن الكسر الآخر؟ سنعالجه ببساطة كما كنا نفعل في بداية الكتاب.

وإذا كان $a \geq b+2$ نصل لتناقض فوري اذاً نناقش $a=b$

$$\frac{2}{a-1} \leftarrow \frac{a+1}{a-1} \leftarrow \frac{a^2+a}{a^2-a}$$

من الملحوظ في مسائل القسمة أن المقام لا يتغير.

إما $a-1=2 \quad a=3$

أو $a-1=1 \quad a=2$

**مثال 2:** هنا تبدأ زيادة الصعوبة ويبدأ الفهم **العميق** للقسمة.

إذا كان $m! + n! \mid m! \cdot n!$ حيث $m, n$ أعداد صحيحة موجبة.

أثبت أن $3m \geq 2n + 1$

**الحل:**

بفرض $m \leq n$ نختصر على $m!$

$$1 + (m+1)(m+2) \cdots n \mid n!$$

لاحظ الـ $n$ موجودة مرتين هذا رأساً يوحي بالشك أن $n$ أولية مع اليسار لذا لن تفيده يمكنها أن تطير

$$1 + (m+1) \ldots . (n-1)n \mid (n-1)!$$

ولكن بعد ذلك سننتبه أنّ $n$ ليست وحدها في هذا الموقف

هناك أكثر من $n$ كل منها نختصره من اليمين

$$1 + (m+1) \ldots . (n-1)n \mid m!$$

والآن الفكرة الأكثر قوة، لاحظ أننا كنا نبحث عن شيء موجود إلى جانب الـــ 1 لنقول عنه أنه سيكون أولي مع اليسار إذا ماذا هناك أيضاً؟!!

$(m+1) \cdots\cdots (n-1)n$ هو جداء $n - m$ عدد لذا هو مضاعف لـ $(n-m)!$ سيطر من اليمين،

الآن بالطبع نريد بعد اختصار $(n-m)!$من $m!$ أن يبقى أكبر من اليسار

نطبق متراجحة إذاً ونقضي على المسألة.

**مثال 3: (IMO)** أوجد $m, n$ أعداد صحيحة موجبة بحيث $\frac{n^2+m}{nm-1}$ عدد صحيح.

**الحل:**

لا يمكننا فرض $m \geq n$ حالياً ولكن يوجد فرصة طالما المقام متناظر لو استطعنا أن نحصل على البسط المناظر.

1 $$nm-1 | n^2+m$$

نضرب البسط بـ $m$

$$nm-1 | m^2+n^2m$$
$$nm-1 | m^2+n(nm)$$
$$nm-1 | m^2+n$$

1 نفرض أن $m \geq n$ ولكن لدينا حسب

$$n^2+m \geq nm-1$$
$$n^2+1 \geq m(n-1)$$

$n = m$ أو $n+1$ لا تعطي تناقض أما بعدها فتنقلب المتراجحة لذا نناقش الحالتين:

$$\frac{2}{n^2+n-1} \quad \frac{n^2+n+1}{n^2+n-1}$$

$$\frac{1}{n-1} \leftarrow \frac{n}{n-1} \leftarrow \frac{n^2+n}{n^2-1}$$

إذا $n-1=1$ أي أن $n=2$

**مثال 4:** أوجد $(l,m,n)$ أعداد صحيحة موجبة

$$\text{عدد صحيح} = (l+m+n)\left(\frac{1}{l}+\frac{1}{m}+\frac{1}{n}\right)$$

**الحل:**

بما أنها متجانسة إذاً (درجة البسط نفس درجة المقام)، نختصر القاسم المشترك الأكبر للأعداد الثلاثة

$$3+\frac{m+n}{l}+\frac{n+l}{m}+\frac{l+m}{n}$$

أول محاولة أن نأخذ القاسم المشترك بين اثنين ونثبت أنه يقسم الثالث عندها نصل لتناقض وعندها كله أوليان فيما بينهما مثنى مثنى.

ولكن هذه ليست حالتنا هنا أصعب، سنأخذ القاسم المشترك الأكبر بين كل عددين مثنى مثنى أي
$a=(l,n)\ \ b=(l,m)\ \ \mathrm{c}=(\mathrm{m},\mathrm{n})$

$$l=abl' \qquad m=bcm' \qquad n=can'$$

$l', m', n'$ أولية فيما بينها مثنى مثنى.

وبما أن $(l,m,n)$ كما في الأعلى يساوي واحد لذا $(b,n')=1$ لا يمكن لأنه لـ $n$ أن يشترك بشيء مع الشيء المشترك بين $l, m$

والآن وداعاً لـ $l, n, m$ والتعامل مع الـ 6 مجاهيل الجديدة.

$(a,m')=1, (c,l')=1$ الآن استفد من كل هذه الأشياء لتطيير الكثير

أولاً خذ قسمة $l'$ وأثبت أنه $l' \mid am'+bn'$

والآن خذ قسمة $c$ وأثبت أنه $c \mid am'+bn'$ وبما أنهما أوليان فيما بينهما أي $cl' \mid am'+bn'$ وهنا تبدأ تصلنا الاشارات الحجمية بأنه لو أثبتنا المعادلتين المناظرات سيبدأ حجم المقام يصبح قريباً جداً على البسط

أثبت الـ 2 الأخريان $am' \mid cl'+bn'$ $\quad bn' \mid cl'+am'$ واختم المسألة.

وهذه الطريقة كثيرة الاستخدام ونستخدمها قريباً في قسم using perimeters-diophantine equations وذلك للتخلص من العامل المشترك الذي يمكن أن يوجد في جميع المجاهيل وبأخذ أي قيمة وخاصة في المعادلات متجانسة (لا درجة ذاتها في جميع الحدود).

**مثال 5:** $(\boldsymbol{Apmo})$ أوجد جميع الأعداد $n$ بحيث:

$$\frac{n^2+1}{\lfloor\sqrt{n}\rfloor^2+2} \text{ عدد صحيح}$$

**الحل:**

قد تظهر أنها مسألة بمجهول واحد ولكنها عملياً ليست كذلك، سنرى أننا نحتاج إلى تحسين المظهر والتخلص من الجذر حتى نستطيع التعامل، إذا أردنا كتابة $\lfloor\sqrt{n}\rfloor = k$ ما هي صفات $k$ ؟؟

$$(k+1)^2 > n \geq k^2$$

ولكي نربط $n$ بـ $k$ نقول

$$n = k^2 + s \quad \text{حيث} \quad 2k \geq s$$
$$\frac{(k^2+s)^2+1}{k^2+2} \rightarrow \frac{(s-2)^2+1}{k^2+2}$$

والآن الطريقة الجديدة، كنا نقول فقط $(s-2)^2+1 \geq k^2+2$ ولكن يمكننا حقيقة أن نقول

$$(s-2)^2+1 \geq 4(k^2+2)$$

ولكن هذه المتراجحة ستصل بنا لتناقض مع $2k \geq s$

حيث اذا تحققت المتراجحتين سيكون لدينا $(2k-2)^2+1 \geq 4(k^2+2)$

$$-3 \geq 8k$$

تناقض بالفعل

وأن نناقش حالة 3,2,1 منفصلاً

- حالة تحقق المتراجحة أي ناتج القسمة أكبر أو يساوي 4 عندها

$$(2k-2)^2+1 \geq (s-2)^2+1 \geq 4(k^2+2) \quad \text{تناقض}$$

- **حالة 1:** $(s-2)^2 - k^2 = 1$ سهلة
- **حالة 2:** $(s-2)^2 = 2k^2+3$

كيف سننقض هذه الحالة؟؟ لاحظ أننا لدينا مربعين.

نعم $3\ mod$ يقتضي كون كل منهما $0\ mod\ 3$ وهي مربعات لذا ستصبح $0\ mod\ 9$ وهذا التناقض لا تكافئ $0\ mod\ 9$ .

**حالة 3:** $(s-2)^2 = 3k^2 + 5$

$3\ mod$ تناقض أسرع حيث لا يوجد مربع يكافئ $2\ mod\ 3$

**مثال 6:**

أثبت أن المعادلة:

$$\frac{1}{10^n} = \frac{1}{(n_1)!} + \frac{1}{n_2!} + \frac{1}{n_3!} \dots \frac{1}{(n_k)!}$$

ليس لها حلول صحيحة بحيث $n_k > \cdots n_2 > n_1 \geq 1$:

للوهلة الأولى تبدو وكأنها ليست نظرية أعداد، فقد تعودنا على الأكثر وجود كسر واحد ... فعلاً كلام سليم وهذا ما يدفعنا بثقة للتخلص من المقامات، التخلص منها بسيط، فقط اضرب بالكبير، إذاً:

$$\frac{(n_k)!}{10^n} = \frac{(n_k)!}{(n_1)!} + \frac{(n_k)!}{(n_2)!} + \cdots + (n_{k-1}+1) \dots n_k + 1$$

$$\frac{(n_k)!}{10^n} = \underbrace{(n_1+1) \dots n_k + (n_2+1) \dots n_k + \cdots + (n_{k-1}+1) \dots n_k}_{A} + 1$$

بهذا الشكل لابد وأنك أحسست بالمشكلة في هذه المعادلة ... نعم إنها الـ 1 من أجل القسمة على $n_k$، فجميع الحدود على اليمين $A$ تحوي $n_k$ حتماً، أما اليسار فالاعتماد عليه في إنقاذ الـ 1، بالفعل:

$n_k = 2^a \cdot 5^b$ حيث $a, b \leq n$ ... اي لايسمح لها باعداد اولية اخرى

لكن لنعرف اكثر عن $n_k$ هل الـ 2 والـ 5 معاً حصراً في $n_k$؟ أم أحدهما؟ أم ما هو المقبول لـ $n_k$؟

نفرض أن $a, b > 0$ عندها $A$ تحوي الـ 2 والـ 5،، هنا حدث امر جميل .. انه الطرف الأيمن ككل لا يحوي كليهما، إذاً يترتب على $10^n$ أن تخطف كل الـ 2 والـ 5 من $(n_k)!$ دون زيادة ((لأنه عندها $\frac{(n_k)!}{10^n}$ ليس صحيحاً)) ودون نقصان لأن الطرف الأيمن لا يستقبل 2 أو 5.

إذاً: $n = v_5(n_k)$ و $n = v_2(n_k)$

وهذا التناقض واضح لأن $v_2(n_k) > v_5(n_k)$، فما أن يخطف $10^n$ كل الـ 5 من العاملي سيفيض الـ 2 فيه.

وبسبب هذه المشكلة التي هي $v_2(n_k) > v_5(n_k)$

لا يجب أن يحوي $n_k$ أي 2، وبالتالي **الطرف الأيمن يستقبل الـ 2** الفائض من العاملي، والـ $10^n$ تخطف دون زيادة ونقصان الـ 5 في العاملي، إذاً:

$$v_5((n_k)!) = n \qquad n_k = 5^a$$

الآن لنطمئن على مصير الـ 2 الفائض ... $n_k$ لم يعد مهدداً في موضوع ال2، ولكن هل هو لوحده بالاساس كان مهددا؟ ... هنالك أيضاً $n_{k-1}$ موجود في كل حدود $A$، وسيكون زوجياً حتماً ... هنالك طريقة وحيدة لعدم تواجد $n_{k-1}$ في اخر حد على اليمين من A وهي أن يكون $n_{k-1} = n_k - 1$.

وبالتالي الاخر حد على اليمين في $A$ يصبح ببساطة $n_k$

والحد الذي يليه على يساره سيحوي $n_k(n_k - 1)$ حتماً، إذاً $n_k - 1$ موجودة في هذا الحد وكل الحدود على يساره وفي $\frac{(n_k)!}{10^n}$ دون قوة الـ 2 التي فيه، إذاً يجب أن يكون موجوداً في $n_k + 1$، إذاً

$$\frac{n_k - 1}{2^S} \mid n_k + 1$$،

ولكن $(n_k - 1, n_k + 1) = 2$ تناقض

## نظرية ويلسون

تنص النظرية على أن:

$$(\boldsymbol{p-1})! \equiv -\mathbf{1}\ \boldsymbol{mod\ p}$$ حيث $\boldsymbol{p}$ عدد أولي

**الإثبات:**

ذكرنا من قبل أنّ أي باقي بالـ $mod\ p$ له معكوس ضربي (مقلوب) وهذا الباقي يكون مختلفاً عن معكوسه الضربي إلا في حال $x$ معينة فلنحددها:

$$x \equiv \frac{1}{x}\ mod\ p$$

$$x^2 \equiv 1 \; mod \; p$$
$$x^2 - 1 \equiv 0 \; mod \; p$$
$$(x-1)(x+1) \equiv 0 \; mod \; p$$

إما $x \equiv 1$ أو $x \equiv -1$ عند هاتين القيمتين يكون معكوسها الضربي هو نفسه.

لذلك في الجداء $(p-1)!$ يوجد $1, -1$ وأزواج من الأعداد جداءها واحد (العدد ومقلوبه) وبالتالي

$$(p-1)! \equiv -1 \; mod \; p$$

ملاحظة: لهذه النظرية استخدامات محدودة نوعاً ولكنها ستفيدنا قريباً في العديد من الحالات التي يوجد فيها ضرب العديد من البواقي.

**مثال 1:** هل يمكن أن يكون $(a_1b_1, a_2b_2, \dots, a_{p-1}b_{p-1})$ بواقي كاملة $mod \; p$ إذا علمت أن $(a_1, a_2, a_3, \dots, a_{p-1})$ و $(b_1, b_2, b_2, \dots, b_{p-1})$ متسلسلتي بواقي كاملة كل منهما على حدا؟

تذكر مجموعة البواقي الكاملة هي $\{1,2,3, \dots, p-1\}$ المتسلسلة هي كل هذه الأرقام بترتيب معين.

والذي يبقى ثابتاً، دائماً السؤال الأقوى في معظم المسائل ما الذي يبقى ثابتاً في سلسلة البواقي الكاملة مهما اختلف الترتيب؟!

جداء كل الأعداد، مجموع كل الأعداد، مجموع مربعات كل الأعداد والكثير الكثير .....

**مثال 2:** إذا كانت $(a_1, a_2, \dots, a_{p-1})$ -حيث $p$ عدد أولي- مجموعة بواقي كاملة ما هو أكبر عدد ممكن من البواقي التي تعطيها المتتالية

$$\{ia_i\}_{i=1}^{i=p-1}$$

**الحل:**

هذا التمرين أكثر تشويقاً، سنفرض في البداية أن $\{ia_i\}_{i=1}^{i=p-1}$ ستعطي كل البواقي ثم سنصل للتناقض، ولكن كيف نصل للتناقض؟

بالفعل لو ضربنا كل العناصر $ia_i$ يجب أن يكون الناتج $-1$ حسب ويلسون ولكن الجداء هو عبارة عن جداء جميع البواقي مرّتين مرة في $a_i$ ومرة في $i$ وهنا التناقض (لأن جداء جميع البواقي مرتين هو $+1$)

والآن هنا الإبداع البحث عن المتسلسلة التي تعطيك $p-2$ أي 2 متساويين فقط.

$a_i = i^2 \ mod \ p$ ليست بواقي كاملة

$a_i = i \ mod \ p$ أو أي شيء خطي عند التعويض في $i$ $a_i$ سيصبح تربيعي ولن يعطي $p-2$ باقي

$mod \ p$ ثابت $a_i \equiv$ لا تعطي كل البواقي طبعاً.

$a_i \equiv \frac{1}{i} \ mod \ p$ ليست بالضبط.

لا بد من التلاعب قليلاً هنا نريدها كسرية ولكن دون أن يذهب البسط مع المقام.

$a_i \equiv \frac{1}{i+1} \ mod \ p$ ولكن ماذا عن $a_{p-1}$ ((فلا يجوز أن نعطيها قيمة $\frac{1}{p}$ أي $p$ في المقام دون وجود بســـط مضاعف لـ $p$) فنعطيها الباقي المتبقي طبعاً وهو 1

أثبت أنها تحقق المطلوب أي أن

$\{ia_i\}_{i=1}^{i=p-1}$ الـ

تعطي كلها بواقي مختلفة عدا الـ $p-1$. ■

**مثال3:** أوجد جميع الأعداد الطبيعية $k, m$ التي تحقق:

$$k! + 48 = 48(k+1)^m$$

**الحل:**

أولاً 48 يقسم $k!$ إذاً $k \geq 6$ ونختصر على 48 هذه خطوات منطقية وابتدائية.

$$720 \cdot \frac{k!}{720} + 48 = 48(k+1)^m$$
$$15\ \frac{k!}{720} + 1 = (k+1)^m$$

والآن إلى أفكار أقوى.

الآن إن اســتطعنا تجزئة $k+1$: ســنلاحظ تداخل الحدين $15\ \frac{k!}{720}$ و $(k+1)^m$ في الأعلى الذين فرقهما واحد واللذين يجب ألا يتداخلا، فأي عامل في الجزئيين أكبر أو يســاوي 7 موجود في $\frac{k!}{720}$ (تذكر وجود الـــ 1 الذي يجعل $k+1$ أولي مع $k!$)

5 أو 3 موجودة في 15 وبالتالي يسمح لـ $k+1$ أن يحوي فقط 2 والآن بعد صفنة قصيرة

نلاحظ أن $\frac{k!}{720}$ ما أن يتجاوز الـــ 7 حتى يحوي 2 من جديد إذاً $k = 7$ وحدها الممكنة نعوضــها (حالة $k = 6$ تجعل $k+1$ عدد أولي وبالتالي غير قابلة للتجزئة):

$$105 + 1 \neq 8^m$$

إذاً $k+1$ يجب أن يكون عدداً أولياً أي $k! = (p-1)!\ ,\ k+1 = p$

يبدو لي أن المسألة قد انتهت هنا

نعم سنطبق ويلسون على الأصلية نجد أن $p$ يقسم 47 إذاً $p = 47$

وبالتعويض نجد التناقض الواضح.

إذاً لا يوجد حلول المسألة.....

**الان سـندخل في اعمااق نظرييية الاعداد وسـنبدا بمواضـييع اقوى لتقوينا في مواجهة مسـالة ثانية او خامسة**

بالنسـبة للموضـوع التالي مباشرة ،هو للعقول الكبار .. في حال شـعرت بالعجز في هذا الموضـوع تجاوزه للموضوع التالي ص93 ثم عد اليه فيما بعد

الم نستخدم في مسائلنا الكثير من اعداد مختلفة$mod$ .....وكثيرا ما اوجدنا جداول المربع الكامل بالنسبة لكل موود منهاا.. وربما لاحظنا او لم نلاحظ بعض الظواهر في نتائج الجدول ..سـنتعرف الى بعضـها الان وكاننا نتعرف الى ما وراء كواليسـها ..لان هذه الخفايا سـتفيدني في حل عدد لا باس به من المسـائل المتقدمة

- **قواعد في الـ $mod$**
  - لا يمكن أن نجذر في علاقة الـ $mod$

أي إذا كان $a^2 \equiv b^2 \ mod \ n$ هذا لا يعني $a \equiv b \ mod \ n$

ما نفعله هو $a^2 - b^2 \equiv 0 \ \ mod \ n$

$$(a-b)(a+b) \equiv 0 \ mod \ n$$

إذا $n$ تتوزع على القوسـين $a+b \ , a-b$ لو جذرنا لكنا أهملنا دور $a+b$ وشـلفنا المسـؤولية كلها على $a-b$

- ما هي البواقي المربعة $mod \ 5$ هي (ماعدا الصفر)

$$1, -1$$

$mod \ 7$ هي (ماعدا الصفر)

$$1, 2 \ ,4$$

$11\ mod$ هي (ماعدا الصفر)

$$1, 3, 9, 5, 3$$

إذاً إن المربع لا يعطي كل البواقي وإذاً ما عدد البواقي التي يعطيها الـ $p\ mod$

ربما نشعر بأن عددها $\frac{p-1}{2}$ وذلك بملاحظة الأمثلة: كيف نثبتها؟؟

الآن كيف نحصل على البواقي التربيعية عادةً مربع كل البواقي

$$1^2, 2^2, 3^2, 4^2, \dots . \left(\frac{p-1}{2}\right)^2, \left(\frac{p+1}{2}\right)^2, \dots, (p-1)^2$$

لكن

$$\frac{p-1}{2} \equiv -\left(\frac{p+1}{2}\right) \quad p-2 \equiv -2 \quad p-1 \equiv -1\ mod\ p$$

لذا النصف الثاني مكرر الآن نثبت أن النصف الأول ($\frac{p-1}{2}$ باقي) كلها مختلف

نفرض $x$ و $y$ عددين مختلفين أصغر من $\frac{p-1}{2}$ يحققان

$$x^2 = y^2\ mod\ p$$

$$(x-y)(x+y) \equiv 0\ mod\ p$$

إما $x \equiv y$ مرفوض

أو $x \equiv -y$ مرفوض في النصف الأول.

وبالتالي انتهى الإثبات.

### الآن نناقش متى يكون $-1$ باقياً تربيعياً في $p\ mod$

نلاحظ بوجوده في $(mod\ 3, mod\ 5)$ وعدم وجوده في $(mod\ 7)$

نضع

$$a^2 \equiv -1\ mod\ p$$
$$a^2 + 1 \equiv 0\ mod\ p$$

لنناقش الشكل $a^2+1$ مطولاً.

**النظرية تقول:**

من أجل عدد أولي $p$ $(3\ mod\ 4)$ لا يوجد $a$ تحقق $p|a^2+1$

ومن أجل عدد أولي $p$ $(1\ mod\ 4)$ يوجد دائماً $a$ يحقق $p|a^2+1$

**بصياغة أخرى:** (أي قاسم أولي لـ $a^2+1$ هو من الشكل $1\ mod\ 4$ ولا يمكن أن يكون $3\ mod\ 4$)

**الإثبات:**

- لنثبت أولاً أنه لا يمكن لعدد أولي $3\ mod\ 4$ أن يقسم $(a^2+1)$ بنقض الفرض.

$$p|\ a^2+1$$
$$a^2 \equiv -1\ mod\ p$$

إذا أردنا الاستفادة من مبرهنة فيرما نرفع العلاقة السابقة للأس $\frac{p-1}{2}$.

$$1 \equiv a^{p-1} \equiv (-1)^{\frac{p-1}{2}}\ mod\ p$$
$$\Rightarrow \frac{p-1}{2} \quad \text{زوجي}$$
$$p \equiv 1\ mod\ 4 \quad \text{إذاً}$$

- لنثبت ثانياً أنه لأي عدد أولي $p \equiv 1\ mod\ 4$ يوجد $a$ يحقق $p|\ a^2+1$.

لدينا حسب ويلسون.

$(p-1)! \equiv -1\ mod\ p$ لنكتب $(p-1)!$ على شكل مربع

$$\left(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right)\left(\frac{p+1}{2} \cdot \ldots \cdot (p-1)\right) \equiv -1 \ mod\ p$$

$$\left(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2}\right) \cdot \ldots \cdot (-1) \equiv -1 \ mod\ p$$

$$(-1)^{\frac{p-1}{2}} \cdot \left(1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}\right)^2 \equiv -1 \ \ mod\ p$$

$$\text{زوجي} \frac{p-1}{2}$$

$$\Rightarrow \left(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right)^2 \equiv -1 \ mod\ p$$

وبالتالي يوجد $a$ يحقق المطلوب.

## دراسة الشكل $a^2 + b^2$

**إذا وجد عدد أولي $p \equiv 3 \ mod \ 4$ يحقق $p|a^2 + b^2 \Rightarrow p|a, b$**

لنفرض أن $p$ لا يقسمهما كليهما الآن:

$$a^2 + b^2 \equiv 0 \ mod \ p$$
$$a^2 \equiv -b^2 \ mod \ p$$

نقسم $b \neq 0 \ mod \ p$

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

$k^2 \equiv -1 \ mod \ p$ تناقض (حسب النظرية السابقة)

إذاً $p|a, b$ عندها $a = pa_1 \ \ b = pb_1$ ونلاحظ عندها

$$a^2 + b^2 = p^2(a_1^2 + b_1^2)$$

$p^2$ بقوة زوجية ستكون حصراً في الشكل $a^2 + b^2$

الآن من أجل عدد أولي $p \equiv 1 \ mod \ 4$ من الواضح وجود $a \ , b$

$$p|a^2 + b^2$$

ولكن ما نريد أن نثبته **الآن هو وجود $a \ , b$** بحيث $a^2 + b^2 = p$ من أجل أي عدد $p \equiv 1 \ mod \ 4$

نأخذ $u$ بحيث

$$u^2 \equiv -1 \ mod \ p$$
$$x^2 + 1 \cdot y^2 \equiv x^2 - u^2y^2$$
$$\equiv (x - uy)(x + uy) \ mod \ p$$

لنثبت وجود أعداد $-\lfloor\sqrt{p}\rfloor \leq x, y \leq \lfloor\sqrt{p}\rfloor$ تحقق $x - uy \equiv 0 \ mod \ p$

نعوض كل الأزواج $(x, y)$ بحيث $0 \leq x, y \leq \lfloor\sqrt{p}\rfloor$ في $x - uy$

لاحظ اننا أخذنا الموجب فقط على $x$ و $y$ (سنعلم بعد قليل لماذا)

عندها نعلم أن $\lfloor\sqrt{p}\rfloor^2 < p$

إن لم تحقق أي منها $x - uy \equiv 0 \ mod \ p$ على الأقل يوجد زوجين يحققان:

$$x_1 - uy_1 \equiv x_2 - uy_2 \ mod \ p$$
$$(x_1 - x_2) - u(y_2 - y_1) \equiv \quad 0 \quad mod \ p$$

$-\lfloor\sqrt{p}\rfloor \leq x_1 - x_2, y_2 - y_1 \leq \lfloor\sqrt{p}\rfloor$ يحققان المطلوب مع $\underbrace{x_1 - x_2}_{X}$ , $\underbrace{y_2 - y_1}_{Y}$

$$\Rightarrow \ X^2 + Y^2 \equiv 0 \ mod \ p$$

ولكن

$$0 < X^2 + Y^2 < 2p$$
$$\Rightarrow X^2 + Y^2 = p$$

الآن لنترك الـ $1-$ ونناقش البواقي التربيعية بشكل عام

إذا كان لدينا باقيان تربيعيين فإن جداؤهما تربيعي $\underbrace{b_1 b_2}_{(mk)^2} \Leftarrow \underbrace{b_1}_{k^2}, \underbrace{b_2}_{m^2}$ تربيعي

$$bc \Leftarrow \underbrace{b}_{\text{تربيعي}} , \underbrace{c}_{\text{غير تربيعي}}$$ غير تربيعي

لو كان $m^2 \equiv bc$ عندها $c \equiv \left(\frac{m}{k}\right)^2$

وأيضاً:

$$c_1 c_2 \Leftarrow \underbrace{c_1, c_2}_{\text{غير تربيعي}}$$ تربيعي

**لإثبات آخر خاصية نستعرض طريقتين:**

إذا كان $b$ باقي تربيعي عندها $b^{\frac{p-1}{2}} \equiv +1 \ mod \ p \ \Rightarrow b \equiv a^2 \ mod \ p$ وذلك حسب فيرما

الآن $X^{p-1} \equiv 1 \ mod \ p$

$$\left(X^{\frac{p-1}{2}}-1\right)\left(X^{\frac{p-1}{2}}+1\right)\equiv 0\ mod\ p$$

الآن لو نظرنا لـ $X^{\frac{p-1}{2}}-1$ ككثير حدود (لذلك كتبت $X$).

إن لـ $X^{\frac{p-1}{2}}-1$ جذر على الأكثر (لأنه من الدرجة $\frac{p-1}{2}$) ولكن جميع البواقي التربيعية $b$ تحقق أنها جذور له وعددها $\frac{p-1}{2}$.

إذاً بقية البواقي (الغير تربيعية) $c$ هي جذور لـ $X^{\frac{p-1}{2}}+1$.

$$c^{\frac{p-1}{2}}\equiv -1\ mod\ p$$

وبضرب عنصريين يحققان هذا نحصل على 1 بدل $-1$ وهذا يثبت النظرية.

**الطريقة الثانية** (فقط لتوسيع الأفق في نظرية الأعداد)

نريد أن نعرف جداء باقيين غير تربيعيين لمَ لا ندرس جداء جميع البواقي مع نفسها

بمعنى آخر عناصر جداء المجموعتين

$$\{1\ ,2,3,\dots,p-1\}\times\{1\ ,2,3,\dots,p-1\}$$

نلاحظ أنّ أي باقي يتكرر نفس العدد من المرات لذا عدد البواقي التربيعية يساوي عدد البواقي غير التربيعية. أي عدد البواقي الغير التربيعية هو $\frac{(p-1)^2}{2}$

ولكن إذا أخذنا باقي تربيعي من الأولى وغير تربيعي من الثانية $\left(\frac{p-1}{2}\right)^2$ طريقة نحصـــل على باقي غير تربيعي

وإذا أخذنا باقي غير تربيعي من الأولى وتربيعي من الثانية بـــ $\left(\frac{p-1}{2}\right)^2$ طريقة نحصل أيضاً على باقي غير تربيعي

وبالمحصلة $\frac{(p-1)^2}{2}$ باقي غير تربيعي وهي العدد الكلي لها

إذاً جداء باقيين غير تربيعي هو باقي تربيعي

الفكرة السابقة هي التجانس أو التعادل أو تكافؤ الفرص أو أن أي عدد من المجموعة$\{1, 2, 3 \dots . , p-1$ لا يتميز عن غيره.

فكرة يجب أن نشعر بها ونلاحظها دائماً لأنها ستفيدنا كثيراً.

**والآن أصبح لدينا خبرة في الـ $mod$ لذا لا بد من مثال قوي في التعامل بالـ $mod$ وأكثر من ذلك**

**المسألة**: ليكن لدينا عدد صحيح موجب $d$ ولتكن $S$ مجموعة كل الأعداد الصحيحة الموجبة التي تكتب بالشكل $x^2 + dy^2$ حيث $x, y$ أعداد صحيحة غير سالبة

1. أثبت أنه إذا كان $b$ ينتمي لـ $S$ و $a$ أيضاً ينتمي لـ $S$ عندها $ab$ كذلك ينتمي لـ $S$
2. أثبت أنه إذا كان $t$ ينتمي لـ $S$ و $p$ أيضاً بحيث يكون $p|t$ عندها $\frac{t}{p} \in S$ حيث $p$ عدد أولي

**الحل:**

1. إذاً ليكن $a = x^2 + dy^2$ و $b = m^2 + dn^2$ ويكون $ab$ (هنا سنستخدم نفس أسلوب ومتطابقة عندما كان $d = 1$)

$$ab = (m^2 + dn^2)(x^2 + dy^2) = m^2x^2 + m^2y^2d + n^2x^2d + d^2n^2y^2$$
$$= m^2x^2 + 2mxdny + d^2n^2y^2 + m^2y^2d + n^2x^2d - 2mxdny$$
$$= (mx + dny)^2 + d(my - nx)^2 \quad \blacksquare$$
$$= (mx - dny)^2 + d(my + nx)^2 \quad \text{أو بطريقة أخرى}$$

2. الآن الطلب يبدو أنه نفس فكرة 1) ولكن أقوى فهو **بالاتجاه المعاكس** ليكن $p = a^2 + db^2,\ t = m^2 + dn^2$ ولدينا $p|\ m^2 + dn^2$ الآن سنستخدم معلومة أن $p|\ a^2 + db^2$ رغم غرابتها نعم أو بكتابة أخرى $a^2 \equiv -db^2 \ mod\ p$ وذلك لمعرفة موقع $d$ بالنسبة لـ $p$ حيث لاحظنا أنها موجودة بالقسمين $m^2 \equiv -dn^2 \ mod\ p$.

إذاً $d = -\frac{a^2}{b^2} \ mod\ p$ نعوض بالعلاقة الأخرى

$$m^2 \equiv \frac{a^2n^2}{b^2} \ mod\ p$$
$$m^2b^2 - a^2n^2 \equiv 0 \ mod\ p$$
$$(mb - an)(mb + an) \equiv 0 \ mod\ p$$

الآن أحد القوسيين على الأقل فيه $p$.

والآن بعد أن أوجدنا هذا العلاقة التي ترتبط كل الأعداد ببعضها في الـ $mod\ p$ التي سنستفيد منها حتماً ولكن نحتاج إلى فكرة أخرى قوية تدخلنا في عمق المسألة.

خطتنا هي أن نقول لو فعلاً كان صـحيحاً لتوجب حدوث الفرض عندها (من مبدأ ما معقول تكون المسـألة خاطئة) وهي استراتيجية قوية جداً كأنك تقول (أخي من الأخير شو بدك بالضبط).

المتطابقة المستخدمة هي

$$(a^2+db^2)(x^2+dy^2) = (ax+dby)^2 + d(ay-bx)^2$$
$$= (ax-dby)^2 + d(ay+bx)^2$$

إذاً إذا وجد عددين ما $x, y$ بحيث

$$m = ax - dby$$
$$n = ay + bx$$

يتحقق المطلوب

ولاحظ هنا أخذنا الشكل الأول.. هنالك شكل ثاني للمتطابقة

لكي نعرف إمكانية وجود هذه الـ $x, y$

ما هو الشيء الذي قد يمنع وجودهما؟! هو عدم الانتماء للأعداد الصحيحة فقط ولا وجود لمشكلة اخرى..

ولنعرف إذاً $x, y$ ستكون صحيحة، ببساطة نعزلهم

$$y = \frac{an-bm}{a^2+db^2} = \frac{an-bm}{p}$$

هذا عدد صحيح تذكر من الصفحة السابقة آخر ما توصلنا إليه هو أحد احتمالين

إذا كان $p \mid bm-an$ عندها $y$ صـحيح وإذا كان $p \mid bm+an$ عندها نسـتخدم الشـكل الثاني للمتطابقة ونحصل على ذات النتيجة أن $x, y$ يكونان صحيحان ويحققان

$$(a^2+db^2)(x^2+dy^2) = m^2+dn^2$$

وهو المطلوب.

- لاحظ لو كان $d=1$ لكان الموضوع أسهل وذلك لأن أي عدد أولي يقسم $t=m^2+n^2$ سيكون من الشكل $p=x^2+y^2$ ومن قاعدة الجداء **نركب** كل الأعداد الأولية الباقية غير $p$ (نركبهم بمعنى أن نجعل جداء عددين من الشـكل $x^2+dy^2$ إلى عدد واحد من الشـكل ذاته) باستخدام المتطابقة في الأعلى لـلوصول لـ $t$ ما عدا $p$ الذي قسمنا عليه. فنحصل على عدد يكتب

بنفس الشكل أيضاً (بالاستقراء طبعاً)

■

**مسألة ثانية:**

أوجد جميع **الأعداد $n$** الصحيحة الموجبة التي من أجلها يوجد عدد صحيح $m$ يحقق $2^n - 1 \mid m^2 + 9$

**الحل:**

أول ما سنلاحظه في مسألة كهذه هو أن الطرف الأيمن هو عبارة عن مجموع مربعين وبالتالي سنحاول استغلال هذه النقطة بأن نبحث عن الحالات التي يعطي من أجلها $2^n - 1$ عدد أولي $3 \ mod \ 4$ ولكن أيضاً نلاحظ أن $m^2 + 9$ قد يحوي $3^2$عندما $m = 3m'$ أيضاً قد تعيق العمل قليلاً.

الآن نبدأ بتجريب بعض الأرقام $n = 1$ مقبولة

ونلاحظ أن $2^n - 1$ عند $n \geq 3$ سيكون $3 \ mod \ 4$ وبالتالي يجب أن يوجد عدد أولي $3 \ mod \ 4$ فيه ولكن وحده المقبول هو 3 (أما بقية القواسم فستكون $1 \ mod \ 4$ )وبالتالي يجب أن يكون $2^n - 1$ مضاعف لـ 3 إذاً $n$ زوجي وبالتالي $n = 2k$ الآن هل سنتوقف عندها أم هنالك شيء يخطر لنا لنتابعه؟!! $2^{2k} - 1 = (2^k - 1)(2^k + 1)$ بتطبيق نفس المناقشة على $k$ إما أن يكون زوجي أو 1 من هنا نستنتج أن $n = 2^t$.

الآن بتجربة الكثير من الأمثلة نلاحظ أن $n = 2^t$ محققة، بقي أن نثبت أنها محققة بمعنى أنه من اجلها يوجد $m$ يحقق:

$$2^{2^n} - 1 = \left(2^{2^{t-1}} - 1\right)\left(2^{2^{t-1}} + 1\right)$$
$$= 3(2^2 + 1)(2^4 + 1)(2^8 + 1) \ldots\ldots \left(2^{2^{t-1}} + 1\right)$$

تذكر من الفكرة التي استخدمناها قبل قليل وذلك لكي يكون عدد من الشكل $t^2 + n^2$ يكفي أن يكون كل أعداده الأولية من الشكل $1 \ mod \ 4$ عندها من متطابقة الجداء تركب أعداده الأولية مع بعضها.

ونعم نستنتج أن كل أعداده الأولية $1 \ mod \ 4$ بسهولة وذلك لأن: كل قوس هو عبارة عن مجموع مربعين.

وبالتالي اقتربت من أن تنتهي المسألة حيث نحصل بعد تركيب جميع الأعداد الأولية على $(\mathrm{t}')^2 + (\mathrm{n}')^2$ الآن ستشعر بالصعوبة لأننا لا نستطيع حساب $t'$.

وبالتالي لا نستطيع حساب الـ $m$ ولكن نتذكر أنها غير مطلوبة فيرتاح قلبنا.

**ملحوظة:** كان بالإمكان دون أن نقحم فكرة الأعداد الأولية أن نســتخدم المتطابقة الخاصــة بالجداء مباشرة على الأقواس $(2^{2^i}+1)$ ونركب الأقواس مع بعضها.

والآن لم ننتهي

علينا أن نحول $(m')^2+(n')^2$ إلى **الشكل** $x^2+1$

هل هناك ما نضربه به حتى يتحول إلى هذا **الشكل** (شعور تأنيب الضمير بأنك كبرت العدد وضخمته مرات عدة يجب أن **يختفي** تماماً) بالتأكيد سنركبه مع مجموع مربعين آخرين.. لمَ لا!

$$((m')^2+(n')^2)(x^2+y^2)=(m'x+n'y)^2+(m'y-xn')^2$$

علينا إيجاد $x,y$ بحيث $m'y-xn'=1$

الشرط الوحيد لوجود ذلك هو $(m',n')=1$

وهذا سهل إثباته (كيف تتوقع) تذكر من أين نحن جئنا بالـ $n',m'$ نثبت الأولية بنفس الطريقة

بالاستقراء أثناء الجداء نعم

■

**الآن الموضوع الاخر لكي نتابع في أعماق نظرية الأعداد:**

هناك شيء سنلاحظه أثناء ذلك.

سيزداد اعتمادنا على الأعداد الأولية ومثلاً قد تكون المسألة على الــ $n$ فتتفاجأ بأنني استدعي عدد أولي من $n$ الأصغر مثلاً أو الأكبر والذي يحقق خاصية ما.

لماذا؟!! لأن الأعداد الأولية هي وحدة لا تتجزأ وهي أصــغر وحدة ولأنه ينطبق عليها قواعد لا تنطبق على غيرها.

والآن نستعد لدخول القسم الثاني المتقدم من الكتاب بالتوفيق.

لنرى بعض هذه النظريات الآن بعد هذه المسألة في المقدمة

**مثال 1:** أثبت أنه من المستحيل أن يكون

$$n| \ 2^n - 1$$

**الحل:**

نختار **أصغر** عدد أولي في $n$ وليكن $p$ عندها

$$p| \ 2^n - 1$$

ولكن لدينا النظرية التالية المهمة جداً في السياق

## نظرية 1:

$p$ عدد أولي، إذا تحقق $p|a^b - 1$ , $p| \ a^c - 1$ عندها $p|a^{(b,c)} - 1$

**الإثبات:**

كيف ذلك؟ خذ هذا المثال. لدينا مثلاً علاقتي القسمة التاليتين نستنتج منهما

$p|a^{17} - 1 , p|a^5 - 1$ بضرب القوة بـ 3 $p|a^{15} - 1$ وبطرحها ومن الأولى نجد $p|a^{17-15} - 1$

ومنها $p|a^2 - 1$ ومن الأخيرة ومن القوة 5 معها نجد $p|a^{5-2*2} - 1$ ومنها $p|a^1 - 1$.

وصلنا للواحد الذي هو **القاسم المشترك الأكبر** وبالأصل هذه طريقة الوصول للقاسم المشترك الأكبر لأي عددين (الطريقة الاقليدية).. اذاً هذا كان إثبات معنوي وليس رسمياً ...الرسمي هو بتطبيق خوارزمية اقليدس (والتي طبقناها عمليا في مثالنا العددي).

صراحةً نستخدم هذه النظرية دائماً عندما نحصل على $d$ يحقق $p|a^d - 1$ لأن $p|a^{p-1} - 1$ أي أن أس الـ $a$ يتكرر عند الـ $p - 1$ لذا نريد معرفة وضع $d$ بالنسبة لها **(نهاية الـ *lemma* )**

بالعودة للمسألة:

إذاً $p|2^{(n,p-1)}-1$

ولكن $n$ لا تحوي أي شيء من $p-1$ لأن أصغر عدد أولي في $n$ هو $p$ وأي عدد أولي في $p-1$ أصغر من $p-1$ إذاً $p|2^1-1$ تناقض.

## نظرية 2: Lifting the exponent (LTE)

مهمتنا في هذا البحث معرفة قوة عدد أولي $p$ الموجودة في $x^n-y^n$ **حيث $p$ موجودة $p|x-y$.**

وهذا الشرط $p|x-y$ ضروري جداً للنظرية التالية التي سنستعرضها وهذا الشرط يبعدنا عن التفكير بالنظرية السابقة $q|\frac{x^p-1}{x-1}$ والتي تعطي صفة لـ $q$.

**الآن نص النظرية**: إذا كان $p|x-y$

تكون قوة $p$ الموجودة في $x^n-y^n$ هي القوة الموجودة في $x-y$ مضافاً إليها القوة الموجودة في $n$

أو بمعنى آخر أن $\frac{x^n-y^n}{x-y}$ يحوي قوى من الـ $p$ فقط بمقدار ما يحوي $n$ من قوى للـ $p$ (تخيل ذلك أي أنّ الـ$n$ الذي هو أس ويضخم الحد كثيراً لا يستطيع أن يعطي قوى للـ $p$ إلا أن يحتويها هو نفسه)

أو بالترميز

$$v_p(x^n-y^n)=v_p(x-y)+v_p(n) \quad \text{حيث} \quad p\geq 3$$

حيث الرمز $v_p$ هو أكبر قوة موجودة في العدد.

**الإثبات**: سيكون الإثبات على **خطوات**، هذه الخطوات هامة للفهم لأنها تستعرض مبادئ تعامل أساسية مثل الخطوة الأولى سنستخدمها في برهان نظرية أخرى والخطوة الثالثة سنعرض طريقة للقفز من الباقي على $p$ إلى $p^2$ والآن اتركك مع الإثبات:

### 1 الخطورة الأولى:

إثبات إذا كان $(t,p)=1$ عندها

$p \nmid \frac{x^t-y^t}{x-y}$ لا ننسى الشرط الوحيد $p|x-y$

الاشارة $\nmid$ تعني لا يقسم

نفرض أنّ

$$p|\frac{x^t-y^t}{x-y}$$
$$p|x^{t-1}+y.x^{t-2}\ldots+y^{t-1}$$

وبما أنّ $x \equiv y \ mod \ p$

$$\Rightarrow p|t.x^{t-1}$$

وهذا تناقض.

**2 الخطوة الثانية**

$p||\frac{x^p-y^p}{x-y}$ أي أكبر قوة فيها هي 1

صراحة هنا الخطوة التي تكررت معنا مسبقاً وهي فحوى النظرية

إثبات أن $p|\frac{x^p-y^p}{x-y}$ سهل لأن

$$\frac{x^p-y^p}{x-y}=x^{p-1}+y\cdot x^{p-2}+y^2\cdot x^{p-3}\ldots+y^{p-1}\equiv px^{p-1}\equiv 0 \ mod \ p$$

هنا نلاحظ أنّ المقدار يكافئ $p\cdot x^{p-1}$ بالـ $p \ mod$ ولكننا وما زلنا لا نعرف طبيعته بالـ $p^2 \ mod$ سندرس $mod \ p^2$

الآن ونثبت أنه لا يكافئ $0 \equiv mod \ p^2$

إن $x=y+pt$ لأن $p|x-y$

نعوض الآن

$$\frac{x^p-y^p}{x-y}=\frac{(y+pt)^p-y^p}{pt}$$
$$=\frac{y^p+p\cdot y^{p-1}\cdot(pt)+\binom{p}{2}\cdot y^{p-2}(pt)^2+\cdots-y^p}{pt}$$

باقي الحدود الغير مكتوبة تحوي $p^3$ وعندما نختصر على $pt$ يبقى $p^2$ وبالتالي تطير بالـ $mod\ p^2$ عندما $p \neq 2$ $p|\binom{p}{2}$ وبالتالي أيضاً $\binom{p}{2}y^{p-2}(pt)^2$ يطير

يبقى:

$$\frac{x^p - y^p}{x - y} \equiv p.y^{p-1}\ \ mod\ p^2$$

اذاً تحوي $p$ واحدة فقط.

**3 الخطوة الثالثة:**

$$p^n \| \frac{x^{p^m} - y^{p^m}}{x - y}$$

$$\frac{x^{p^m} - y^{p^m}}{x - y} = \frac{\left(x^{p^{m-1}}\right)^p - \left(y^{p^{m-1}}\right)^p}{x - y}$$

$$= \left(\frac{x^{p^{m-1}} - y^{p^{m-1}}}{x - y}\right)\left(\frac{a^p - b^p}{a - b}\right)$$

حيث $a = x^{p^{m-1}}\ b = y^{p^{m-1}}$

هذا القوس الأيمن يحوي $p$ واحدة فقط وبالتالي بتكرار العملية نجد $\frac{x^{p^m} - y^{p^m}}{x-y}$ تحوي فقط $p^m$

**الخطوة الرابعة:**

ليكن لدينا $t$ حيث $(t, p) = 1$

$$p^m \| \frac{x^{tp^m} - y^{tp^m}}{x - y}$$

$$\frac{x^{tp^m} - y^{tp^m}}{x - y} = \frac{(x^t)^{p^m} - (y^t)^{p^m}}{x - y} = \frac{x^t - y^t}{x - y} \cdot \frac{(x^t)^{p^m} - (y^t)^{p^m}}{x^t - y^t}$$

وبالتالي من الخطوة الثانية والثالثة:

$$p^m \| \frac{x^{tp^m} - y^{tp^m}}{x - y}$$

وبالتالي أكتمل الإثبات

ماذا عن 2 إذا وجدت في $n$ عندها السؤال سيكون:

ما هي قوة الـ 2 الموجودة في $x^{2^n} - y^{2^n}$ حيث $x, y$ فرديان:

$$x^{2^n} - y^{2^n} = (x-y)(x+y)(x^2+y^2)\cdots\left(x^{2^{n-1}} + y^{2^{n-1}}\right)$$

نلاحظ أن هذه الأقواس لا تخالف الخطوة الثانية فهي لا تحوي أكثر من 2 وذلك حسب $mod\ 4$ ولكن يبقى $x+y$ الذي يمكن أن يحوي 4 أو أكثر من قوى الـ 2

إذاً $x^{2^n} - y^{2^n}$ تحوي ما يحويه $x-y$ إضافة لـ $(n-1) + x + y$

ولكن الملحوظة أن فقط واحد من $x+y\ ,\ x-y$ يمكن أن يحوي أكثر من 2 لأن

$$gcd(x-y, x+y) = 2$$

وبالتالي إذا كان $4|x-y$ أو أكثر تصبح مطابقة للنظرية السابقة حيث يضطر $x+y$ أن يأخذ 2 فقط وحصراً

العدد 2 أقل استخداماً ولكنه يبقى مهماً.

**وتتحقق نفس النظرية على $x^n + y^n$ إذا كان $n$ فردي**

الآن لنواجه بعض الأمثلة:

**المثال1**: أوجد أكبر قوة لـ 1991 في

$$1992^{1991^{1990}} + 1990^{1991^{1992}}$$

**الحل:**

اولاً نعلم أن 1991 هو أولي لذا المسألة وكأنها توجهنا نحو النظرية السابقة

ولكن أولاً يجب أن نجعل الأسس متساوية – التعامل مع أس الأس ليس صعباً مطلقاً- على اليمين 1990 مرفوع للأس 1991 ,,,1992مرة لذا ندخل اثنتين منها إلى العدد على الأرض فيصبح $1990^{(1991)^2}$)$^{1991^{1990}}$ فنحصل على نفس الأس (هذه العملية ليست صعبة نفس مبدأ $3^{25} = ((3^5)^5 = 3^{5^2})$

$$1992^{1991^{1990}} + \left(1990^{(1991)^2}\right)^{1991^{1990}}$$

$$v_p(x^n + y^n) = v_p(x + y) + v_p(n)$$

هنا $p = 1991$ $x = 1992, y = 1990^{(1991)^2}, n = 1991^{1990}$

من الواضح أنّ

$$, v_{1991}(n) = 1990$$

$$v_{1991}(x + y) = v_{1991}\left(1992 + 1990^{(1991)^2}\right)$$

ولكن

$$x + y = 1991 + \left[(1990)^{(1991)^2} + 1\right]$$

ما داخل القوس تحوي 3 من 1991 (تطبيق سريع لـ$LTE$...لهذه الدرجة من البديهية )

لذا المقدار ككل يحوي 1991 واحدة.

**مثال 2: لنحاول حل هذه المسألة**

أوجد جميع الأعداد $n$ الطبيعية الموجبة بحيث $\frac{2^n+1}{n^2}$

**الحل:**

يوجد حلول كثيرة لـ $n|2^n+1$ على عكس $n|2^n-1$ و $n^2|2^n+1$

لنرَ الأخيرة

لنأخذ أصغر عدد أولي $p$ يقسم $n$

$$p|2^{2n}-1 \Leftarrow p|2^{(2n,p-1)}-1 \Leftarrow p|2^n+1$$
$$p|2^2-1 \quad p=3$$

إذاً عرفنا أن أصغر عدد أولي في $n$ هو 3 ولكن لم نستفد كثيراً

ماذا عن $q$ العدد الأولي الأصغر الموجود في $n$ وأكبر من 3 أيضاً

$$q|2^{(2n,q-1)}-1$$

هنا اختلف الموضوع فكلاهما $n$ , $q-1$ قد يحتوي على "3 ات بلاوي"

إذاً لو عينّا كم 3 تحوي $n$ أي إذا قلنا: إن $n$ تحوي $3^a$ أي $3^a||n$ عندها حسب $LTE$ فإن $2^n+1$ تحوي $a+1$

$n^2$ تحوي $2a$ يجب أن يكون $2a \leq a+1 \Leftarrow a \leq 1 \Leftarrow a=1$

إذاً القاسم المشترك الأكبر في الأعلى حيث وقفنا هو إما 3 أو 1 وذلك حسب $q-1$ لا يهم فسنناقش الحالتين

إما $q|2^2-1 \quad q=3$ مرفوضة لأننا قلنا أنّ $q \geq 3$

أو $q|2^6-1 \quad q|63 \Leftarrow q=7$

**هنا يجب التنويه** لأمر **هام** دائماً يتكرر عندما نطبق **النظرية 1**

هو أنه **قد نبدأ بـــ** + أي $p|2^n+1$ نضرب بـــ 2 الأس لنحصل على سالب $p|2^{2n}-1$ لذا الحل الذي نحصل عليه في النهاية قد يحقق $p|2^{2n}-1$ ولكن لا يحقق $p|2^n+1$ الأصـــلية لذلك علينا التعامل مع ذلك كما في الأعلى.

لو كان $q|2^3-1$ عندها برفع للقوة الصحيحة $\frac{n}{3}$ نجد $q|2^n-1$ وهذا تناقض.

إذاً $q|2^3+1$ هذه الحالة الوحيدة **وكأننا نعيد سحب الـ 2 التي أعطيناها بداية**.

**المثال الثالث**:

أوجد ثنائيات $(n,p)$ حيث $p$ عدد أولي و$n$ عدد طبيعي $n^p|\ (p-1)^n+1$

**الحل:**

إما $n=1$ وهي حالة مقبولة مهما كانت $p$

أصغر عدد أولي يقسم $n$ هو $q$.

$$q|(p-1)^n+1$$
$$q|(p-1)^2-1 \Leftarrow q|(p-1)^{(2n,p-1)}-1 \Leftarrow q|\ (p-1)^{2n}-1$$

كما قلنا نرفض أحد الحالات وذلك وكأننا نعيد سحب الـ 2 التي وضعناها والحالة الاخرى:

$q|(p-1)+1 \Leftarrow q=p$ أي أن $p$ من قواسم الـ$n$.

إذاً يوجد على الأقل $p$ من $p$ $(p^p)$على اليسار هل يوجد الكمية المناسبة على اليمين؟!!

لنحسب كم $p$ يوجد في كلا الطرفين على فرض $n$ تحوي $a$ من $p$

حسب النظرية $\rightarrow ap \leq a+1$

هذا تناقض إذاً لا يوجد حلول.

**السؤال الرابع:**

$b \in \mathbb{N}$ أثبت أنه لا يمكن أن تكون جميع القواســـم الأولية الموجودة في $b^p - 1$ نفســـها الموجودة في $b - 1$ (حيث $p > 3$ عدد أولي)

**الحل:** لنفرض العكس على سبيل الجدل عندها

$$b^p - 1 = (b-1)(b^{p-1} + b^{p-2} + \cdots + b + 1)$$

إذاً فإن جميع الأعداد الأولية الموجودة في $b^{p-1} + b^{p-2} \ldots . b + 1$ موجودة في $b - 1$

الآن يمكن أن نأخذ القاســـم المشـــترك الأكبر كما اعتمدنا أن نفعل في مثل هذين التركيبين (إثبات النظرية)

$$(b^{p-1} + b^{p-2} + \cdots + b + 1\,, b - 1)$$
$$= (p, b-1)\ |p$$

إذاً العدد الأولي الوحيد الذي يمكن أن يكون مشتركاً هو $p$

إذاً $\frac{b^p-1}{b-1} = p^a$ ولكن بما أن $p|b-1$ و $2 \neq p$

حسب $LTE$ أكبر قوة لـ $\frac{b^p-1}{b-1}$ هي واحد

$$\frac{b^p - 1}{b-1} = p \Leftarrow$$

وهذا تناقض لأن $\frac{b^p-1}{b-1} > p$ بوضوح

وكالعادة نختم العمل بتناقض تراجحي، وإن هذا النمط من العمل يتكرر كثيراً.

ستصبح من المسلمات عندما نأخذ القاسم المشترك الأكبر لـ

$$\left(b^r + 1 \quad \text{أو حتى} \quad \left(\frac{b^r - 1}{b-1}, b-1\right)\ |r\right)$$

حيث $r$ عدد أولي.

**السؤال الخامس:**

إذا كان $a^m + 1 \mid (a+1)^n$ أثبت أن $m = 1$

**الحل:**

$$a^m + 1 \mid (a+1)^n$$

$$\frac{a^m + 1}{a+1} \mid (a+1)^{n-1}$$

لن نستفيد من القسمة السابقة إلا استنتاج أن جميع قواسم الأولية لـ $\frac{a^m+1}{a+1}$ هي من قواسم $a+1$ وذلك لأن وجود الـ $n$ على اليمين يمنع التراجح.

(إذاً إنها نفس المسألة السابقة ولكن معممة على $m$ وليس $p$)

لذا سنستخدم الصيغة المعممة لـ ***LTE***

بما أن جميع الأعداد الأولية $p$ بحيث $p \mid \frac{a^m+1}{a+1}$ تحقق $p \mid a+1$ (الشرط الأساسي)

$$v_p\left(\frac{a^m + 1}{a+1}\right) = v_p(m)$$

لجميع $p$ الموجودة في $\frac{a^m+1}{a+1}$ وهذا الشرط يؤدي إلى

$$\frac{a^m + 1}{a+1} = m$$

(يعني نفس الأعداد الأولية ونفس القوى فالعددين متساويين) فما نحسه ونتداركه بناءً على هذه المسألة أنّ المقدار من الشكل $\frac{a^m+1}{a+1}$ يجب أن يحوي أعداد أولية خارج $a+1$ لتعوض فرق الحجم

المساواة الأخيرة تناقض إلا في حال $m = 1$.

**السؤال السادس:**

أثبت أنه إذا كان لـ $b^n - 1 , b^m - 1$ نفس القواسم الأولية عندها $b + 1$ قوة للـ 2 حيث $m \neq n \;\; b \neq 1$

**الحل:**

قبل الإثبات تذكر كيف أثبتنا أن:

$$gcd(b^m - 1 , b^n - 1) = b^{gcd(m,n)} - 1$$

**الحل:**

كما فعلنا من قبل نفس الفكرة: فرض الـ ق.م.أ هو $d$ عندها

$d|b^n - 1 \quad d|b^m - 1$ ← إذاً $b^m - 1 , b^n - 1$ تحوي أعداد أولية من $b^{(m,n)} - 1$

لسهولة الحركة سنسمي الـ ق. م. أ بـ $d$ و $m = dn' \quad n = dn'$

إذاً $b^{dn'} - 1$ له نفس الأعداد الأولية لـ $b^d - 1$

إذاً الأعم $\frac{b^{dn'}-1}{b^d-1}$ له نفس الأعداد الأولية لـ $b^d - 1$

مناقشة قد تصفي ذهنك وتساعدك في التفكير، $n', d$ مستقلان عن بعضهما تماماً وعليك أن تركز في $n$ فقط دون $m$ لأن إذا تمكنت $n'$ من النفاد من الشرط في الأعلى لا شيء يمنع $m'$ فهما في نفس الموقع (نفس المناقشة على $n'$ تنطبق على $m'$

إذاً هذا شكل جديد للمسألة □

والآن نستفيد من الخبرة السابقة خذ أي عدد أولي في $n'$ وطبق السؤال الرابع أو الخامس.

**السؤال السابع:**

هل يوجد عدد طبيعي $n$ يحقق $n|2^n+1$ وأيضاً أن $n$ يقسمه تماماً $2000$ عدد أولي مختلف (يمكن وجود قوة لنفس العدد الأولي ولكن كلها تحسب عدداً اولياً واحداً).

**الحل:**

قبل أن تحل المسألة بتحقيق الشرطيين يجب أن تتخيل بحر حلول للشرط الاول أو على الأقل طريقة لعدد غير منتهي من الحلول.

يجب عند قدومك لمثل هذه المسـألة من خبرتك أن تعرف أن $3^a | 2^{3^a}+1$ أي أن $n$ يمكن أن تحوي أي قوة من 3 ولكن هذا كيف يساعد في وضع الـ 1999 عدد أولي المتبقي؟

لنضف عدداً أولي واحد فقط لنستكشف $p| 2^{3^a \cdot p}+1$

$\Leftarrow$ أخذنا الباقي على $p-1$ فيرما $p| 2^{3^a}+1$

نريد أن يكون العدد إذاً قاسـم لهذا المقدار $2^{3^a}+1$ دون ما تبقى من الـــ $n$ الذي نختاره على كيفنا، هذا أول تفكير ولكن دائماً التفكير المعاكس دائماً يجب أن يكون حاضراً وخاصةً مع الأعداد الأولية.

لمَ نختار $p$ عكيفنا ثم نبحث له عن $a$ مناسبة؟!! فلنختر $a$ ونأخذ 1999 عدد أولي من $2^{3^a}+1$.

نعم بهذه البساطة

بقي إثبات أنه يوجد $a$ بحيث يحوي المقدار $2^{3^a}+1$ أكثر من $2000$ عدد أولي (أي إثبات أنّ العوامل الأولية لـ $2^{3^a}+1$ ليست محصورة في عدد محدود من الأعداد الأولية)

كيف نفعل ذلك؟!!

ستشعر بدايةً بنوع من التقيد، عليك أن تتحرر فقيم $a$ مفتوحة لك مهما كبرت.

نعم الأقوى أن تبدأ من الصفر وتزيد الـ $a$ واحداً واحداً.

**مثال**: إذا كان لدينا $a^p = 1 \ mod \ p^n$ حيث $p$ عدد أولي و$a$ عدد صحيح أثبت أنه عندها

$$a = 1 \ mod \ p^{n-1}$$

**الحل:**

هناك $p$ في الأس وقوة لـ $p$ في الـ $mod$ لذا هنالك إيحاء كبير باستخدام $l.t.e.$

ولكن بدايةً، يجب أن نوجد أساس الـ $l.t.e.$ كيف نفعل ذلك

في العلاقة المعطاة لو أخذنا $p$ واحدة فقط في الـ $mod$ (أي نخفف عن العلاقة) عندها:

$$a^p \equiv 1 \ mod \ p \quad \Longrightarrow$$

حسب فيرما

$$a \equiv 1 \ mod \ p$$

والآن نحن جاهزون

في المقدار $a^p - 1$، الأس يساهم في قوة واحدة فقط لا أكثر وبالتالي ما دون القوس يجب أن يتحمل الـ $n - 1$ قوة المتبقية:

$$\Longrightarrow a \equiv 1 \ mod \ p^{n-1}$$

.

## الآن مع امثلة منوعة

مثال: أوجد $p$ عدد أولي بحيث

$$p^{p+1} + (p+1)^p = \text{مربع كامل}$$

**الحل:**

$$p^{p+1} + (p+1)^p = k^2$$

دائماً فيما عدا $p = 2$ نبدأ كـ $p$ فردي ومن الواضح ما الهدف من ذلك.

$$(p+1)^p = k^2 - p^{p+1}$$

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

نلاحظ أنه لدينا جداء قوسين هما القوة $p$ لعدد، هذا يذكرونا بحالة جداء قوسين يساوي عدد ثابت أو بالأصح جداء قوسين يساوي مربع كامل والآن قوة أكبر من التربيع المشترك بين كل ما سبق أنه لدينا معادلة ممتازة.

الآن:

$$gcd\left(k - p^{\frac{p+1}{2}}, k + p^{\frac{p+1}{2}}\right)$$

$$= gcd\left(k - p^{\frac{p+1}{2}}, 2p^{\frac{p+1}{2}}\right) = 2$$

نلاحظ أنه لكل الأعداد الأولية غير الـ 2 يجب أن تكون مرفوعة الأس $p$ في كل قوس لوحده اذاً كلا القوسين من الشكل $2\square a^p$ , $2\square b^p$

ماذا عن الـ 2 ؟

لا يمكن أن يشترك القوسين في أكثر من 2 لذا أحد الأقواس تحتوي 2والأخرى تحتوي $2^{p-1}$ (( إذا احتوى الجداء على $2^{2p}$ أو أكثر (وهذا ممكن) عندها نكون قد أدخلنا الـ $2^p$ الزائدة في $a$ أو $b$ سلفاً))

اذاً حالتين:

| الحالة الأولى | الحالة الثانية |
| --- | --- |
| $k - p^{\frac{p+1}{2}} = 2a^p$ | $k - p^{\frac{p+1}{2}} = 2^{p-1}b^p$ |
| $k + p^{\frac{p+1}{2}} = 2^{p-1}b^p$ | $k + p^{\frac{p+1}{2}} = 2a^p$ |

لنبدأ بالحالة الأولى لكن قبل أن نتابع يجب أن نلاحظ أن هاتين المعادلتين لا تكافئ المعادلة الأصلية كفاية التي حصّلناها منها، فهذه المرة كما أخبرتكَ نفسك أن ناتج جداء القوسين ليس أي مجهول عادي يمكنه تلقي أي شيء بل هو $p+1$ إذاً نلاحظ بخباثة علاقة ثالثة مضافة أن $p+1=2ab$.

والآن نتخلص من $k$ في المعادلتين لأنه مجاله مفتوح ولا شروط عليه وهو مصدر إزعاج.

**الحالة الأولى:**

$$p+1=2ab \text{ مع } p^{\frac{p+1}{2}} = 2^{p-2}b^p - a^p$$

يمكننا أن نراجع أحجام الأرقام بداية فقط ليبقى لنا تصور عن الأرقام التي نتعامل معها ... يوجد لدينا

$$p+1 \geq 2b \text{ و } 2^{p-2}b^p \geq p^{\frac{p+1}{2}}$$

ولكن نجد أنها ليست كافية اذاً يجب أن نبحث عن خاصية "نظرية الأعداد" بحتة

وبالفعل الأقرب ستكون هي $mod\ p$ بسبب إيحاءات فيرما.... بأخذه للمعادلة الأولى

$$0 \equiv 2^{-1}b - a\ mod\ p$$

$$\Longrightarrow 2a \equiv b\ mod\ p$$

ولكن هذين المقدارين أصغر من $p$ (لماذا؟ هنا تظهر فائدة تقدير حجوم المسبق للأعداد) $0 = 2a - b$ والتتمة بسيطة.

**مثال:** أثبت أن عدد قواسم أي عدد فردي التي تكافئ $1 \ mod \ 4$ أكبر أو يساوي من عدد القواسم التي هي $3 \ mod \ 4$.

**الحل:**

أول تفكير هو هل من الضروري عدد القواسم الأولية $1 \ mod \ 4$ أكبر من $3 \ mod \ 4$؟

بالتأكيد لا فالعدد من اختيار صاحب المسألة وليس اختياري.

إذاً هل تأثير العدد الأولي $1 \ mod \ 4$ يشابه تأثير $3 \ mod \ 4$

كلا لأن $1 \ mod \ 4$ تأثيره رائع جداً حيث لا يغير من باقيه بالنسبة الـ $4$ فوجوده مثل عدمه ما عدا القواسم الإضافية التي تأتي من هذا العدد وحده.

لذلك نفرض جميع الأعداد الأولية $3 \ mod \ 4$ كأسوأ حالة.

اذاً هذا بالنسبة للعدد الأولي وتذكر دائماً الخطوة التالية هي قوة العدد الأولي وبالتأكيد سيكون محقق لأنه صاحب المسألة قد يختار العدد قوة لعدد أولي.

اذاً لنثبت على أن $p^{a_1}$ إذا كان $a_1$ فردي يكون التساوي بين نوعي القواسم (لا ننسى وجود $-p^0$ أهم فكرة) وأنّ $p \equiv 3 \ mod \ 4$

إذا كان $a_1$ زوجي يكون عدد القواسم من الشكل $1 \ mod \ 4$ أكبر بقاسم واحد اذاً أيضا محق

بقي لو تداخل عددين أوليين معاً $q_1^{a_1}$ , $p_1^{a_1}$ الجدول التالي يوضح:

| | $p$ | $q$ |
|---|---|---|
| $1 \ mod \ 4$ | $x_1$ | $x_2$ |
| $3 \ mod \ 4$ | $y_1$ | $y_2$ |

لنجري التداخل الآن

$$x_1x_2 + y_1y_2 \geq x_1y_2 + y_1x_2$$

الآن إثبات المتراجحة التالية هو على إعادة الترتيب ولكن حتى لو لم تخطر بالبال مجرد معرفتك أنها حتماً محققة وملاحظتك وجود الكثير من المجاهيل جميعها من الدرجة الأولى ينبأ بسهولتها ...

الآن كيف نعمم على أكثر من عددين أوليين

أكثر ما سيخطر لنا هو الاستقراء بالفعل حيث العددين الأوليين في الأعلى سنعتبرهما عدد واحد أثبتنا أنّ قواسمه التي هي $1 \ mod \ 4$ أكبر من عدد القواسم $3 \ mod \ 4$ لذا نضعه في جدول مع العدد الأولي الجديد ونطبق إعادة الترتيب من جديد وهكذا بالاستقراء نتابع.

أثبت أنه لا يوجد متتالية منتهية حسابية بحيث جميع حدودها قوى لعدد صحيح.

**الحل:**

الآن المتتالية من الشكل $a + kd$ من أجل أي $k$ طبيعي

الملاحظة القوية أنّ حدود المتتالية ما هي إلا الأعداد $a \ mod \ d$

يجب أن تراها وفيرة ومنتشرة بقدر ما ترى الأعداد $3 \ mod \ 5$ وبالتالي نرى أن المسألة بدأت تبدو أسهل

ماهي الطرائق السريعة لنعبر عن عدد ما بدون معرفته بشكل كاملاً؟؟
أحد الطرق هي الـ $mod$ لأعداد معينة لكن لا يمكننا استخدامه لأنه لأي عدد نختاره أولي مع $d$ ستعطي المتتالية كل البواقي في موده

إذاً ما هي الطريقة الأخرى التي تجعلنا نحكم على عدد أنه ليس قوة لعدد صحيح من خلال معرفة أبسط معلومات عنه

كما لاحظنا في الجملة في الأعلى أنه يمكننا الحصول على أي باقي في $mod$ أي عدد أولي مع $d$

الآن كيف نستخدم الـ $mod$ في ايجاد عدد اولي وحيد؟!!

الإجابة هي بأخذ $k$ التي تحقق مثلاً $a + kd \equiv 7 \ mod \ 49$ مثلاً وعنها هذا الحد حتماً ليس قوى لعدد صحيح

حيث 7 اولية مع $d$ (نختار عدد نحن اولي مع $d$ ).

**مثال:** لدينا $p$ عدد أولي و $n \in \mathbb{N}$ أثبت أنّ $n$ هو عدد أولي:

$$3^n - 2^n = p^a$$

**الحل:**

نشعر بأنه لا يريدنا أن نحلل اليسار اذاً بنقض الفرض نضع $n = mq \quad m \neq 1$

(هنا انتبه نضع $q$ أولي لأنه أصغر وحدة نخرجه من $n$ إن وجد)

$$3^{mq} - 2^{mq} = p^a$$

لابد أن $lifting\ exponent$ تلوح بالأفق حيث أساسها واضح لأن المقدار كله يكون قوى لـ $p$ ما الذي سيكون $a, b$ هنا؟

بالتأكيد $a = 3^m\ , b = 2^m$ لأن $q$ قدرته أضعف في الأس نستفيد من ذلك:

$$(3^m - 2^m)\left(\frac{(3^m)^q - (2^m)^q}{3^m - 2^m}\right) = p^a$$

الآن القوس الثاني إما أن يحوي $p$ واحدة إذا كان $q$ هو $p$ أو لا يحوي $p$، نفرض أنه يحوي واحدة عندها:

$$p^{a-1} | 3^m - 2^m$$

أين التناقض في ذلك برأيك ما هو الغير منطقي؟

بالضبط من شكل المتطابقة وهذه من الواضح أن $\frac{(3^m)^q - (2^m)^q}{3^m - 2^m}$ أكبر من $3^m - 2^m$ (وليس بقليل بل بكثير لأن اليمين مرفوع للأس $q$)، اذاً التناقض واضح.

إذاً فعلا $n$ لا يجب أن يتحلل إذاً هو عدد أولي.

### المسألة الثامنة

من أجل أعداد طبيعية $n, m$ أثبت أن $2^n - 1$ | $(2^m - 1)^2$ إذا وفقط إذا $n$ | $(2^m - 1)m$

**الحل:**

سنبدأ بـ $2^n - 1$ | $(2^m - 1)^2$ ونثبت للطرف الآخر

قبل أن ندبر أمر الـ $(2^m - 1)^2$ مربع أي القوس مرّتين فنبدأ بواحد منهم، أي لدينا

$$2^m - 1 \mid 2^n - 1$$

وهذه حسب الطريقة التي يجب أن تكون قد تعودنا عليها

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$$

- إذاً $2^m - 1$ يقسم $2^{(m,n)} - 1$ لأن ما يحوي الطرف الأيمن خارج القاسم المشترك الاكبر لا يمكن أن يفيد الطرف الأيسر فنسقطه (كما فعلنا في البدايات،،،، حولنا مسألة قسمة إلى إيجاد قاسم مشترك ...هي حركة بدائية وليست معجزة وقوية)

وبالتالي بالتراجح نجد $(m, n) = m$ أي $n$ | $m$ أو **بدءاً من اللحظة يمكنك مباشرة استنتاج كون $m|n$.**

وبطريقة أخرى نقول ببساطة $n = mq + r$ ونجد بتخفيض المرتبة ☺ أنّ $2^m - 1$ | $2^r - 1$ وبما أنّ $r$ أصغر من $m$ نجد أنّ $r = 0$

- إذاً $n = mk$ ونعود لتدبير وضع

$$(2^m - 1)^2 \mid 2^{mk} - 1$$

علينا أن نثبت أن $k$ | $2^m - 1$ كيف ذلك

أولاً

$$2^m - 1 \mid \frac{2^{mk} - 1}{2^m - 1}$$

لو تخيلنا $2^m$ هي $a$ مثلاً بماذا تذكرك الجملة الرياضية الأخيرة

$$\left(a - 1, \frac{a^k - 1}{a - 1}\right) = (a - 1, k)|k$$

لاحظ أنّ هذا القاسم المشترك الأكبر حسبنا مثله في إثبات *LTE* الخطوة الأولى.

ولكي تتحقق القسمة يجب أن يقسم $2^m - 1$ الـ $gcd$

$$2^m - 1 | \, k \quad \Leftarrow$$

وبهذا بالتأكيد نصل للهدف

$m(2^m - 1) | \, n$ نلاحظ أنه اتجاه سهل

الآن الاتجاه الآخر لو كان $n \mid (2^m - 1)m$

يكفي إثبات طبعاً

$$(2^m - 1)^2 | \; 2^{m(2^m-1)} - 1$$

بالمثل تماماً

$$2^m - 1 | \; \frac{(2^m)^{(2^m-1)} - 1}{2^m - 1}$$

لو فككنا الطرف اليمين لوجدنا $2^m - 1$ حد وكل منهم قوة ل$2^m$ أي $1$ بالـ $mod\ (2^m - 1)$.

## نظرية أخرى هامة جداً:

إذا كان $p,q$ عددين أوليين و $x,y$ أوليان فيما بينهما إذا كان $p|\frac{x^q-y^q}{x-y}$ عندها إما $p=q$ أو $p\equiv 1\ mod\ q$

طريقة برهانها تشبه الآلية التي استخدمناها كثير لكن هنا الأس عدد أولي إذاً:

$$p|\frac{x^q-y^q}{x-y}$$
$$p|x^q-y^q$$
$$p|x^{(q,p-1)}-y^{(q,p-1)}$$

الجميل هنا أنه يوجد عدد أولي في أحد طرفي القوس فالآن إما $q$ موجودة في $p-1$ إذاً $p=1\ mod\ q$ أو غير موجودة عندها.

$$p|x-y$$

إذاً أصبح $p$ في $x-y$ أيضاً وفي" البنية الأسية $q$" (هذا المصطلح سنطلقه على $\frac{x^q-y^q}{x-y}$)

لكن

$$(x-y,x^{q-1}+x^{q-2}y+\cdots-y^{q-1})=(x-y,qx^q)$$
$$=(x-y,q)|q$$

إذاً $p|q \Leftarrow p=q$ تم الإثبات.

ملاحظة:

في الحالة الأولى لم نصل إلى $p|x-y$ لذا لم نقترب من LTE

في الحالة الثانية وصلنا إلى $p|x-y$ لذا اقتربنا من LTE

فكما تقول النظرية الأخيرة إذا أردنا ل $p$ ان تكون محتواة في "البنية الأسية ل $q$" وال $x-y$ في نفس الوقت عندها $p=q$ ....فعلياً ما فعلناه للتو لاثبات هذا الشيء هو إحدى خطوات برهان النظرية lte (تذكر)

الآن إذا كان لدينا:

$$p|x^q - y^q$$

إذا بدأنا بهذه الصيغة $x^q - y^q$

عندها إما $p|x - y$ أو

$$p \equiv 1 \ mod \ q \leftarrow p|\frac{x^q - y^q}{x - y}$$

- لذا كمحصلة حالتين إما أن يدخل $p$ في $x - y$ عندها نذهب للنظرية الأولى.
- او $p = 1mod\ q$
- بتعبير أبسط: إذا أردت الدخول يا أيها العدد الأولي $p$ بالبنية الأسية ل $q$ حقق شرطها $(p = 1mod\ q)$
  - وإلا فاتركها وشأنها.

وأحيانا ماذا نفعل عندما يكون $p|x^n - y^n$ يعني $n$ غيرأولي نخرج عدد أولي $q$ من الأس $n$, $p|x^{n'q} - y^{n'q}$

$$p|\left(x^{n'}\right)^q - \left(y^{n'}\right)^q$$

لو اردت الدخول فحقق الشرط $p \equiv 1 \ mod \ q$

أو ادخل $p|x^{n'} - y^{n'}$

لنرى كيف سنستفيد من هذه النظرية في التمارين ولا تنسَ أنها تنطبق عالـ + أيضاً بدل الـ – نفس التطبيق تماماً.

**مثال1:** أوجد $p, q$ أعداد أولية

$$pq|(5^p - 2^p)(5^q - 2^q)$$

إما $p|5^p - 2^p \Leftarrow p = 3$

أو $p|5^q - 2^q$ إما $p = 3$ أو $p \equiv 1 \ mod \ q$

بالمثال لـ $q$ إما $q = 3$ أو $q \equiv 1mod\ p$

لا يمكن أن يكون $q \equiv 1 mod\ p$ و $p \equiv 1\ mod\ q$

إذاً أحدهما ليكن $q = 3$

إما $p = 3$ (3,3) حل أو $p|5^3 - 2^3 \Leftarrow p = 13$

(13,3) حل و (3,13) أيضاً.

**مثال2**: حل المعادلة التالية حيث

$$\frac{x^7 - 1}{x - 1} = y^5 - 1$$

**الحل:**

لدينا $\frac{x^7-1}{x-1}$ شـــكله محبوبه كل أعداده الأولية 0 أو1 $mod\ 7$ لذا هو ككل $0,1\ mod\ 7$ ولكنه ليس فقط بهذه الظرافة إنه أظرف فكر كيف ذلك!

حقيقة أي جزء منه يكون $0,1\ mod 7$

إذاً ماذا عن

$$(y - 1)(y^4 + y^3 + y^2 + y + 1)$$

إذا كان $y - 1 \equiv 0\ mod\ 7$ عندها القوس الآخر $5\ mod\ 7$ وهذا تناقض.

وإذا كان $y - 1 \equiv 1\ mod\ 7$ عندها القوس الآخر $3\ mod\ 7$ أيضاً تناقض.

إذا لا يوجد حلول.

**والآن إلى المثال الأقوى لهذه الفكرة**

**تمرين**: أوجد ثلاثيات الأعداد الأولية التي تحقق

$$q|r^p+1 \quad , \quad r|p^q+1 \, , \quad p|q^r+1$$

**مسألة :**

ليكن $n>3$ عدداً صحيحاً فردياً بكتابة على الشكل $n = p_1^{a_1}p_2^{a_2} \dots p_k^{a_k}$ وليكن

$$m = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_n}\right)$$

أثبت وجود عدد أولي $p$ بحيث $p \mid 2^m-1$ ولا يقسم $m$:

أولاً نلاحظ أن $m = \emptyset(n)$ وبالتالي $n \mid 2^m-1$ إذاً سيخطر لنا أن نأخذ عدداً أولياً في $n$ غير موجود في $m = \emptyset(n)$، وهذا يتطلب حسب طريقة حسابنا لل $\emptyset(n)$ وجود عدد اولي $p_i$ مرفوع للقوة 1 في $n$ وهذا غير كافٍ، ربما يوجد $p_i$ في $p_j-1$ (اي ان ياتي$p_i$من مكان اخر ... إذاً هذه الفكرة ضعيفة.

عملياً أصبح $n$ في طلب المسألة خارجاً (استخدموه للتضليل)، والـ $m$ يمكن معاملتها كأنها أي عدد خاصة أن التابع $\emptyset$ يعطي معظم القيم التي تريدها اذا هذا التابع لايقيد قيم $m$ بشكل كبير ... إذاً ما هي طريقة معاملة $2^m-1$ مع $m$؟ ما هي النظريات التي تعلمناها والتي يمكن أن تطبق؟؟

بالفعل نظرية $2^q-1$ هنالك خواص لقواسمها الأولية خاضعة لقوانين $q$: إما أن يساوي $q$ أو $1\ mod q$.

إذاً سنأخذ عدد أولي $q$ من $m$ ونخرج $2^q-1$ من $2^m-1$ونأخذ عدد أولي $p$ يقسمه)

نحصل على عدد أولي $p$ مجبور على الخواص في الأعلى (إما أن يساوي $q$ أو $1\ mod q$ )، كيف نضمن أنه ليس في $m$؟...

نعم بأن نفرض $q$ هو **الأكبر الموجود في $m$** ... إذاً إذا كان $p \equiv 1\ mod q$ فهو حتماً غير موجود في $m$ لأن $q > p_j-1$ ... إذاً يسمح له فقط أن يكون $p=q$، هل دمرت هذه الاحتمالية عملنا أم بإمكاننا انهاؤه؟

لا لا يدمر لانه لاحظ اي احتمالية اختار ال$p$ الذي هو يفترض ان يكون اكبر الاعداد الاولية

كيف للاعداد الاولية الاصغر منه ان تكون $\equiv 1\ mod q$

... فالآن كل الأعداد الأولية في $2^q - 1$ هي $q \Longleftarrow 2^q - 1 = q^t$ سنصل لتناقض $100\%$ (هذا اليقين يمنع التلبك): $2^q = q^t + 1$:

*i.* إن كان $t$ زوجياً فهذا تناقض لأنه مجموع مربعين.

*ii.* أما إن كان فرياً فواحد فقط من $q + 1, \frac{q^t+1}{q+1}$ يمكن أن يكون زوجياً.

إذاً أخبرتك التناقض واضح، وبهذا نوجد العدد الأولي المطلوب.

هناك مسائل متشابهة نوعاً ما قد تعتقد أنها واحدة، ولكن **لا** (احفظها لكي تخطر لك من أول مرة)

وسنعرض في الأولى فكرة رائعة مبتكرة تفيدنا

**الأولى:**

أثبت تكافؤ العبارتين:

- من أجل أي عدد صحيح $a$ يكون $n \mid a^n - a$.
- من أجل أي عدد أولي $p$ يقسم $n$ يحقق $p^2 \nmid n$ و $p - 1 \mid n - 1$.

الآن لنبدأ بصحة الجملة الأولى أي $n \mid a^n - a$، لأي $a$، ليكن $p$ عدداً أولياً $p \mid n$، لنفرض جدلاً أن $p^2 \mid n$، نضع $p = a$ فنصل لتناقض.

إذاً $n = p_1 p_2 \dots p_t$، والآن لإثبات أن $p-1 \mid n-1$ لدينا: $p \mid a^n - a$ و$p \mid a^p - a$، أهمل $a = 0$،

$\Leftarrow p \mid a^{n-1} - 1$ ، $p \mid a^{p-1} - 1$، الآن إن لم يكن $p-1 \mid n-1$ عندها بمعاملة آخر علاقتي قسمة سنحصل على عدد ثالث: $p \mid a^d - 1$ والذي هو عملياً $p-1 > gcd(p-1, n-1)$ وهذا تناقض لأن $a$ تحقق العلاقة من أجل كل الأعداد $\mathrm{p}-1 \longrightarrow 1$، وهذا يتطلب **كثير حدود درجته $\boldsymbol{p-1}$**، إذاً $gcd$ يجب أن يساوي $\mathrm{p}-1 \Leftarrow p-1 \mid n-1$.

أما العكس فهي الأسهل، فلديك $n = p_1 p_2 \dots p_t$، ستتحقق أن $p_i \mid a^n - a$ حسب فيرما $\Leftarrow n \mid a^n - a$ فعلاً من أجل كل قيم $a$.

**مثال:**

اوجد كل $n$ تحقق ان

$$n \mid a^{25} - a$$

من اجل اي عدد طبيعي $n$

**الثانية:**

في هذه المرة سنثبت $a$ عدد صحيح واحدة ونقول:

إذا كانت $n-1$ هي أصغر قوة لـ $a$ تحقق $n \mid a^{n-1} - 1$ أثبت أن $n$ أولي: (سهلة للغاية)

كيف يمكن أن يكون أصغر عدد وقد اقترب من النهاية أو هو في النهاية عملياً؟

إذاً ماذا عن $\emptyset(n)$الذي هو اصغر من $n$ ؟ إذاً حتما $\varphi(n) = n-1$.

بحل هذه المعادلة البسيطة باستخدام قانون حساب ال φنجد أنه ما لم يكن $n = p$ سيكون $\varphi(n) < n-1$.

**والآن مزيد من الأمثلة الأقوى في هذا المحيط:**

**مثال 1**: أثبت أنه لأي عدد أولي $p$ يقسم $2^{2^n} + 1$ عندها $p \equiv 1 \mod 2^{n+1}$

**الحل:**

نعم نلاحظ أنها تشابه الشكل الماضي وبالفعل تعطي خاصية للعدد الأولي الذي يقسم شكل معين إذاً لنتبع طريقة إثبات النظرية

$$2^{2^n} + 1 \equiv 0 \ mod \ p$$

$$2^{2^n} \equiv -1 \ mod \ p \quad \text{نريد } 1 \text{ وليس } -1 \quad *$$

$$2^{2^{n+1}} \equiv 1 \ mod \ p \quad **$$

$$2^{p-1} \equiv 1 \ mod \ p$$

$$2^{(p-1,2^{n+1})} \equiv 1 \ mod \ p$$

إذاً بالطبع القاسم المشترك سيكون $2^d$ لو افترضنا $d < n + 1$ أي $d \leq n$

$$2^{2^d} \equiv 1 \ mod \ p$$

الآن تذكر أن الانتقال من * إلى ** كان عبارة عن غش وإعطاء حالات زائدة وجاء الآن وقت الدفع

أي يجب أن نتذكر أن $2^{2^n} \equiv -1 \ mod \ p$ ... $(*)$

بملاحظتها مع $2^{2^d} \equiv 1 \ mod \ p$ نلاحظ التناقض أن $d$ أصغر من $n$ لذا إذا ربعنا العلاقة الأخيرة $n - d$ مرة نحصل على $*$ ذاتها ولكن بـ $1$ بدل $-1$ !!

إذاً $1 \equiv -1 \ mod \ p \Leftarrow p = 2$ تناقض

إذاً $d \geq n + 1 \Leftarrow d = n + 1$

إذاً $2^{n+1}$ هي القاسم المشترك بكاملها إذاً:

$$p \equiv 1 \ mod \ 2^{n+1}$$

■

**تعقيب:** إذاً هذا الشيء العظيم الذي حدث في المسألة نشأ فقط عن إشارة الـ + بدل الناقص حيث أصبحت قوة الـ 2 "ضعيفة" أمام الـ + لذا على الـ $p - 1$ أن يأخذها كلها ضمنه (مضافاً لأسها واحد أيضاً $2^{n+1}$) أما عند اشارة الناقص فهي تعامل الكل بنفس المعاملة وتعاملهم وفق النظرية السابقة فقط. (البنية الأسية لـ $q$ عدد اولي غير ال2).

**مسألة**: أوجد الأعداد الأولية $p, q$ بحيث:

$$pq \mid 2^p + 2^q$$

**الحل:**

كالعادة لا قيمة من إبقاء قسمة $pq$ سويةً وانما هي

$$p \mid 2^p + 2^q \quad \text{و} \quad q \mid 2^p + 2^q$$

إذا افترضنا أن $p, q$ ليسا 2 بداية نجد حسب فيرما:

$$p \mid 2^{q-1} + 1 \qquad q \mid 2^{p-1} + 1$$

الآن نلاحظ أنها تشابه شكل النظريات التي تعلمناها مؤخراً. ولكن لا نرى في $p - 1$ عدد أولي واضح ونرى إشارة الزائد لذا ذلك يشير إلى استخدام قوى الـ 2 في $p - 1$.

حسب النظرية السابقة $q - 1$ تحوي القوة لـ 2 الموجودة في $p - 1$ مضافاً إليها 1 (بإمكانك إعادة الخطوات السابقة لتمرن يدك).

إذاً:

$$u_2(q - 1) = 1 + u_2(p - 1)$$

تناقض إذاً ماذا تركنا من حالات أن يكون $p = 2$ عندها:

$$q \mid 6$$

إما $q = 2$ أو $q = 3$ إذاً لدينا $(2,3)$ , $(2,2)$ , $(3,2)$.

**مثال2:**

أثبت أنه من أجل أي عدد أولي $p$ يقسم $m^{2\cdot 3^n}+m^{3^n}+1$ من أجل عددين طبيعيين $m\,,n$ يتحقق $p\equiv 1\ mod\ 3^{n+1}$ حيث $p\neq 3$.

**الحل:**

الآن من جديد مسألة إيجاد خاصية لأي عدد أولي يقسم المقدار من الشكل المعين ولكنه لا يشابه أشكال النظرية السابقة.

حتى تنتبه للمتطابقة $x^2+x+1$.

$$m^{2\cdot 3^n}+m^{3^n}+1\equiv 0\ mod\ p \quad *$$
$$m^{3^{n+1}}\equiv 1\ mod\ p \quad **$$
$$m^{(3^{n+1},p-1)}\equiv 1\ mod\ p$$

أيضاً نقول ليكن القاسم $3^d$ حيث $d<n+1\quad d\leq n$

$$m^{3^d}\equiv 1\ mod\ p$$ 1

الآن مع أي معادلة سنحاول الوصول للتناقض؟

بالتأكيد ليست ** لأنها تحوي "الغش" كما حدث في المرة الماضية

$$m^{2\cdot 3^n}+m^{3^n}+1\equiv 0\ mod\ p$$

بما أن $d\leq n$ إذاً $m^{3^n}\equiv 1$ (نحصل عليها بالتكعيب عدة مرات لـ 1)

نعوض الآن في $(*)$ $3\equiv 0\ mod\ p$ تناقض

إذاً $d=n+1\Leftarrow (3^{n+1},p-1)=3^{n+1}$ بمعنى:

$$p\equiv 1\ mod\ 3^{n+1}$$

■

**تعقيب:** الشكل $x^{2n}+x^n+1$ ضعيف أمام قوى الـ 3 أي يضطر العدد الأولي أن يأكل كل قوى الـ 3 (مع 3 إضافية)

كما كان الشكل $x^n+1$ صفينا أمام قوى الـ 2 حيث $\frac{x^{2n}-1}{x^n-1}=x^n+1$

كما أن $\frac{x^{3n}-1}{x^n-1}=x^{2n}+x^n+1$

ولو أردت مثالاً على أن الشكل $x^{2n}+x^n+1$ ليس ضعيفاً أمام الـ 5

$$p|\ m^{2.5^n}+m^{5^n}+1 \dots\dots\dots .\#$$

عندها مكان (**)

$$m^{3\cdot 5^n}\equiv 1\ mod\ p$$
$$m^{(3\cdot 5^n,p-1)}\equiv 1\ mod\ p$$

الآن إذا دخلت 3 في القاسم المشترك الأكبر أصبح لدينا

$$m^{3\cdot 5^n}\equiv 1\ mod\ p$$

ولا يمكننا حينها التعويض في (#) ولا نصل لأي مكان

**تعقيب:** اســتخدام المتطابقة $x^{2n}+x^n+1$ نادرة أما الأكثر اســتخداماً هي $x^n+1$ ونركز عليها بالطبع.

الآن إلى **مسألة قوية:**

**مثال3**

أوجد أزواج الأعداد الأولية $p, q$ الفردية التي تحقق

$$q^2+1 \mid 2003^p+1 \qquad p^2+1 \mid 2003^q+1$$

**الحل:**

الآن نبدأ مقارعة القسـمات بالأدوات التي في حوزتنا، نلاحظ عدد أولي في القسـمة وهذا يدفعنا مباشرة لـ: أي عدد أولي $r$ في $p^2+1$

$$r \mid 2003^q+1$$

الآن نطبق خطوات إثبات النظرية بسبب الـ +

$$r \mid 2003^{2q}-1$$
$$r \mid 2003^{(2q,r-1)}-1$$

الآن نلاحظ هناك لهذا القاسـم المشـترك حالات قليلة (لوجود الـــ $q$ كعدد أولي طبعاً) وهي بالضـبط 4 حالات:

$1, 2, q, 2q$ ولكن بدل أن أناقشها 4 سأناقشها على مجموعتين فقط

الأولى $q$ موجود في $r-1$

وأقف هنا لأنها أعطتني بالفعل صفة عن العدد الأولي الذي يقسم الشكل.

الثانية $q$ غير موجود عندها

$$r \mid 2003^2-1$$

ولكن نتذكر أننا غششنا في الأعلى (يجب أن تبقى دوماً في البال للنقض السريع)

فلو أخذنا $r \mid 2003-1$ عندها $r \mid 2003^q-1$.

إذاً سنأخذ $r \mid 2003+1$

$$r \mid 8 \times 3 \times 167$$

والآن نرى وجود الكثير من الأعداد التي يمكن أن يأخذها يبدو أنها خريطة طويلة ولن نصـل للحل ولكن نتذكر ما هو الـــ $r$ ؟ نبدأ بالرجوع للأصـل البدئي $r$ هو من قواســم $p^2+1$ والتي تتصـف بأنه كل قواســمها $1 \ mod \ 4$ لذا لا يتبقى سوى 2 واحدة وهذا $r|2$

والآن الذكاء في إيجاد الملخص:

أي عدد أولي في $p^2+1$ هو إما $1 \ mod \ q$ أو هو 2 (واحدة فقط)

ولكن بالمثل أي عدد أولي في $q^2+1$ هو إما $1 \ mod \ p$ أو 2 (واحدة فقط)

الآن ما الخطوة التالية من المخطط التالي أين تجد نوع من التناقض.

بالفعل كل عدد أولي يعطي حجماً جيداً لذا نقول:

$$wlog \quad p \geq q$$
$$p^2+1 \geq q^2+1$$

إذاً $q^2+1$ لا يمكن أن تحوي عددين أوليين فوق الـ 2 لأنهما $1 \ mod \ p$

إذاً $q^2+1=2r$ حيث $r \equiv 1 \ mod \ p$

الان نتامل اخر ما وصلنا اليه هل يمكن ان نستفيد من كون $r$ اولي ...لا نجد اي فائدة واضحة لذا نلجا لخاصية $r$ الاساسية التي جاء بها ..أن

$$r=pk+1$$

بالتعويض نجد مباشرةً

$$q^2-1=2pk$$

أما $p| \ q-1$ مرفوض لأن $p \geq q$

أو $p| \ q+1$ وبما أن $p \geq q$

$$p=q+1 \ \Leftarrow$$
$$p=3 \quad q=2 \ \Leftarrow$$

تناقض لأن الأعداد $p, q$ فردية ولو لم يقل إنها فردية لناقشنا حالة الزوجية $p=2$ مثلاً ونوجد احتمالات $q$

**تعقيب:** وجدنا كيف كانت المسألة شاملة استخدمنا فيها الشكل $p^2+1$ والنظرية "البنية الأسية" وبعض الحركات الجبرية المبتكرة في النهاية.

**مثال 4:** ليكن $p>2$ عدد أولي بحيث $3|p-2$ ليكن

$$S=\{y^2-x^3-1 \mid x,y \text{ صحيحة} \quad 0\le x,y\le p-1\}$$

أثبت أنه على الأكثر $p$ عنصر من $S$ مضاعف لـ $p$.

**الحل:**

كيف سندخل في صلب المسألة حيث نلاحظ وجود $p^2$ ثنائية من $(x,y)$

ما سيخطر لنا هو أن نناقش تساوي عنصرين بالمود $p$ فنقول:

$$y^2-x^3-1\equiv y_0^2-x_0^3-1 \ \ mod\ p$$
$$y^2-y_0^2\equiv x^3-x_0^3\ mod\ p$$

لا يمكن متابعة هذه المعادلة...

لذا سنحاول إيجاد $(x_o,y_0)$ بدلالة $(x,y)$ هذه استراتيجية قوية في الكثير من المسائل وأحياناً لا يكون هذا الإيجاد بغاية السهولة ففي مسألتنا القوة التكعيبية تجعل الأمر صعباً لحد ما.

لذا الآن سنحاول أن نغير إطار تعاملنا مع المسألة، لو أخذنا محور $y$ ثم محور $x$.

$y^2$ ستعطي $\frac{p-1}{2}$ باقي أي فقط قيمتين لـ $y$ ستعطي نفس الـ $y^2$.

ماذا عن $x^3$ كم قيمة مختلفة ستعطي ....ليس لدي أي نظرية جاهزة لذا أبدأ واحدة جديدة

$$x^3\equiv y^3\ mod\ p$$
$$(x-y)\left(\frac{x^3-y^3}{x-y}\right)\equiv 0\ mod\ p$$

القوس الثاني قواسمه إما 0 أو $1\ mod\ 3$ ولكن $p\equiv 2\ mod\ 3$ لذا $p$ حصراً في $x-y$ بمعنى حتى يتساوى باقيين تكعيبيين يجب أن يكون الباقي نفسه، ومنه $x^3$ تعطي كل البواقي

والآن انتهت المسألة لماذا؟!!

بالتأكيد لأن أي قيمة معطاة لـــ $y_0$ سيكون هناك قيمة $x_0$ واحدة فقط تحقق المعادلة $x_0{}^3 \equiv y_0{}^2 + 1 \ mod\ p$ وكأن جبهة $x$ استلمت زمام الأمور.

**المسألة الخامسة:**

أثبت وجود عدد غير منتهي من الأعداد $n$ بحيث يكون أكبر قاسم أولي للعدد $n^4 + 1$ أكبر من $2n$

**الحل:**

المسألة سهلة لا تحملها فوق طاقتها فقط تتطلب خبرة بالهندسة نعم حينما تلتف على المسألة بأن تصل ضلعين وتثبت الآخر يمر من النقطة.

أول الخواطر أنه هل الشكل $2^{2^n} + 1$ يساوي عدد أولي من أجل عدد غير منتهي من القيم لـ $n$هذه الفكرة والدخول فيها تعقيد للمسألة ومبكر جداً الدخول فيها وعلى الحالتين لم يتم إثباتها بعد من العلماء.

وأيضاً سيدفعك توجه ورغبة ذاتية لتحليل الـــ $n^4 + 1$ ولو بالـــ $mod$ ولكن قبل أن تحاول.. التحليل بالأصل سيضرك.

وأيضاً فكرة أن أي عدد أولي يقسم $n^4 + 1$ هو $1,0\ mod 4$ أيضاً ضعيفة جداً.

هنا نشعر بإغلاق الأبواب فلا اختيار في شكل لـ $n$ ينتج عنه $p$ أعرفه.

بعد التفكير المديد والأخذ بأول جملة سنعرف أنه سنحدد $p$ لنختار بعدها $n$ تناسبه.

إذاً نأخذ $p$ عشوائي قابلا لاختيار صفاته فيما بعد

$$p|\ n^4 + 1$$

نريد لـــ $n$ أن يكون صغير ويحقق القسمة لذلك نطلب أول $n$ يحققها لكن كيف أعرف أن $n$ لن يطول انتظاره؟!!

بالفعل لن يطول انتظاره .. لأنه إما أن يكون من $p \leftarrow 1$ أو لا يكون موجودا مطلقاً ...وكيف نمنع الخيار الأخير.

تذكر في $x^2 + 1$ نختار $p \equiv 1\ mod\ 4$ و $x$ يكون موجود (كما فعلنا في ويلسون)

بـ $x^4 + 1$ سنستخدم طريقة تنجي في كل الحالات لدينا

$$\left(x^{\frac{p-1}{2}}-1\right)\left(x^{\frac{p-1}{2}}+1\right)\equiv 0\,,x^{p-1}\equiv 1\,mod\,p$$

نعلم أن نصف الأعداد ستحقق القوس الأيمن أي $x^{\frac{p-1}{2}}+1\equiv 0$

$\Leftarrow 1+\left(x^{\frac{p-1}{8}}\right)^4$ نختار حينها أن يكون $p\equiv 1\,mod\,8$ (لاحظ الخباثة والاحترافية) إذاً يوجد حل $x$ في هذه الحالة

والآن كفكرة اخيرة لتنهي المسالفة

إذا كان $a$ حل عندها $p-a$ أيضاً حل وبالتالي أحد هذه الحلول سيكون أصغر من نصف $p$ ويحقق المطلوب.

دائماً في نظرية الأعداد في مسائل أوجد وما شابه ناقش الاتجاهيين فغالبا أحدهما أسهل من الاخر بدرجة عالية.

## محطة جديدة

**تمرين 1:** ليكن $p$ عدد أولي و $b_0$ عدد صحيح $0 < b_0 < p$ أثبت وجود متسلسلة وحيدة من الخانات.... $b_1, b_2, \dots, b_n, b_{n+1}$ في نظام الكتابة $p$ $\left(p\right.$ بدل النظام العشري$\left.\right)$ بحيث تحقق ما يلي:

لو أخذنا $x$ $x = b_n \dots b_2 b_1 b_0$ من أجل أي عدد $n$ عندها $x$ يحقق $x^p \equiv x \ mod \ p^{n+1}$

**الحل:**

الآن لو أخذنا $n = 0$ بمعنى $x = b_0$ الخانة التي أعطاها هو عندها يتحقق المطلوب بسهولة

$$b_0^{p-1} \equiv 1 \ mod \ p$$

بغض النظر عن قيمة $b_0$ المعطاة.

أما الآن لنحاول التخلص من الشكليات المعقدة الخاصة بالمسألة ونفهم معنى المسألة.

يريدني أن أثبت وجود خانة أضيفها للعدد الذي حقق الخاصية على $p^n$ لأنتقل به إلى $p^{n+1}$ (دون وجود ما يردعني أو يوقفني --خانة مقابل $p$ جديدة--).

لنجرب على $b_1$ بداية $\quad x = b_1 b_0 \quad \Leftarrow \quad x = b_0 + p b_1$

لنثبت وجود هذا الـ $b_1$ الذي يحقق:

$$(p b_1 + b_0)^p = p b_1 + b_0 \ \ mod \ p^2$$

الآن كيف لنا أن نفك الطرف اليسار الذي سيعطي الكثير من الحدود؟

بالفعل معظم الحدود ستحوي $p^2$ وستطير

$$b_0^p + \binom{p}{1} . b_0^{p-1} (p b_1) \dots + .. + .. \equiv p b_1 + b_0 \ mod \ p^2$$

إذاً لا يبقى سوا حد واحد

$$b_0^p \equiv b_0 + p b_1 \ mod \ p^2$$

الآن أصبح الأمر محلولاً لمَ؟

نلاحظ أنّ $b_0^p - b_0$ مضاعف للـ $p$ لذا يمكننا أن نختصر على $p$ ويبقى الناتج صحيحاً

$$\frac{b_0^p - b_0}{p} \equiv b_1 \ mod \ p$$

إذاً وعندها نختار الـــ $b_1$ هي القيمة التي على اليســـار (إذا لم يعجبك هكذا فقل $b_0^p - b_0 = p.k$ عندها نختار $k = b_1$)

الآن لنرى التعميم:

لدينا العدد $x = b_n \ldots . b_2 b_1 b_0$ يحقق (مجرد أن تعرف أن تسمي الـ$x$ يعني أنك داخل بقوة على المسألة

$$x^p \equiv x \ mod \ p^{n+1}$$

الآن العدد الجديد مع الخانة الجديدة $y = b_{n+1} b_n \ldots . b_1 b_0$ كيف سنكتبه

$$y = p^{n+1} b_{n+1} + x$$

نثبت وجود $b_{n+1}$ بحيث

$$(p^{n+1} b_{n+1} + x)^p \equiv p^{n+1} b_{n+1} + x \ mod \ p^{n+2}$$

نفك الطرف اليســـار كما فعلنا في المثال المصـــغر (دائماً حاول الاســـتفادة من طريقة تعاملك مع المثال المصغر إن أمكن)

$$x^p \equiv p^{n+1} b_{n+1} + x \ mod \ p^{n+2}$$

أيضاً: $x^p - x$ مضاعف لـ $p^{n+1}$

$$\frac{x^p - x}{p^{n+1}} \equiv b_{n+1} \ mod \ p$$

إذاً نختار لـ $b_{n+1}$ قيمة ما على اليسار

وبالتالي تم برهان المسألة.

■

**والآن إلى تطبيق عملي:**

أثبت وجود عدد $x \in \mathbb{N}$ يحقق المعادلة

$$x^3 + 17 \equiv 0 \ mod \ 3^n$$

من أجل أي $n$ (أي لكل $n$ نستطيع إيجاد $x$)

**الحل:**

هل هناك ترابط بين هذه المسألة وسابقتها ؟!!هذا من الواضح

أولاً من أجل $n = 1$ يوجد $x = 1$

ومن أجل $n = 2$ أيضاً يوجد $x = 1$

والآن كيف ننتقل من $3^n$ إلى $3^{n+1}$ ؟؟!بالضبط بإضافة خانة

أي ليكن $x$ يحقق $x^3 + 17 \equiv 0 \ mod \ 3^n$

نضيف $(x + 3^n t)^3 + 17$ على أن نختار $t$ لاحقاً.

$$\equiv x^3 + 3 \cdot 3^n t \cdot x^2 + 17$$
$$\equiv x^3 + 17 \ \ mod \ 3^{n+1}$$

عدنا إلى المقدار السابق ذو الـ $3^n$ وكأننا لم نستفد، لقد خسرنا الـ $t$ التي كانت عامل القوة لدينا

وفي مسألة الماضية لم نخسرها $(b_n)$ لأنها كانت على اليمين أيضاً. إذاً ما العمل؟ لابد من طريقة مقاربة

بالفعل نضيف $3^{n-1}t$ كي لا نخسر الحد، عندها:

$$(x + 3^{n-1}t)^3 + 17 \equiv x^3 + 3^n t \cdot x^2 + 17 \ mod \ 3^{n+1}$$
$$\equiv x^3 + 17 \ + 3^n t \cdot x^2 mod \ 3^{n+1}$$

نضع $x^3 + 17 = 3^n m$

$$\equiv 3^n m + 3^n t \cdot x^2 mod \ 3^{n+1}$$
$$\equiv 3^n (t \cdot x^2 + m) mod \ 3^{n+1}$$

وهذه خطية حتماً لها حل $t$ يناسب $x$ و $m$

مضروب بـ

نعامله حينها معاملة $(mod\ 3^2$

إذاً بالضبط هكذا يكون الحل ببساطة.

الآن أين موقع هذه النظرية من النظريات التي أخذناها؟!

لو لاحظنا أنها تستطيع إيجاد قوة كبيرة جداً لـ $p$ في $x^{p-1}-1$.

ربما قبل معرفة هذه النظرية قد يكون لدينا توقع أو إحساس بصعوبة الحصول على أي قوة لـــ $p$ في الشكل في الأعلى بسهولة.

بالإضافة لذلك في $lifting$ مثلاً $x^{(p-1)p^3}-1$ نلاحظ أن الـ $p^3$ في الأس تعطي 3 من $p$ في المقدار.

فلو طلب منا وجود 5 بالمقدار كاملاً عندها حصراً $x^{p-1}-1$ سيأخذ $p^2$ وهذا ليس بالأمر الصعب الآن عندنا ثقة.

إذاً وكأنها مربوطة بالحد الصغير من $lifing$.

## متتالية فيبوناتشي:

على الغالب فإن متتالية فيبوناتشي قد مرت معك في مسائل سابقة، فهي مشهورة كثيراً، وشهرتها لأهميتها كممثلة للكثير من المتتاليات، وخواصها وطرائق إثباتها تستخدم في مسائل متتاليات أخرى ...

إذاً **تعريفها**: $F_1=F_2=1$ ضروري جداً أن تحفظ أن الدليلين الأولين هما $F_1,F_2$ وقيمتهما $1,1$ لكي ينشئوا الحد $F_3=1+1$.

وعلاقتها التراجعية هي $F_{n+1}=F_n+F_{n-1}$، لاحظ $f_0$ سيساوي 0 لأن لكتابتها المختلفة كما تعلمنا جبرياً أن نكتب المتتاليات الخطية، سنستخدم جذور المعادلة $x^2=x+1 \Leftarrow x^2-x-1=0$

$r_1\left(\frac{1-\sqrt{5}}{2}\right)^n+r_2\left(\frac{1+\sqrt{5}}{2}\right)^n$ وباستخدام الحد الأول والثاني نوجد $r_1,r_2$

$$\Rightarrow F_n=\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

بشكل آخر:

$$= \frac{1}{\sqrt{5}}(a^n - b^n)$$

حيث $a, b$ جذور $x^2 - x - 1 = 0$

من أهم خواصها ... حساب الجمع $m + n$ (قاعدة الجمع):

$$f_{m+n} = f_m f_{n+1} + f_{m-1} f_n$$

الآن لإثباتها سنتناول المناقشة التالية ... لو أعطانا أحدهم حدين متتاليين ألن نستطيع حساب كل الحدود التي تليها؟ ... بالطبع وعملياً أكثر فنحن نستطيع حساب الحدود التي تليها بدلالة هذين الحدين المتتاليين كما حسبنا كل الحدود بدلالة $f_1, f_2$ والذان فاجآنا بكون قيمهما $1, 1$

$$\begin{aligned} f_{n+2} &= f_{n+1} + f_n \\ f_{n+3} &= f_{n+2} + f_{n+1} \\ &= 2f_{n+1} + f_n \\ f_{n+4} &= f_{n+3} + f_{n+2} \\ &= 3f_{n+1} + 2f_n \end{aligned}$$

الآن لاحظ وتأمل ما ضمن المربعات ... عندما تطلب مني حساب $f_{n+5}$ أوجد مخي طريقة سريعة لإيجاده، أجمع أمثال $f_{n+1}$ لوحدها و $f_n$ لوحدها: $f_{n+5} = 5f_{n+1} + 3f_n$

ولكن لاحظ الأمثال هي حدود متتالية لفيبوناتشي، ونحن نطبق نفس عملية فيبوناتشي على الأمثال

$$f_{m+n} = f_m f_{n+1} + f_{m-1} f_n$$

وطبعاً استخدمت المقارنة العددية (استخدام المثال) لمعرفة $f_m, f_{m-1}$ بدقة، أمر بسيط للغاية.

الخاصية الثانية هي عدة خواص إخوة:

إذا كان $m \mid n$ عندها $f_m \mid f_n$، وأبعد من ذلك: $gcd(f_m, f_n) = f_{\gcd(m,n)}$

إحدى الطرق وهي الأقوى أنه سنثبت الأخيرة وهي تعطينا الأولى اعتماداً بالتأكيد وكل التأكيد على:

$$f_{m+n} = f_m f_{n+1} + f_{m-1} f_n$$

من أسهل ما يكون إثبات أن $(f_{n+1}, f_n) = 1$، الان

القاسم المشترك لـ $d = (f_{m+n}, f_m)$ يقسم $f_{m-1} f_n$، ولكن $(f_{m-1}, f_m) = 1$، إذاً $d \mid f_n, f_m$ وطبعاً دون الـ $d$ (أي لو اختصرناه من الـ 3 حدود) لن يملك $f_m$ و $f_n$ أي شيء مشترك، وإلا دخل في $f_{m+n}$ وبالتالي $d$ هو الأكبر وبالتالي

$$(f_{m+n}, f_m) = (f_n, f_m)$$

أو كما تعودنا لحساب $gcd$: $(f_{m+n}, f_m)$ نضرب اليمين بـ $f_{n+1}$ ونطرحه من اليسار:

$$\begin{aligned} &= (f_{m+n} - f_m f_{n+1}, f_m) \\ &= (f_{m-1} f_n, f_m) \\ &= (f_n, f_m) \end{aligned}$$

يجب أن تصبح المناقشتان السابقتان بديهيتين (ربما أول مرة نستخدمهما لحل متتاليات مثلاً) ولكن الان عرفنا ..ولست مضطراً لمناقشتها كاملة بعد الان ..تقفز فورا الى النتيجة لو اردت

إذاً $gcd(f_{m+n}, f_n) = gcd(f_m, f_n)$، والآن حسب خوارزمية اقليدس نجد:

$gcd(f_m, f_n) = gcd(f_{m+n}, f_n) = f_{\gcd(m,n)}$ ويتحقق المطلوب.

كثير من المتتاليات تحقق أمور كهذه كالقسمة أو الاعتماد القريب على الدليل كمؤشر قوي للقيمة الخاصة بـ $F$ أصبح التعامل معها أسهل.

إثبات آخر لـ $F_n \mid F_m$ لوحده إذا كان $m \mid n$:

$$\frac{F_n}{F_m} = \frac{a^n - b^n}{a^m - b^m}$$

$$= \frac{a^{km} - b^{km}}{a^m - b^m} = a^{m(k-1)} + a^{m(k-2)}b^m \dots + b^{m(k-1)}$$

ولكن بما أن $a + b = 1$ و$ab = -1$ سنثبت بالاستقراء أن $a^r + b^r$ صحيح دوماً، وبالتالي المقدار المطلوب حسابه حتماً صحيح.

أو حتى يمكننا من إثبات ذلك على عدة خطوات (استقراء)، أي تبدأ بـ $2n$ $f_{m+n} = f_m f_{n+1} + f_{m-1} f_n$ بتعويض $m = n$.

الآن الخاصية الأقوى والتي تعتمد عليها الكثير من المسائل ليس فقط فيبوناتشي، **وهي الدورية** في أي $mod$ وأنها مضاعفة لأي عدد نحتاجه من أجل $f$ معين، مجرد إثبات الدورية يكفي، لأنه تذكر لدينا $\boldsymbol{f_0 = 0}$.

الآن كيف نثبت الدورية؟ نتخيل $mod$ عدد معين $(mod 7)$، الآن إذا تكرر $mod$ معين مرتيين هذا لا يعني أن العدد الذي بعده سيتكرر في المرة الثانية كما كان في المرة الأولى ، لأن ذلك صراحة يعتمد على العدد الذي قبل هذا الموود المكرر في كل من المرتيين.

إذاً ما الالتفاف على ذلك؟ سنأخذ أزواجاً ... هل عددها محدود؟ بالتأكيد، وبالتالي بنفس قوة مناقشة الأعداد بمفردها ... ولكن هذه المرة على الأقل نعرف أنه إذا تكرر زوج معين $(f_{m+1}, f_m) \equiv (f_{n+1}, f_n)$ عندها $f_{n+2} \equiv f_{m+2} \mod \Leftarrow (f_{m+2}, f_{m+1}) \equiv (f_{n+2}, f_{n+1})$، إذاً الزوج الذي يليه سيتكرر أيضاً، وبالتالي تبدأ الدورية ... ولمن لا يؤمن لنظرية $f_0 = 0$ أعطني الزوج $(1, 1)$ عندما يتكرر واحسب الزوج الذي قبله سيكون $(1, 0)$، إذاً أي عدد كان $n$ سيوجد $f_t$ معينة بحيث $f_t \equiv 0 \mod n$.

*_____*

الآن الأقوى من ذلك ... هل من أجل عدد أولي سيوجد كل البواقي في $mod p$؟ ... هل سنستفيد من كوننا أوجدنا الـ 0 للتو؟

نسخدم خاصية: $f_{m+n} = f_m f_{n+1} + f_{m-1} f_n$، كيف لنا بهذه العلاقة من 5 حدود أن نستخدمها؟ اخترناها في المقام الأول لأنها تعطي فكرة عن حدين بعيدين عن بعضهما بشكل منتظم، فتعطي الأمل بأن نتحكم بالبعيد ...

لكي نقلل الحدود نأخذ $n$ بحيث $f_n \equiv 0 \ (mod p)$

$$\Longrightarrow f_{m+n} \equiv f_m f_{n+1}$$

هنالك فائدة أخرى لاختيارنا $p \mid f_n$، هل تدرك ما هي؟ أن $f_{n+1}$ أولي مع $p$، ما فائدة ذلك؟ ... بالتأكيد إنه الشكل الذي يسكن أفئدتنا $ak, a^2k, a^3k$ ...

لم ينتهي الاثبات، فقد تعطي الاشكال $a^n k$ دائرة غير كاملة اذا وجدنا عدد $a^n \equiv 1 \ mod p$ اصغر من $n$ و $p-1$ ، عندها تلتفت لاحتمالية ألا تكون الجملة صحيحة، وبعد تجريب أرقام عديدة بالفعل نصل لمثال مناقض للاسف ...اي لا تحوي كل البواقي

الآن خاصية أخرى: أثبت أن: $F_{n+2} - 1 = \sum F_i$.

وخاصية أخرى هامة، إذا كان $n$ زوجياً فإن $F_n^2 + 1 = F_{n-1} F_{n+1}$،

وإذا كان $n$ فردياً فإن $F_n^2 - 1 = F_{n-1} F_{n+1}$، (**)

وأخرى $F_{n+1}^2 - 3F_n^2 + F_{n-1}^2 = 2(-1)^n$، وشبيهة بالشكل للسوابق، ولكن مختصرين فقط.

تحقق متسلسلة فيبوناتشي الفردية $F_{2n+1} = 3F_{2n-1} - F_{2n-3}$،

(*) $F_{n+1}^2 - F_n F_{n+1} - F_n^2 = \mp 1$

ولدينا بشكل مباشر من **علاقة الجمع** $f_{2n+1} = f_{n+1}^2 + f_n^2$ و $f_{2n} = f_n(f_{n+1} + f_{n-1})$، وطبيعي في العلاقة (*) أنه لربط عنصرين متتاليين ستزداد الدرجة التي يرفع لها حد فيبوناتشي، لأنه أدركنا مسبقاً أن حساب $f_{n+1}$ باستخدام $f_n$ صعب، وها هو مازال صعباً.

الآن معظم هذه الخاصيات مستوحاة من مسائل كانت فيبوناتشي جزء منها أو هي قد تكون مجموعة الحلول لاحد المعادلات الديوفنتينية (يساعدك جداً معرفة أن الحلول فيبوناتشي لأنك أكثر تمرساً عليها واكثر دراية بخواصها)

وعن مسألة أخرى فإليك هذه المسألة:

- أثبت أن $f_t + 1$ ليس عدداً أولياً مهما كان العدد الصحيح الموجب $t \geq 4$:

مجرد أننا جربنا جملة أنه هل فيبوناتشي يعطي كل البواقي يعني أنها الحالة الغالبة، وبالتالي لا نجرب كثيراً أن يكون $-1$ في $mod$ عدد إلى الأبد،

وتوزيع المهام على عدة $mod$ لا يجدي نفعاً من واقع خبرتنا مع نظرية الأعداد، بسبب وجود نظرية البواقي الصينية!

وما هي الصفات الأخرى التي تميز عدداً مركباً يمكن اختبارها؟ المشكلة أن كل ما نعرفه من قواعد نعرفها عن فيبوناتشي وليس $f + 1$، وبالتالي جاءت $f$ هي المشكلة، هناك من يستطيع حل مشكلة الـ 1 بالتأكيد،، $f_n^2 - 1 = f_{n-1}f_{n+1}$ من أجل $n$ فردي.

$$(f_n - 1)(f_n + 1) = f_{n-1}f_{n+1}$$

إذا كان $f_n + 1$ عدداً أولياً $\Leftarrow$ إما $f_n + 1 \mid f_{n-1}$ مستحيل، أو $f_n + 1 \mid f_{n+1}$ طبعاً $f_{n+1} > 2f_n \Leftarrow$

$f_{n+1} = f_n + 1 \Leftarrow f_n = 2$ وهذا تناقض لأن $t \leq 4$.

ماذا عن حالة $n$ زوجي؟

$f_n^2 + 1 = f_{n-1}f_{n+1}$ لا أرى $f_n + 1$ كأحد الجداءات، هذا يعني أن الطريقة تغطي الفردي فقط، وهي طريقة فاشلة، لا ... بهدوء سنحاول الالتفاف أولاً، ربما نحاول إظهاره في علاقة الفردي كـ $F_{n+1}$:

$$f_n^2 - 1 = f_{n-1}f_{n+1}$$
$$f_n^2 - 1 = f_{n+1}(f_{n-1} - 1) - f_{n+1}$$

نطرح $f_{n-1}$ أيضاً لنكمل المتطابقة أكثر:

$$f_n^2 - 1 = (f_{n-1} + 1)(f_{n+1} - 1) + 1 - f_{n+1} + f_{n-1}$$
$$f_n^2 - 1 = (f_{n-1} + 1)(f_{n+1} - 1) + 1 - f_n$$

تتمنى لو أن الـ 1 كحد تزال من الطرفين، ولكن تتذكر أنك جئت من علاقة بالأصل فيها $+1$ وبالتالي لا داعي لأن نأتي به إلا في علاقته:

$$f_n^2 + 1 = (f_{n-1} - 1)(f_{n+1} + 1) + 1 - f_n$$
$$f_n^2 + f_n = (f_{n-1} - 1)(f_{n+1} + 1)$$
$$f_n(f_n + 1) = (f_{n-1} - 1)(f_{n+1} + 1)$$

اذا هذا شكل جديد وظريف للعلاقة (**)

حيث $n$ زوجي، وبنفس المناقشة نصل للتناقض، وصراحة من هذه العلاقة كافية للتناقضين معا.

* _____ *

## المتتاليات:

الآن بعد استعراض فيبوناتشي نتذكر أن أكثر مسائل "الشورت ليست" هي متتاليات وليست فيبوناتشي بالضرورة، بل وأكثر من ذلك فهي مع التوابع ومع نظم العد ومع حساب البواقي الطويلة تمثل 90% من المسائل 5, 2 من معظم المسابقات ... الآن لنبدأ بها إذاً.

أولاً علينا حتماً أن نكون على اطلاع على مسائل المتتاليات الجبرية وآليات التعامل معها حتماً، فقد تكون جزءاً حيوياً من مسألة نظرية الأعداد، ثم عليك بحل المسائل التالية بالمتتاليات التي يمكن أن نعتبرها بسيطة ولكن ليس للغاية، فهي لا تتطلب تراكب أفكار وتعقيد.

***A.*** إذا كان $a_0 = 1$ و$a_{n+1} = 2a_n + \sqrt{3a_n^2 - 2}$، أوجد الصيغة المغلقة للمتتالية:

أولاً هذا شكل تراجعي غير مريح أبداً لابد أن نتخلص منه ووضوحاً صعب جداً لأنه يربط بين حدين متتاليين فقط ... إذاً يجب أن نبحث عن شكلها عندما كانت بثلاث حدود،

سهلة، نربع ثم ناخذ العلاقة التي تليها ونطرح، لأنه كما كان يحدث في كثيرات الحدود سيحدث اختصار حتماً

$$(a_{n+1} + a_{n-1} - 4a_n)(a_{n+1} - a_n) = 0$$

نرى هنا احتمالين لـ $a_{n+1}$ أي منهما نختار؟

بالطبع اليسار، لأن اليمين بتعويضه في العلاقة الأساسية نصل إلى تناقض، وهذا الخيار تولد أصلاً **بسبب التربيع**، إذاً: $a_{n+1} = 4a_n - a_{n-1}$، اذا هذا هو الاصل الذي جاءت من علاقة المسالة

والآن إيجاد الصيغة المغلقة سهل للغاية تعلمناه في متتاليات الجبر.

***B.*** لنتأمل المتتالية $a_1 = b\ ,a_2 = c$: $a_{n+2} = |3a_{n+1} - 2a_n|$، أوجد جميع الأزواج $(b, c)$ التي لأجلها تتضمن المتتالية عدداً محدوداً من الأعداد المركبة:

بتجربة عدة أزواج سنلاحظ أمراً هاماً (انتبه في هذا النمط من المسائل ستلاحظ أن **التجربة هامة جداً** وضرورية لاكتشاف أمور عديدة، ولتصبح المسألة أكثر منطقية ولتكتشف أين موضع الضعف في المسألة) سنلاحظ أنه إذا كنا عند زوج الحد الثاني أكبر أو يساوي الأول ستصبح المتتالية بعدها متزايدة، وسيصبح المقدار داخل القيمة المطلقة موجباً دوماً.

إذاً هل من مهرب من هذه الحالة؟ ... بالتأكيد لا، افرض أن التناقض مستمر، سنصل لقيمة سالبة وهذا غير ممكن، وبعد أن نصل للتزايد تصبح المتتالية $a_{n+2} = 3a_{n+1} - 2a_n$ كيف نثبت أنها تحوي عدداً غير منتهٍ من الأعداد المركبة؟ في هذه المرة بسيطة، يمكننا الاعتماد على رقم واحد.

وكما في فيبوناتشي نثبت الدورية، فقط نحتاج لـ 0 الأولي لكي يتكرر، بسهولة نختار عدداً أولياً في $b$ أو في $c$ وتنتهي المسألة.

محاولة الكتابة الصيغة المغلقة بالتأكيد سيحل المسألة أيضاً بسهولة، ولكن لو لم تكن الأرقام 3, 2 ربما لم تكن بنفس السهولة.

المسألة الثالثة ستكون أكثر جدية:

C. لتكن $a, b$ أعداداً صحيحة أكبر من 1 والمتتالية ... $x_0, x_1, x_2,$ معرفة كما يلي: $x_0 = 0\ , x_1 = 1$ و $x_{2n+1} = bx_{2n} - x_{2n-1}\ \ , x_{2n} = ax_{2n-1} - x_{2n-2}$، أثبت أنه لأي عددين طبيعيين $n, m$ فإن $x_{m-1}x_m \mid x_{n+1}x_{n+2} \dots x_{n+m}$:

الآن أكثر ما يزعجنا هو أن تظهر $b$ في خطوة ثم الـ $a$، ولكن ما الحصيلة؟ هل يتفاضل $b$ بظهور أكثر كونه الأول؟ ... كيف سأعرف؟ ببساطة بأخذ خطوتين دائما.

أي نبدأ مثلاً بفردي وننتقل إلى الفردي، المشكلة أنها تقيد إعطاءنا زوجي ... إذاً كيف نعزل لو قررنا الفردي عن الزوجي؟ (كما تعلمنا في المتتاليات الجبرية كيف نعزل متتالية $a_n$ من جملة معادلتين بـ $b_n, a_n$)

سنقوم بالمثل في العلاقة $x_{2n} = ax_{2n-1} - x_{2n-2}$، سنضربها بـ $b$ وسنعوض $bx_{2n}$ و $bx_{2n-2}$من العلاقة الأخرى، نسخدمها مرتين فنحصل على $x_{2n+1} = (ab-2)x_{2n-1} - x_{2n-3}$ ممتاز جداً، هناك شيء رائع جداً في هذه العلاقة وسيكون هذا الشيء الرائع نفسه موجودت في علاقة الزوجي، هو أن $a$ اجتمعت مع الـ $b$ لتشكل مجهولاً محايداً.

الآن نلاحظ مدى الاستقلال الهائل بين الزوجي والفردي، لذا سنحولهم تماماً إلى متتاليين مختلفين، ولكن ماذا عن الطلب؟

سيأخذ كل من $x_m, x_{m-1}$ حدود الموافقة من $x_{n+1}x_{n+2} \dots x_{n+m}$، ولاحظ أن $x_m$ سيصبح $y_{\lfloor \frac{m}{2} \rfloor}$ وعدد الأعداد المطلوب أن يتواجد فيها أيضاً نفس العدد $\left\lfloor \frac{m}{2} \right\rfloor$، ممتاز جداً وكأن الطلب لم يتغير بل تحول إلى متتاليتين مستقلتين، نثبت على واحدة والثانية تتبع وحدها ،، أن المتتالية $y_{k+1} = (ab-2)y_k - y_{k-1}$ تحقق أن $y_t \mid y_{n+1}y_{n+2} \dots y_{n+t}$، ستقول لي بسيطة سنستخدم $f_{m+n} = f_m f_{n+1} + f_{m-1}f_n$، ولكن هنا الأمور ليست نفسها تماماً كفيبوناتشي، لذا **نعود لطريقة إثباتها**:

نبدأ من عند الـ $y_t$ نفسها (بالنسبة للزوجي): $y_1 = 0\ \ \ y_2 = a$ ،

$$y_{t+2} = cy_{t+1} - y_t$$
$$y_{t+3} = (c^2 - 1)y_{t+1} - cy_t$$

حيث: $f_{m-1}(c) = cf_{m-2}(c) - f_{m-3}(c)$ ، $c = f_1(c)$ ، $f_0 = 1$، لا يهمني كيف يبدو التابع.

الآن $y_{t+m} = f_{m-1}(c)y_{t+1} - f_{m-2}(c)y_t$ من أجل أي $t$ أو $m$ تتمناه.

الآن أخذنا $t$ بشكل عام بدواعي قسمة، ولكن لو طلب منا حساب الصيغة المغلقة سنضع $t = 1$

$$y_{m+1} = af_{m-1}(c)$$

هذه هي الصيغة المغلقة، والآن نعوض بدل الـ $f$ الدخيل بـ $y$ لنعود للقسمة:

$$y_{t+m} = \frac{y_{m+1}y_{t+1}}{a} - \frac{y_m y_t}{a}$$

(عرفت الان لم لم نوجد صيغة ال $f$

$$y_{t+m} = \frac{y_{m+1}y_{t+1} - y_m y_t}{a}$$

الآن ببساطة نأخذ $mody_t$ ونعوض $m = t - 1$ 9

... ثم نثبت أن واحد من الأعداد $y_{n+1}, y_{n+2}$ ... $y_{n+t}$ ( $t$ حدد متتالي) مضاعف لـ $y_t$.

*_____*

- مسائل الأوجد

- أثبت أنه من أجل أي عدد طبيعي $a_1 > 1$ يوجد متتالية متزايدة من الأعداد $a_1, a_2$ ... بحيث $a_1 + a_2 \ldots + a_n \mid a_1^2 + a_2^2 \ldots + a_n^2$:

يجب ألا تتلبك من الشكل أو نأخذ الأمور كلها بدفعة واحدة أو محاولة تخيل شكل لكل $a_i$ (والتي طبعاً ستجرب بها بدايةً، وربما تعجز)

تبدأ بـ $a_1 + a_2 \mid a_1^2 + a_2^2$، تلاحظ بسهولة القدرة على التعويض: $a_1 + a_2 \mid 2a_1^2$، لاحظ عوضنا $a_2$ بدلالة $a_1$ وليس العكس، وكل ذلك إشارات لوجود استقراء واستفادة من القديم بالجديد،

$a_1 + a_2 + a_3 \mid a_1^2 + a_2^2 + a_3^2$، لقد حددنا $a_1, a_2$، لكن كيف سيتصرف $a_3$؟ بالطبع:

$$a_1 + a_2 + a_3 \mid a_1^2 + a_2^2 + (-a_1 - a_2)^2$$

ومن ثم نختار $a_3 = (-a_1 - a_2)^2 + a_1^2 + a_2^2 - a_1 - a_2$، هكذا ببساطة ووضوح نجد أن المتتالية متزايدة وبالتالي هذا هو المطلوب #.

**D.** لنفرض المتتالية من الأعداد الصحيحة غير السالبة $a_1, a_2 \dots a_{1997}$ تحقق $a_i + a_j \le a_{i+j} \le a_i + a_j + 1$ لكل $i, j \ge 1$ ليس بالضرورة مختلفين، أثبت أنه يوجد عدد حقيقي $x$ بحيث يحقق: $a_n = \lfloor nx \rfloor$ ، $1 \le n \le 1997$:

أولاً نلاحظ من تعريف المتسلسلة بأن $a_{i+j}$ إما أن يكون مجموع الحدين أو مجموعهما $+1$، أي بشكل عام إضافة الحدين والاكتفاء أو نضيف 1 على ذلك المجموع.

والمطلوب هو البحث عن ذلك الـ $x$ الذي هو بمثابة وسيط روحي للمتتالية الذي سيساعد كل حدود المتتالية، فجزؤه العشري يراعي بعد ضربه بـ $n$ أن يكون ضمن الحد الأعلى والأدنى، أي $a_n, a_{n+1}$.

طبعاً هنالك حدود لمسايرته مهما كان هذا ال$x$، إذاً علينا أن نثبت أن المتراجحة مشابهة لبناء الفلور فلا تسمح بأخطاء لا يتحملها هذا ال $x$.

أولاً: $a_1 = \lfloor x \rfloor$، نلاحظ أن هذا الـ $\lfloor x \rfloor$ هو الأرضية الأساس فسيكون $n\lfloor x \rfloor \le a_n \le n\lfloor x \rfloor + n - 1$ وضوحاً من المتراجحة الأساسية وهي معنوياً تنفي أن $a_n$ سيحوي الـ $n\lfloor x \rfloor$ حتماً، ولكن فوق ذلك قد يضاف إليه من $0 \longleftarrow n - 1$ بحسب عدد الخطوات التي تزيد 1 والتي يجب أن يحددها $\{x\}$، إذاً كل المسؤولية على $\{x\}$، لذا نتخلص من $\{x\}$ بإنشاء متتالية جديدة: $b_n = a_n - n\lfloor x \rfloor$، نلاحظ أنها تحقق $b_i + b_j \le b_{i+j} \le b_i + b_j + 1$ ، $b_i = \lfloor n\{x\} \rfloor$ ، $b_1 = 0$.

الآن كل ما فعلناه هو إراحة مخنا من كثرة المعلومات ولنزيد سيطرتنا على الوضع.

والآن جاهزون لنرى ما هي الأمور التي قد لا يتحملها $\{x\}$، فهو عدد حقيقي وقوي جداً وقادر جداً على التلبية، لذا نترك الأمور عليه:

$$b_i = \lfloor i\{x\} \rfloor$$
$$b_{i+1} \ge i\{x\} \ge b_i$$
$$\frac{b_{i+1}}{i} \ge \{x\} \ge \frac{b_i}{i}$$

لدينا $n$ متراجحة من هذه، يمكن إيجاد هذا الـ $\{x\}$ السحري إن لم يتدخل أحد الحدود اليمينية مع اليسارية، أي علينا إثبات أن: $\frac{b_{i+1}}{i} \ge \frac{b_j}{j} \Longleftarrow jb_i + j \ge b_j i$ من المتراجحة بالطبع، نفرض العكس أن $jb_i + j \le b_j i$ بتجربة مثال نجد أنه علينا أن نعرف من الأكبر؟ $i$ أم $j$؟ لكي نطبق المتراجحة الأساسية،

إذا كان $i > j \Longleftarrow j(b_{i-j} + b_j) + j \le b_j i$ (ويجب أن نكون واثقين من هذه التطبيقة لأن الضعف سيأتي في تجزيء الطريق من $i$ إلى $j$، فالأقوى هو الوصول بخطوة واحدة)، والضعف أيضاً لو نزلنا بـ $b_i$ إلى $b_{j-1}$ مثلاً، إذاً بعد التطبيق:

$$jb_{i-j} + j \le b_j(i - j)$$

نلاحظ أن الشكل تكرر تماماً ولكن على $j$ ، $i-j$، مباشرة نأخذ استقراء ونصل إلى تناقض (حركة خبث)، ومن أجل $i \le j$:

$$jb_i + j \le ib_j$$

$$jb_i + j \le ib_j \le i(b_i + b_{j-i} + 1)$$

$$(j-i)b_i + j - i \le ib_{j-i}$$

أيضاً تكررت من أجل $i, i-j$ وطبعاً بالاستقراء نصل للتناقض ولصحة العلاقة المطلوبة وهو المطلوب #.

**ملحوظة:** قد يخطر لك أن تؤدي ذلك مباشرة وتحل معك بعدة سطور، ولكن لو ضعت ولم تخطر معك فهذا هو السبيل الهادئ والآمن للوصول.

**E.** تعطى المتتالية $\{a_n\}$ بالعلاقة:

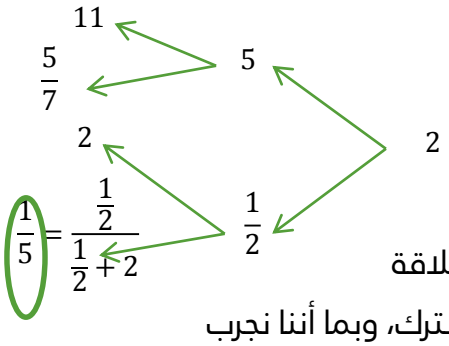
$$a_{n+1} = \begin{cases} \dfrac{a_n - 1}{2} & a_n \ge 1 \\ \dfrac{2a_n}{1 - a_n} & a_n < 1 \end{cases}$$

معطى أن $a_0$ عدد موجب صحيح $a_i \neq 2$ من أجل $n = 1, 2, \dots 2001$ و $a_{2002} = 2$، أوجد $a_0$:

لاحظ هنا أعطانا $a_{2002}$ وطلب حد قبله $a_0$، وبالتالي نوجد العلاقات العكسية $b_a = 2$

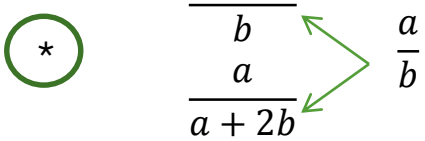
$$b_n = \begin{cases} 2b_{n-1} + 1 & b_a = 2 \\ \dfrac{b_{n-1}}{b_{n-1} + 2} \end{cases}$$

نلاحظ عدم وجود شرط لـ $b_{n-1}$ لكي تحسب لي $b_n$، أي دائماً هناك طريقتين، إذاً ما الذي يحدد لي قيمة $b_{2002}$؟ نعم مطلوب أن يكون عدداً صحيحاً:



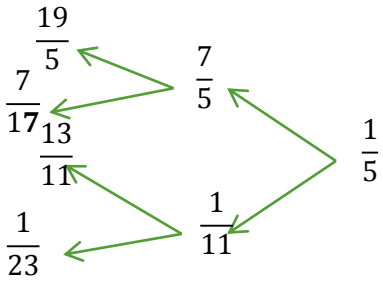

نلاحظ تطبيق العلاقة من المقام المشترك، وبما أننا نجرب وقتاً كثيراً الأولى سهلة، أما الثانية نتعذب، ودائماً نتخلص أرقام نحاول أن نسهلها لكي لا يأخذ التجريب

$$b_{n-1} = \frac{a}{b}$$




نلاحظ أن طريق 11 أظرف طريق – طريق الـ 2 مرفوض، أما $\frac{1}{5}$ ، $\frac{5}{7}$ سنجرب فيهم وفق *

الآن آلية حل الحالة هذه آلية مشهورة وتتكرر جداً في كثير من المسائل وخاصة مسائل الألعاب، وهي حيوية للغاية، وأكيد فيها أنها طريقة أيضاً نابعة من الإحساس والمنطق:




نلاحظ أنه مهما طالت العملية لا يحدث أي اختصار ... كيف سنحصل على عدد صحيح فجأةً إذاً؟ وما تفسير عدم وجود الاختصار؟

لدينا $\frac{a}{b}$ لا يوجد فيه اختصار لأنه $(a,b)=1$ و $a,b$ تمثل $\frac{1}{5}$ مثلاً أو الحالة الاستقرائية البدئية، الآن من أجل $\frac{2a+b}{b}$: $(2a,b)=(2a+b,b)=1$ لأن $b$ فردي و$a$ أيضاً، كيف نثبت أن $a,b$ فردي أيضاً؟ بالاستقراء $a,b$ فردي $\Leftarrow 2b+a,2a+b$ فرديان أيضاً، إذاً $(2a,b)=1$

ومن أجل $\frac{a}{a+2b}$: $(a,2b)=(a,a+2b)=1$ أيضاً، وبالتالي لا يوجد هنالك اختصارات وبالتالي لن نحصل على عدد صحيح في أي طريق يبدأ بكسر مقامه أكبر من 1 وبسطه ومقامه فرديان، إذاً:

$$b_n=3\cdot 2^n-1 \qquad b_{n+1}=2b_n+1 \qquad 11=2\times 5+1 \leftarrow 5^{b_1} \leftarrow 2^{b_0}$$

$$a_0=b_{2002}=3\cdot 2^{2002}-1$$

*_____*

والآن إليك هذ المسائل للتدريب، طبعاً المصادر التي أشرنا إليها بالترتيب ذاته ستكون غنية بمثل هذه المسائل، ولكن هذه مفضلة لدي.

المسألة الأولى (Apmo 2015):

متسلسلة من الأعداد الحقيقية $a_0,a_1$ ... يقال عنها جيدة إذا تحققت الشروط الثلاث التالية:

الأول قيمة $a_0$ عدد صحيح موجب.

لكن عدد صحيح غير سالب لدينا:

$$a_{i+1}=\frac{a_i}{a_i+2} \quad , \quad a_{i+1}=2a_i+1$$

يوجد عدد صحيح $k$ بحيث $a_k=2004$.

أوجد أصغر عدد صحيح موجب $n$ بحيث توجد متسلسلة جيدة $a_0,a_1$ ... من الأعداد الحقيقية مع الخاصية $a_n=2004$.

المسألة الثانية (ibroamerican 2009):

لتكن المتسلسلة $\{a_n\}_{n\geq 1}$ المعرفة كما يلي: $a_1 = 1\ ,\ a_{2k} = a_k + 1\ ,\ a_{2k+1} = \frac{1}{a_{2k}}$، لكل عدد $k \geq 1$ أثبت أن كل عدد نسبي موجب سيظهر مرة واحدة في المتسلسلة $\{a_n\}$.

والان نتابع تسلسل المسائل الاصلي:

**F.** أوجد جميع المتتاليات غير المنتهية المحدودة من الأعلى $a_2, a_1$ ... من الأعداد الصحيحة الموجبة بحيث يكون لكل $n > 2$:

$$a_n = \frac{a_{n-1} + a_{n-2}}{\gcd(a_{n-1}, a_{n-2})}$$

الآن بعد تأمل المتتالية سنعوض $a_{n-1} = da'_{n-1}$ و $a_{n-2} = da'_{n-2}$ وتجد أن: $a_n = a'_{n-1} + a'_{n-2}$، هذا يعني أن $(a_n, a'_{n-1}) = 1$، هل إذاً نعوضها في العلاقة التي تليها ويصبح $(a_n, a_{n-1}) = 1$ والأمور بسيطة؟ ... لا ... لأن $a_n$ قد يشترك مع $d$ الذي حذفته، إذاً:

$$\gcd(a_n, a_{n-1}) = (a_n, a'_{n-1}\ d) = (a_n, d) |\ d$$

إذاً هو أحد قواسم $d$ والتي يمكن أن تكون كثيرة ... إذاً ما فائدة ذلك؟ ... بالطبع لا تدع أي فائدة تغفل عنك، انسَ كل عالم المتتالية وركز على فكرة $d_2 \mid d$، نعم إنه الـ $d$ (القواسم المشتركة لـ $(a_i, a_{i+1})$ متناقصة، وطبعاً لديها حد للتناقص التام، فهي فقط ضمن قواسم الـ $d$).

هذه المعلومة في الجملة السابقة ضعيفة، ولكن عبرنا عنها كما يلي، أنه بما أننا لن تستطيع التناقص التام باستمرار، لذا سيوجد قيمة لـ $\{d\}$ تبقى ثابتة للأبد (هنا القوة في استثمار الفكر، نضع قيمة ثابتة t لـ gcd)

$$a_n = \frac{a_{n-1} + a_{n-2}}{t}$$

ماهو الشيء السيئ في هكذا متتالية ....نكشف الحقيقة سريعاً بالتجربة ... جرب $t = 10$، سنلاحظ هبوطاً دراماتيكياً في قيم أول عنصرين بدأت بهما، وتثبت أنها متناقصة تماماً ونصل لتناقض.

هل 10 كبير؟ نجرب 3 وأيضاً نصل لتناقص تام في قيم الحدود، وطبعاً $t = 1$ مرفوض لأن المتتالية تتزايد وتصبح غير محدودة $\Leftarrow t = 2$ هو الـ gcd الذي سيثبت عنده

$$a_n = \frac{a_{n-1} + a_{n-2}}{2}$$

وكل الأعداد يجب أن تكون زوجية.

هذا متوسط حسابي، والجميل بالمتوسط الحسابي أن القيمة تكون بين العددين تماماً إلا إذا تساوى العددان، وهذا مرفوض لأن قاسمهما المشترك الأكبر هو 2، إلا إذا كان كلاهما يساوي 2، نفرض أن ليس كلاهما يساوي 2، سيكون المتوسط بينهما تماماً ...

وبتكرار العملية عدة مرات لن يبقى هناك متسع من الأماكن لأعداد صحيحة جديدة، وبالتالي

$$2 = a_{r+1} = a_r$$

*_____*

**G.** لنعرف المتتالية $\{c_n\}$ بحيث يكون $0 \leq n$ و $x_0 = 0$

$$x_n = \begin{cases} x_{n-1} + \dfrac{3^{r+1} - 1}{2} & : n = 3^r(3k+1) \\ x_{n-1} - \dfrac{3^{r+1} + 1}{2} & : n = 3^r(3k+2) \end{cases}$$

أثبت أن كل عدد صحيح سيكون موجوداً مرة واحدة فقط:

لاحظ أنها علاقة تراجعية، ولكن كل ما ستتم إضافته يتعلق بـ $n$ فقط، والمقادير التي سيتم جمعها معروفة في لحظة.

سنسميها $b_n$ والتي ستعبر عن المقدار الذي سنضيفه لـ $x_{n-1}$ لنحصل على $x_n$، أي $b_n = x_n - x_{n-1}$، أي الشكل $\frac{3^{r+1}-1}{2}$ أو الشكل الآخر هو الـ $b_n$، والآن في هذه المسألة صراحةً لا أستطيع أن أقول لك جرب استنتج أثبت حتى لو كان الاستنتاج مركباً وليس بسيطاً.

كيف سنوسع الأعداد الطبيعية والسالبة ضمن حدود المتتالية بدءاً من $x_1$ في أرقام الحدود الموجبة؟ ... يعني أن أول $n$ حد لن يحتوي الأعداد من $1 \leftarrow n$ بالتأكيد ... كيف تتوقع أن يكون التوزيع؟ جرب واستنتج.

**H.** لتكن $a_1, a_2$ ... متسلسلة من الأعداد الصحيحة الموجبة التي تحقق الشرط:

$0 < a_{n+1} - a_n \leq 2001$ لكل الأعداد الصحيحة $n \geq 1$ ، أثبت أنه يوجد عدد غير منتهٍ من الأزواج $(p, q)$ بحيث $p \neq q$ :$a_p \mid a_q$

الحل

ربما ستقول في قلبك يقيناً هذه ليست مسألة إنشاء متسلسلة تحقق، ولكن عملياً تتطلب نفس المهارات والإبداع.

لاحظ أن المعطى قليل جداً جداً ... ولكن القسمة مسايرة جداً بطبيعتها لذلك سيكون المعطى كافياً ... بالطبع إذا أخذنا $a_p$ ونظرنا إلى مضاعفاته سيكون الأفق أوسع من التفكير بـ $a_q$ والنظر لقواسمه.

بعد عدة خطط واستراتيجيات مثل المتراجحات (أي مضاعفات كل حد كم تعطي) فكرة قوية ولكن ستفشل.

ستأتي إلى الاستراتيجية المحتمة، وهي أن توحد المجهول لتعطي 2001 عدداً متتالياً، ستقول نظرية البواقي الصينية:

$$n \equiv 1 \; moda_{i_1}$$
$$n \equiv 2 \; moda_{i_2}$$
$$n \equiv 2001 \; moda_{i_{2001}}$$

لو وجد هذا الـ $n$ فهو يحقق حتماً، ولكن من الصعب إثبات وجوده لأنه يتطلب إثبات أن أي قاسم مشترك أكبر $d$ بين هذه الأعداد أقل من 2002 لأنه عندها $i \equiv j \; mod \; d \quad , \quad i, j < 2002$، وبالتالي اقتربنا جداً ولكن يبدو أننا سنحمل عبء الإنشاء كلياً.

لو حاولت بعدد واحد (بباقٍ واحد على 2001) لن تصل أبداً للحل، فمضاعفته تبدي إمكانيات كثيرة، ولكن لا يمكن استثمارها لوحدها.

خذ 2001 عدداً متتالياً، الآن ولّد منها مضاعفات..... 2001 عدداً متتالياً، ببساطة إذا كانت الأعداد $x_1, x_2, \ldots \; x_{2001}$ سأضع متسلسلة جديدة على $1 \leq i \leq 2001$: $\prod_m x_m + x_i$ أيضاً 2001 عدد متتالي ولاحظ انه كل $\prod_m x_m + x_i$ مضاعف ل$x_i$ فاختيارنا للشكل كان مبدعا

..وبالتالي من كل من هذه المتسلسلتين سنختار عنصر $a_k$، حتماً اثنان بـ$i$مختلفة، لا يجوز تكرار الi ذاته لانه سنحصل على عدد مضاعف للاخر وتنتهي المسألة

... الآن تتذكر ما قلته عن عدم الخوف من الأعداد الكبيرة أو عدم ضرورة تخيل مخك لحجم المقدار الذي ستكتبه وكيف يجب ألا يؤثر عليك هذا الحجم

نأخذ $\prod(\prod x_i + x_i) + \prod_m x_m + x_i$ متسلسلة ثالثة من 2001 عدد متتالي (نلاحظ ان كل حد منها مضاعف ل$\prod_m x_m + x_i$ لذا سناخذ من هذه المتسلسلة الثالثة عنصر بـإٍ ثالثة مختلفة ايضا لكي لا نحلص على عددين مضاعفين لبعضهما، الآن لو كنت جيداً بالترميز ستريح نفسك، سمِّ $y_1 = \prod x_i$ أي

المتسلسلة الاولى $x_i$

المتسلسلة الثانية $y_1 + x_i$

(جداء مركب مرة واحدة،) وسمِّ $y_2 = \prod(y_1 + x_i)$،

المتسلسلة الثالثة $y_2 + y_1 + x_i$

الآن المتسلسلة الرابعة ننشؤها بنفس الطريقة تصبح ببساطة: $\prod(y_2 + y_1 + x_i) + y_2 + y_1 + x_i$،

ونسمي $y_3 = \prod(y_2 + y_1 + x_i)$،

فتصبح المتسلسلة الرابعة $y_3 + y_2 + y_1 + x_i$

وبالطبع لا نكتفي وننشئ المقدار الذي نريده من المتسلسلات، ولكن يكفينا 2002 لنضمن تكرار أحد الi أو الـ $x_i$ مرتين وسيكون هذان العنصرين يحققان ان احدهم مضاعفا للاخر.

اضطر لإنشاء عددين مضاعفين لبعضهما في يوم من الأيام.

## بوابة جديدة

والآن ننتقل إلى نمط من المسائل وورودها شائع جداً في المسابقات العالمية وبالإضافة للشورت ليست **short list** وهي مسائل تطلب منك إثبات وجود سلسلة أو متتالية أو عدد ما يحقق خاصة مطلوبة وقد يطلب إيجاد متتالية بأي حجم مهما كبر، وهنا يكمن التحدي.

والهدف في هذه المسائل ليس بالضرورة إيجاد الأرقام التي تحقق خاصة معينة، فقد يُطلب فقط إيجاد طريقة إنشاء لها كالاستقراء والبواقي وغيرها.

الآن نبدأ ببعض الأمثلة البسيطة:

أثبت وجود عدد غير منتهي من الأعداد التي لا تحوي الخانة "0" في تمثيلها العشري وتحقق أن مجموع خانات أي عدد منها يقسم هذا العدد.

**الحل:**

لكي أثبت أن العدد مضـــاعف لمجموع خاناته بغض النظر عن قيمة هذا المجموع لا بد أن يكون هذا العدد الذي نختاره جيد الكتابة بالترميز وليس فقط في النظام العشري.

ما هي الأعداد التي تعرفها تحقق ذلك؟!!

لدينا

$$\frac{10^n-1}{9}=\underbrace{1111111}_{n \text{ مرة}}$$

هل هذا يحل المسألة؟

نعم ولكن نختار أعداد معينة لـ $n$ ما هي؟

$10^n-1$ يحوي 9 في $10-1$ وهي موحية ب $LTE$ وبالتالي نجعل $n=3^k$ من أجل أي $k$ عندها تحقق المطلوب.

**المثال الثاني:**

أثبت أن أي عدد صحيح يكتب على شكل مجموع مكعبات خمس أعداد **صحيحة**.

**الحل:**

لاحظ أن الأعداد صـحيحة وبالتالي يمكن السـالب وعندها يمكن للفرق بين المكعبين أن يكون صـغيراً وليس بهذا التباعد

كيف نعبر عن ذلك رياضياً

$$(k+1)^3 - k^3 = 3k^2 + 3k + 1$$
$$k^3 - (k-1)^3 = 3k^2 - 3k + 1$$

وأصغر من ناتج الطرح هو طرح ما في الأعلى السطرين

نحصل على 4 مكعبات ب

$$(k_1)^3 + (k-1)^3 - 2k^3 = 6k$$

ولكن $6k$ لا تعطي كل الأعداد رغم أنها خطية بسبب الـــ 6 إذاً: سنجعل من المكعب الخامس فقط ليصلح الباقي على 6 ونعم المكعب يعطي كل البواقي على 2 و3 وبالتالي على 6.

**المثال الثالث:** إذا كان $a = 3k^2 + 3k + 1$ أثبت أن $2a$ و $a^2$ كل منها يكتب على شكل مجموع 3 مربعات حيث $a, k \in \mathbb{Z}$.

**الحل:**

$$2a = 6k^2 + 6k + 2 = (2k + 1)^2 + (k + 1)^2 + k^2$$

مباشرة لاحظ أن $2k + 1 = k + 1 + k$ وخاصة لـ $a^2$ فربما تدل على شيء، $a, b, a + b$

وأيضاً الخبرة في المعادلات الديوفانتية تشير لنا أن $2k + 1, k + 1, k$ هي حلول $(x, y, z)$ لـ

$$x^4 + y^4 + z^4 = 2x^2y^2 + 2y^2z^2 + 2z^2x^2$$

يمكنك التعويض والتأكد ومن ثم الاعتياد على الخاصية

ولكن هذا كيف يوصلنا للمطلوب؟!! حاول بيدك

$$x^4 + y^4 + z^4 + 2\sum x^2y^2 = 4\sum x^2y^2$$

$$\left(\sum x^2\right)^2 = 4\sum x^2y^2 \Leftrightarrow \left(\frac{\sum x^2}{2}\right)^2 = \sum x^2y^2$$

لاحظ موقع $2a$ أين هي الآن ومربعاتها الثلاث

وبالتالي:

$$(3k^2 + 3k + 1)^2 = \big(k(k + 1)\big)^2 + \big(k(2k + 1)\big)^2 + \big((k + 1)(2k + 1)\big)^2$$

■

والآن إلى مسائل أصعب.

**المسألة الرابعة:**

أثبت أنه من أجل أي عدد طبيعي $n \geq 2$ يوجد متتالية من الأعداد الصـــحيحة $(a_1, a_2, \dots, a_n)$ بحيث أنه من أجل أي عددين $i, j$ يتحقق ما يلي

$$i \neq j \quad a_j - a_i \mid a_j + a_i$$

**الحل:**

الآن كيف نبدأ بمثل هذه المسألة؟!!

ربما نجرب إيجاد مثال 3 أعداد أو 4 وهنا نلاحظ أننا يطلب منا جعل الأعداد قريبة فيما بينها مع جعل مجموعها كبيراً كفاية وسنلاحظ أن أي عددين متتاليين يحققان أو أي عددين مختلفين بـ 2 أيضاً.

وهنا يتضح ما يجب علينا فعله في كل هذه المسائل: أن نوجد أشياء سريعة لإيجاد مثل هذه الثنائيات التي تحقق الخاصية انطلاقاً من $a_i$ لإيجاد $a_j$ المناسب مثلاً.

أو إيجاد ثنائية انطلاقاً من أخرى ولكن الأهم أنه "بسرعة" أو "بسهولة".

وأهم ما قد نستنتجه أنه يمكن أن نضرب العددين بـ $t$ معين دون أن يتغير شيء في هذه العلاقة وأن ضرب كل الأعداد بـ $t$ ولا يتغير شيء.

**والخطوة الثانية** استنتاج أنه لو جمعنا لكل الأعداد $m$ معين لا يتغير الطرح وهذا جيد كفاية لأن الفروق هي المقام والتي هي الأصعب في التلاعب دائماً

الآن

$$a_i - a_j \mid a_i + a_j + 2m$$
$$a_i - a_j \mid 2m \quad \Leftarrow$$

إذا ببساطة نذكر أن نضع الفروق في $m$

أو يمكن إذا تذكرنا $a_i - a_j \mid 2a_i$ إذا جعلنا $a_i \mid m \Leftarrow a_i - a_j \mid 2a_i \mid m$ لذا نضــع كل $a_1, a_2, \dots, a_n$ مع 2 إضافية في $m$

كيف نستفيد من هذه الاكتشافات... طبعاً بوضوح

الآن نفرض بالاستقراء أننا أوجدنا $n$ عدداً ونريد إنشاء عدد جديد $a_{n+1}$ (بذلك نتخلص من عبء وحمل

الـ $n$ عدد $(a_1, a_2, \dots, a_n)$

بالتأكيد لن نحافظ على استخدام هذه الـ $n$ عدد بذاتها دون أي تعديل عليها لأنها داخلة في القسمات الجديدة التي تحوي $a_{n+1}$ ومع تقدم الحدود $a_i$ ستصبح صغيرة جداً بالنسبة للحدود الجديدة لذا سنعطيها تعديلاً محترماً وننشئ على أساسها $a_{n+1}$

التعديل هو $(ta_1 + m, ta_2 + m\ , ta_3 + m)$ حيث $t, m$ عوامل قوة لنحددها فيما بعد (ضروري هذا التصرف في مثل هذه المسائل)

$$a_{n+1} - ta_k - m \mid a_{n+1} + ta_k + m$$

الآن نختار $a_{n+1}$ قبل $m\ , t$ لندعهم للأخير حتى تتوضح معالم القسمة

ونذكر لتختار $a_{n+1}$ اختار بما يراعي المقام (الأخبث) ثم البسط يحل أمره

إذاً نضع $a_{n+1} = m$

$$t\ a_k \mid\ ta_k + m$$
$$t\ a_k \mid m \quad \Leftarrow$$

نضع $t = 1$ لأنه أصبح دون فائدة ونضع

$m = a_1 a_2 \dots . a_n$ (هنا صدفة كانت $m$ تحوي جداءات والـ $a_i$ كما اشترط لها في البداية)

وبهذا تتم كل علاقات القسمة وتنتهي المسألة.

**المسألة الخامسة:**

أثبت أنه من المجموعة الغير منتهية

$$\{a^2+a-1, a^3+a^2-1\ , a^4+a^3-1, \dots.\}$$

يمكن إيجاد عدد غير منتهي من العناصر بحيث كل اثنان منها أوليان فيما بينهما.

**الحل:**

الآن بالفعل ستحاول أن تبحث عن حساب القاسم المشترك

$$(a^{n+1}+a^n-1, a^{m+1}+a^m-1)$$

ولكن هذا لا يحسب نهائياً أي أننا لا نحصل على عدد ثابت أو واحد أو مقدار يحوي على $a$ دون $m\ , n$

لذا كيف نعرف أننا وصلنا لأبسط شكل؟!!

إذا وصلت لحدين بدل من 3 فهذا إنجاز كافي

$(a^{n+1}+a^n-1\ , a^{m+1}+a^m-1)$ نضرب $a^{m+1}+a^m-1$ بـ $a^{n-m}$ ونطرحه من الأيسر.

$$(a^{n+1}+a^n-1-a^{n+1}-a^n+a^{n-m}, a^{m+1}+a^m-1)$$
$$=(a^{n-m}-1, a^{m+1}+a^m-1)$$

ممتاز. الآن نتذكر أننا نبحث عن **ثنائية سريعة** $m, n$ **(شروط بسيطة)** تحقق أن هذا الـ $gcd = 1$

طبعاً نحن نعرف كيف أنه من المسموح والمفتوح التعامل بالـــ $mod$ داخل الـــ $gcd$ والتعويض وكل هذه الأمور وبالتالي يمكننا أن نعوض $a^{n-m} \equiv 1$ في الطرف الايمن لذا نجعل $m \mid n-m \Leftarrow$

$$(a^{n-m}-1, a^{m+1}+a^m-1)=(a^{n-m}-1, a+1-1)=(a^{n-m}-1, a)=1$$

إذاً فقط من أجل أي $m\ , n$ نختارهما يجب

$$m \mid n-m$$

هل هذا صعب الاختيار؟

كلا فلقد أنشـــأنا متتالية للتو بهذه الخاصـــية.. الآن دائماً يجب في هذه الأشـــكال أن تأتيك قوة ايجابية أنه بإمكانك أن تنشا المتتالية بلمحة.

(من بعد هذه المسـائل يجب أن تشـعر بأن مثل هذه الأمور غالباً نسـتطيع إيجاد المتتالية فالأرقام مفتوحة أمامك وكان فقط ينقصك الثقة).

إذاً أنشأ المتتالية مع الخاصة $n \mid n-m$ حتى دون الـ 2 التي كانت في المسألة السابقة وتنتهي المسألة.

**طريقة أخرى:**

هي الأسهل والأقوى ولكن الجميل بالمسألة السابقة أنها تستخدم فكرة المسألة التي سبقتها

لدينا $m-1$ حد من المتتالية نريد إيجاد الـ $t_m$

$$a^{t_m+1}+a^{t_m}-1$$
$$a^{t_m}(a+1)-1$$

أي عدد $x$ ناخذه من قواسم $a^{t_m}-1$ يحق $a^{t_m}(a+1)-1 \equiv a \mod x$ ولكن $x$ أولي مع $a$

وبالتالي يكون x اولياً مع $a^{t_m+1}+a^{t_m}-1$

وبعدها نقحمه استقرائياً.

ماهي هذه ال xالتي سنستفيد منها

نعم سنجعل الء$x$ هي الحدود السابقة

ولكن كيف سنجعل

$$a^{t_{m-1}+1}+a^{t_{m-1}}-1 \mid a^{t_m}-1$$

ببســاطة فقط أعلم أن $t_m$ هو الزعيم والكبير ولا يؤثر $t_{m-1}$ عليه ولا تخف أبداً أن يصــبح $t_m$ عملاقاً أو مشوهاً

تماماً نجعل ضمن $t_m$ مضاعف $\emptyset(a^{t_{m-1}+1}+a^{t_{m-1}}-1)$

وبالمثل لـ $t_{m-2}$ ، $t_{m-3}$ إلى $t_1$ (استقراء)

ويتم إنشاء $t_m$ وتنتهي المسألة.

**المسألة السادسة:**

أثبت أنه من المتتالية $a_n = \{2^n - 3\}_1^\infty$ يكون لدينا متتالية غير منتهية كل عنصرين فيها أوليين فيما بينهما.

**الحل:**

بالفعل كما في المسألة السابقة نختار $m$ عنصراً من الشكل $2^n - 3$ ولتكن $a_1, a_2, , \dots . a_m$ وننشأ الـ $m + 1$

وذلك بجعل $a_{m+1} = 2^{\emptyset(a_m)\emptyset(a_{m-1})\dots\emptyset(a_1)} - 3$

عندها

$$(a_{m+1}, a_k) = (1 - 3, a_k) = 1$$

وهو المطلوب.

هنا صعوبة المسألة أن تتجاهل بنية الـ $2^n - 3$

وأن تضعها كاملة في الأس (ولو ضمن الـ فاي $\phi$ يعطي قيمة قريبة للعدد أي قد تشعر أيضاً بأن العدد $a_{m+1}$ سيصبح كبير وتبدأ بالتردد والقلق)

تضعها كاملة رغم حجمها الكبير.. هذا الحاجز يجب أن يُكسر لأنه لا يهمك مهما كبر العدد ووصل للمريخ.

نتابع الآن مع مسائل هامة قريبة لهذا النمط (إثبات وجود).

**المسألة الأولى:**

أثبت أنه من أجل أي $n \geq 2$ العدد $n!$ يمكن كتابته على مجموع $n$ قاسم **مختلف** من قواسمه.

**الحل:**

بعد تجريب عدة أرقام والتفكير بالانتقال للأعداد الأكبر والتعميم سنلاحظ أولاً فشل كل طرائق التقسيم بالتساوي حتى لو بشكل غير مباشر فهي تتكرر كثيراً في محاولاتك.

نلاحظ أن الـ $n!$ تتقبل وضع أي مقام لها ذو قيمة بسيطة (غير مركبة ومجاهيل وهيك).

إمكانية الاستفادة من تجزئة الأعداد التي تسبقها.

فشل إمكانية التعديل على مجموعة من $n$ عنصر كلها قيمتها $(n-1)!$ لأن الجمع يصبح غير ذو أهمية في القواسم الكبرى وأيضاً لا يمكن استخدام مضاعفات الـ $(n-1)!$ فقط لأنه من الممكن أن يكون $n$ عدداً أولياً.

لذلك تفكيرنا بها لطريقة رح يبقى طريقة مما يلي:

- إما الاستقراء
- أو مقامات $n!$

لنبدأ بمقامات $n!$ سنحاول البحث عن مقامات بسطها 1 ومجموعها 1 لأننا سنخرج $n!$ عامل مشترك – حاول هنا-

أقوى وأبسط شيء هو استخدام الـ 2 لوحده ولكن سنلاحظ أنه بدون تكرار لن نصل لـ 1.

كيف سنصلح هذه المشكلة؟!!

رغم بساطتها هذه الحركة تدل على الخبرة والقدرة – فلو استخدمنا –

$$\frac{1}{2}+\frac{1}{2^2}\dots+\frac{1}{2^m}=\frac{2^m-1}{2^m}$$

يبقى لـ 1 فقط $\frac{1}{2^m}$ لكن لا يمكننا وضعها فماذا سنضع إذاً؟

نعم سنقحم الـ 3

$\frac{1}{3}+\frac{2}{3}$ من $\frac{1}{2^m}$ وتنتهي المسألة

$$\frac{1}{2}+\frac{1}{2^2}\dots+\frac{1}{2^m}+\frac{1}{2^m\cdot 3}+\frac{1}{2^{m-1}\cdot 3}$$

طبعاً هنا سنختار $m=n-2$

والقواسم هي عملياً (تأكد أنها صحيحة!)

$$\frac{n!}{2}+\frac{n!}{2^2}\dots+\frac{n!}{2^m}+\frac{n!}{2^m\cdot 3}+\frac{n!}{2^{m-1}\cdot 3}$$

**طريقة ثانية:**

للمقامات هو أن نتذكر **الجمع التليسكوب** $\frac{1}{n(n-1)}=(\frac{1}{n-1}-\frac{1}{n})$

$$\left(\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}\dots\dots\frac{1}{n(n-1)}\right)+\frac{1}{n}$$

**والآن إلى طريقة الاستقراء** الذي لابد لنا أن نتعلمه جيداً لأنه الحل في كثير من الأوقات.

ماهي الفكرة التي سيبنى عليها الاستقراء الآن؟

مع تأمل لحالات صغيرة بشكل منظم أكثر، نلاحظ أنه يمكننا دائماً إيجاد مثال فيه)

ولكن ما علاقته بالحل وكيف الحصول عليه دائماً؟ نفرض صحته ولدينا $n$ عدد منهم 1 تحقق :

$$1+a_2+a_3+\cdots+a_n=n!$$

لاحظ أني ابتكرت فرض استقراء من عندي فوضعت الحد الاول دائماً 1

بهذه العملية اضمن وجود الـ 1 وأنا أنتقل من خطوة $n$ إلى ما بعدها ولكن لا تخف، أيضاً يجب أن أوجده في نهاية الخطوة $n+1$ والآن نضرب بـ $n+1$

$$(n+1)+(n+1)a_2+\cdots+(n+1)a_n=(n+1)!$$

بالفعل الآن الـ $n$ حد أصبحت من قواسم $(n+1)!$ ولكن عددها $n$

لذا نفرق $n+1$ إلى $n$ , 1 ويتم المطلوب

## المسالة الثانية:

لدينا $2^n$ عدد أولي مكتوبين في سطر، ونعلم أن بينها فقط $n$ عدد أولي مختلف على الأكثر، أثبت أنه يوجد متسلسلة من هذا السطر جداء عناصرها هو مربع كامل

الحل:

لو جربت أمثلة فعلاً ستلاحظ أنك ستعجز عند كتابة الحد رقم $2^n$ وستلاحظ أثناء تجربتك أنه سيظهر التناقض ربما من بداية السلسلة، والذي لن يسمح لك بوضع عدد أولي معين (أثناء إنشائك للسلسلة).

إذاً لابد لنا من مسجلة تسجل هذا الأمر لكي تنبهنا مباشرة في حال في حال وضعنا عدد اولي اوصلنا لمربع كامل .

الآن من الأفكار التي تخطر "الاستقراء" مثلاً ننظر إلى عدد أولي جديد $P_{n+1}$ ضمن $2^{n+1}$ عدد، فمثلاً لو وجد $P_{n+1}$ وحيد سنأخذ الطرف على جانب $P_{n+1}$ الذي يحوي أعداداً أكثر وبالتالي أكثر من $2^n$ ولو وجد 2 من $P_{n+1}$ إما أن يكون بين جذوره أكثر من $2^n$ عدد سنأخذهم ونطبق الاستقراء، وإما على الأطراف أكثر من $2^n$ سنأخذ كل ما بين الـ $P_{n+1}$ والـ $P_{n+1}$ الأخرى ونجعل الأعداد على الأطراف تعطي ما يكمله لمربع كامل {وكاننا نعمم المسألة لإثبات أنه في $2^n$ عدد فان المتسلسلات المختلفة تعطي كل شيء، أي مثلا $(p_1, p_2, p_3, p_4 \dots . p_{n+1}) = (1, 0, 0,1 \dots . 1)$ وعند هذا الخاطر سنترك هذه الطريقة التي تبدو عقيمة ونذهب لما ذكرناه في البداية (المسجلة)}... ولما اوحاه الخاطر لنا هي اخذ المتسلسلات كلها التي تبدا بالحد الأول ..واطوالها مختلفة وبالتالي هنالك $2^n$ متسلسلة من هذا النوع ... ووفقا للمسجلة (0,1,1,0,1,0) يوجد بالضبط $2^n$ احتمال للمسجلة ...وبالتالي اما المتسلسلات المختارة تعطي كل الاحتمالات ومنها (0,0,0,0,0,0....) والتي هي مربع كامل ..او لاتعطي هذا الاختيار وبالتالي هنالك متسلسلتان تعطيان نفس النتيجة ...باختصار عناصر المتسلسلة الأقصر ..نحصل على متسلسلة لاتبدا من الحد الأول ..تحقق ان جداء عناصرها (0,0,0,0,0.....0)

---

## المسألة الثالثة:

أوجد أكبر عدد $n$ الذي من أجله يوجد $n$ غير سالب $x_1, x_2, \dots, x_n$ ليست كلها صفرية بحيث لأي سلسلة من العناصر $\{e_1, e_2, \dots e_n\}$ من $\{-1,0,1\}$ ليست جميعها 0 بحيث $n^3$ لا تقسم المجموع

$$e_1x_1 + e_2x_2 + e_3x_3 + \cdots + e_nx_n$$

**الحل:**

الآن يجب ألا تخاف من شكل أي مسألة لأنه ستكتشف بالنهاية أنه كلهم نفس الشي ولكن بعد تفكير.

الآن بتجريب عدة أرقام سيكون بدءاً من الرقم 5 صعوبة التنبؤ مباشرة بصحة الحل ولكن بعدها ستشعر أننا يجب أن نأخذ الأرقام متباعدة، طبعاً سنختارهم بالمحاولة على الترتيب، أضمن ما سيكون أن نضع عدد **أكبر من مجموع كل ما سبقه** وبالفعل هذه الطريق تنفع مع عدة أرقام وإثباتها يبدو واضحاً لذا:

ما هو الـ $n$ الموافق لهذه الاختيار؟ أولاً سنبدأ بالـ 1 كي لا نضيع أرقام $1, 2, 4, 8$ بالفعل كان اختيارنا عبارة عن قوى الـ 2.

وعلى هذا الأساس سيحققه أكبر $n$ يحقق $n^3 > 2^n - 1$ وهو الرقم 9 نعم بالفعل

والآن كيف نثبت أن الاختيار بالفعل $n^3$ لا يقسم المجموع؟

هو واضـح تماماً فكرة الإثبات ولكن لكي نعبر عنه نفرض أنّ $x_k$ هي أكبر عناصر $x_i$ التي $e_i$ الموافق لها ليس الصفر ونفرض دون فقد العمومية أن $e_k = 1$

$$e_1x_1 + e_2x_2 \dots . e_nx_n = 2^{k-1} + e_{k-1}x_{k-1} + \cdots + e_1x_1$$
$$\geq 2^{k-1} - 2^{k-2} - 2^{k-3} \dots . . -1 \geq 1$$

بقي

$$A = e_1x_1 \dots . . e_nx_n < 1 + 2 + \cdots + 2^{k-1} = 2^k - 1 \leq 2^n - 1$$

والآن $n \geq 9$ نجد $0 < A < n^3$

إذاً $A$ ليس مضاعفاً لـ $n^3$

الاتجاه الاخر هو تحدي لك.

**المسألة الرابعة:**

لتكن $M$ مجموعة من 1985 عدداً صحيحاً موجباً مختلفاً ولا يحوي أيٌ منهم قاسم أولي أكبر من 26 ، أثبت أن $M$ تحوي على الأقل مجموعة جزئية واحدة من 4 عناصر مختلفة بحيث جداءها هو القوة الرابعة لعدد صحيح.

**الحل:**

أولاً لنلاحظ أنه لدينا فقط عدة أعداد أولية متاحة $2, 3, 5, 7, 11, 13, 17, 19, 23$ ومن أجل أي عدد أولي يوجد 4 احتمالات لأسه (لأن ما يهمنا هو مود 4)

الآن عدد كل الاحتمالات

$4^9$ كبير جداً من الـــ 1985 ولكن تذكر أنك لديك 4 عناصر لتتحكم بها (سيقول البعض أنه وجود هذه الـــ 4 عناصر أمر سيء أيضاً لأن الثالث سيكون صعب التحكم به ومن بعده الرابع أيضاً ولكن هذا خاطئ.. يجب أن نستغل وجودهم لصالحنا).

ولكن هنا ما سنجربه هو أخذ ومناقشة عنصرين فقط، بدايةً هذه سيزيد من الاحتمالات، وكأنّ جداء أي عنصرين هو عنصر آخر. ولكن الفكرة أنه حتى لو حصلت على احتمالين مكررين تخشى أن يكون بينهم عنصر مشترك (لأن كل احتمال هو عبارة عن جداء عنصريين فربما يتساوى عنصر من الاحتمال الأول مع عنصر من الاحتمال الثاني) وإقحام 3 عناصر فقط أيضاً لن يفيد لنفس السبب.

إن وجود قيم مكررة سيجعل الأمور أصعب، لذلك علينا التفكير باستراتيجية أقوى (ما سبق كأرقام والأفكار كانت مبدئية وتجري في دقيقتين)

التفكير الذي لا يفارقك هو أنه لو كانت غاية المسألة الحصول على مربع كامل لكانت غاية في البساطة.

لأنه يوجد $2^9 = 512$ احتمال فقط وهو أصغر من 1985

إذاً لم لا نبدأ بإنشاء مربعات ومن ثم ننتقل للقوة الرابعة؟!!

كلما أخذنا 512 عدد عطرف نخرج منهم 2 جداءهم مربع كامل

كم زوج لو تصرفنا **بحنكة** سنشكل دون تبذير؟؟؟

سنبقى ننقص 2 حتى يتبقى ما هو أقل من 512

أي سننقص 1474 وبالتالي 737 زوج كل من هذه الأزواج يمثل مربع والآن المتبقي يبدو أنه أصبح واضحاً

لو أخذنا هذه المربعات دون تربيع سنحصل على $512 < 737$ عدد

سنحصّل منها زوجاً هو مربع كامل وبالتالي إذا أعدنا التربيع سنحصل على قوة رابعة

لاحظ أن 1985 كان زائداً عن المطلوب وذلك تم اختياره حسب سنة الفحص..

## المسالة الخامسة :

ليكن $P$ عدداً أولياً فردياً، ولتكن لدينا متتالية الأعداد الصحيحة المتزايدة تماماً وتحقق:

$a_i = i$ كل $0 \leq i \leq P-2$ و $a_n$ بدءاً من $n \leq P-1$ معرف بأنه أصغر عدد صحيح موجب **لا** يشكل متتالية حسابية بطول $P$ ($P$ حد) مع أي من الحدود السابقة. أثبت أن $a_n$ هو ناتج كتابة العدد بالنظام $P-1$ ثم قراءته بالنظام $P$.

الحل :

الآن لحل المسألة يجب أن نأخذ وقتنا بتجربة بعض الأعداد فقط لنؤكد لأنفسنا صحة ما يطلبه ولكي نفهم كيف ننتقل للحد الذي يليه، وعليك قبل أن تفكر بأن تحل المسألة أن تستنتج ما يلي:

- أن النظام الحقيقي المعمول عليه هو الـ $P$ (هذا متوقع لأن $P$ هو طول المتتالية).

إذاً ما هو دور $P-1$: هو فقط للعد والمشي بين الحدود ... ولكن لمَ $P-1$ بالذات:

لأن حبكة المسألة أن حدود $a_n$ تهرب من أن تحوي المنزلة $P-1$، لذا يبدو ونحن نعد ونمشي في الحدود أننا نستخدم نظام $P-1$، ولكن القيمة الرياضية للمقدار هي نظام $P$.

أول فضول يأتي إليك كناقد ومحلل للمسألة أنه هل فعلاً الهرب من المنزلة $P-1$ يؤكد أننا لا نحصل على متتالية حسابية من $P$ حد؟ (خصص وقت الآن لإثبات ذلك) ...

بالفعل بما أننا تدربنا جيداً على التعامل وفق رغبات المسألة سنتخيل الحد الأول من متتالية $P$ حد هو:

(1 2 0 3 1 2 3) حيث $P = 5$

و $d = 32400$ هنا نلاحظ الـ $d$ لا يوجد عليه شرط منع الـ 4 لأنه هو فرق بين حدين.

الآن في مثالنا كيف نعرف مباشرةً أن أحد حدودها سيحوي 4؟ ... بسرعة (دون أن نحسب الحدود كاملة) ...

نعم نأخذ أول منزلة غير صفرية في $d$.

نلاحظ أن الخانة المقابلة في $a_i$ ستتبدل وتأخذ كل القيم (واخترنا أول منزلة لنضمن عدم وجود استلاف)

ومن ضمن القيم 4، إذاً طالما لا يوجد 4 يستحيل وجود متتالية حسابية بطول $P$ ... (يا ترى لم الـ 4 بالذات؟؟..)

اللآن لننشئ المتتالية

والآن بالاستقراء طبعاً .. نفرض أن $m-1$ يحققون المطلوب، حيث $a_{m+1} + 1$ يحوي منزلة $P-1$ في النظام $P$ عندها نقول أن $a_m \neq a_{m-1} + 1$، لأن المنزلة التي ستحوي $P-1$ (لتكن $t$) عندها المتتالية الحسابية التي حدها الأخير هو $a_{m-1} + 1$ وفرقها $d = P^t$ تحقق المطلوب (لاحظ أن كل ما أكتبه هو ترجمة رياضية لمثال موجود في مخيلتي).

وإذا $a_m = a_{m-1} + 2$ حيث المتتالية الآن من $a_1 \dots a_m$ لا تحوي أي منزلة $P - 1$ وبالتالي يستحيل وجود متتالية حسابية طولها $P$ وكذلك الأمر للحدود التالية حتى الوصول إلى $m'$ بحيث $a_{m'-1} + 1$ يحوي $P - 1$ منزلة، وتنتهي الخطوة الاستقرائية.

## حساب بواقي طويلة $mod\ p$

**تمرين:** أثبت أن

$$1+2+3+4+\cdots+(p-1)\equiv 0\ mod\ p$$

**الحل:**

$$1+2+3+\cdots+p-1=\frac{p(p-1)}{2}\equiv 0\ mod\ p$$

أو $(1+p-1)+(2+p-2)\ +\cdots+\left(\frac{p-1}{2}+\frac{p+1}{2}\right)\equiv 0\ mod\ p$

**تمرين 2:** أثبت أن $\frac{1}{1}=\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\equiv 0\ mod\ p$

**الحل:**

بما أنه كل عدد مقلوب خاص فيه عندها

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}\ldots\frac{1}{p-1}\equiv 1+2+3\ldots.p-1\equiv 0\ mod\ p$$

**تمرين 3:** أثبت أن

$$1^2+2^2+3^2+4^2+5^2+\cdots+\ (p-1)^2\equiv 0\ mod\ p$$

**الحل:**

نطبق القانون:

$$1^2+2^2+\cdots+(p-1)^2=\ \frac{(p-1)p(2p-1)}{6}\equiv 0\ mod\ p$$

**تمرين 4+5:** الآن نأتي إلى إثبات أشياء عمومية للغاية وظريفة وطريقة الإثبات غريبة نوعاً ما.

أثبت أنّ جداء الأعداد مثنى مثنى مضاعف لـــ $p$ (المقصود بالأعداد هي الأعداد من $1 \leftarrow 1 - p$ وأيضاً جداءهم مثنى مثنى ومثلث مثلث فمثلاً بالـ $mod\ 5$

$$1 \cdot 2 + 1 \cdot 3 + 1 \cdot 4 + 2 \cdot 3 + 2 \cdot 4 + 3 \cdot 4 \equiv 0\ mod\ 5$$
$$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 1 \cdot 2 \cdot 4 + 1 \cdot 3 \cdot 4 \equiv 0\ mod\ 5$$

**البرهان:**

لدينا: $X^{p-1} - 1 \equiv 0\ mod\ p$

إذا نظرنا لـ $X^{p-1} - 1$ على أنه كثير حدود فإن لهذه المعادلة كل الجذور(فيرما) $\{1,2,3, \dots p-1\}$ إذاً

$$0 \equiv X^{p-1} - 1 \equiv (X-1)(X-2)(X-3) \dots \big(X - (p-1)\big)\ mod\ p$$
$$\Rightarrow X^{p-1} - 1 = X^{p-1} - S_1 X^{p-2} + S_2 X^{p-3} - \dots + \underbrace{1 \times 2 \times 3 \dots p-1}_{-1}$$
$$\Rightarrow 0 \equiv -S_1 X^{p-2} + S_2 X^{p-3} + \dots + S_{p-2} X + S_{p-1}\ mod\ p$$

بالمطابقة لأمثال كل قوة نجد أن

$S_1 = 0$ وهو المجموع

$S_2 = 0$ وهو مثنى مثنى

$S_3 = 0$ وهو جداء مثلث مثلث

وهكذا

$S_{p-1} = -1$ وهذه نظرية ويلسون.

**تمرين 6:** أثبت أن:

$$\sum_{0}^{p-1} i^k \equiv 0 \mod p$$

حيث $(k \neq -1)$ في الـ $mod\ p$

أثبتنا للتو ذلك من أجل $k = 1, k = 2$ ولكن لم نعممها

لو أننا نعرف جميع القوانين والصـيغ المغلقة لمجموع القوة $k$ لأول $n$ عدد كما فعلنا في حالة $n = 2$ لكنّا انتهينا... لكننا لحل هذا سنستخدم طريقة استنتاج هذه القوانين لنتأمل المقدار.

$$p^{k+1} = (p^{k+1} - (p-1)^{k+1}) + ((p-1)^{k+1} - (p-2)^{k+1}) + \cdots + (1^{k+1} - 0^{k+1})$$

$$p^{k+1} = \sum_{0}^{p-1} ((i+1)^{k+1} - i^{k+1})$$

$$p^{k+1} = \sum_{0}^{p-1} \left[ \binom{k+1}{1} i^k + \binom{k+1}{2} i^{k-1} + \binom{k+1}{3} i^{k-2} + \cdots + 1 \right]$$

بما أن $k$ ثابت سنضع كل حد في $\sum$ مستقلة.

$$p^{k+1} = \binom{k+1}{1} \sum_{0}^{p-1} i^k + \binom{k+1}{2} \sum i^{k-1} + \binom{k+1}{3} \sum i^{k-2} \ldots$$

لو أخذنا $mod\ p$ للمعادلة السابقة وطبقنا الخطة الاستقرائي:

$$0 \mod p \text{ كلها } \sum i^{k-2} \ldots \quad \sum i^{k-1} \ldots$$

وهذا يؤدي

$$0 \equiv (k+1) \sum_{0}^{p-1} i^k \mod p$$

$$p \nmid k+1 \Rightarrow \sum_{0}^{p-1} i^k \equiv 0 \mod p$$

وتمت الخطوة الاستقرائية وتم المطلوب.

**مثال:** أثبت أن:

$$A = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{p-1} \equiv 0 \ mod \ p^2$$

**الحل:**

نحن أقوياء في الـ $mod \ p$ ماذا عن $mod \ p^2$

نريد إيجاد $p$ في البسوط نختصر عليها فنعود الـ $mod \ p$

نستخدم نفس الطريقة في أول تمرين نضرب بـ 2 ثم

$$A = \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \left(\frac{1}{3} + \frac{1}{p-3}\right) \ldots . \left(\frac{1}{p-2} + \frac{1}{2}\right) + \left(\frac{1}{p-1} + \frac{1}{1}\right)$$

أي تصبح:

$$\mathrm{A} = \sum_{i=1}^{i=p-1} \left(\frac{1}{i} + \frac{1}{p-1}\right)$$

$$A = \sum_{1}^{p-1} \frac{p}{i(p-i)}$$

نختصر على $p$ ولنثبت أن:

$$\sum_{1}^{p-1} \frac{1}{i(p-i)} \equiv 0 \ mod \ p$$

$$\sum_{1}^{p-1} \frac{1}{i(p-i)} \equiv \sum_{1}^{p-1} -\frac{1}{i^2} \equiv -\sum_{1}^{p-1} \frac{1}{i^2} \equiv -\sum_{1}^{p-1} i^2 \equiv 0 \ mod \ p$$

ويتحقق المطلوب.

■

هنا يمكننا تطبيق الـ $mod \ p$ على المقام ....فقط لا نستطيع عندما نخاف أن يكون $i$ مضاعف لـ $p$.

كما سنستنتج عند تعامل مع كسر في الـ $mod\ p$ يحوي جداءات في البسط والمقام

العائق الوحيد للتعامل معه كما نتعامل مع المقدار العادي هو عندما يكون أحد الجداءات مضاعف لـ $p$ عندها قد يكون مضاعف لـ $p$ أو $p^2$ أو $p^3$ لا نعرف فمثلاً $p-i$ إذا كانت $i=p^3$ عندها أكبر قوة في $p-i$ هي واحد لو عوضنا $p-i$ بـ i− كما فعلنا وكانت $i=p^3$ عندها أكبر قوة في $p-i$ هي 1بدل 3

وهنا اختلف الأمر.

لذلك سنحسب القوى في البسط والمقام بالضبط فعندها تعطي $p-i$ فيها 1 (المثال السابق)

إذا كانت قوى البسط أكبر من المقام عندها الكسر هو $0\ mod\ p$ مباشرة

إما إذا كانت متساوية عندها هذا الكسر له قيمة من $1 \to p-1\ \ mod\ p$

لاحظت كيف يمكن أن يتغير الجواب □

حتى لو قلت لي أنه بعد إزالة كل الـ$p$ من البسط والمقام سيعطي $p-i$ نفس القيمة بالمود $p$ .... هذا ليس صحيح لأنه فقط في حالة وضع $i=3p$ مرة و $i=p^2$

هذا **سيهمنا** في مسائل أصعب قريباً الآن

**مسألة 6**: أثبت أنّ:

$$p^5 | \binom{p^2}{p} - p$$

$$\binom{p^2}{p} - p = \frac{p^2(p^2-1)\dots(p^2-(p-1))}{1\times 2\times 3\times \dots \times p-1\times p} - p$$

إذاً علينا أن نثبت أن

$$\frac{(p^2-1)\dots(p^2-(p-1))}{1\times 2\times \dots \times p-1} - 1 \equiv 0\ mod\ p^4$$

الآن هذا مشكلتنا هي الواحد لم نعتاد عليها لذلك نتخلص منها بالضرب المقام

$$(p^2-1)(p^2-2)\dots(p^2-(p-1)) - 1\times 2\times 3\times \dots \times (p-1) \equiv mod\ p^4$$

نلاحظ أن الجداءات على اليسار هي لـ $p-1$ عنصر بل هي $p^2$ مطروحاً منها الـ $(p-1)$ عنصر على اليمين إذا يمكن أن ننظر إليها على أنها

$$(X-1)(X-2)\ \dots (X-p-1)$$

حيث $X = p^2$

- والآن بالفك الخاص بكثير حدود على $X$ والأعداد 1 حتى $p-1$ هي جذوره نجد أن:
  - الحد الأخير هو الجداء الذي على اليمين في علاقتنا والتخلص منه من الطرفيين
  - الحد قبل الأخير $X$ بجداء $p-2$ عدد في كل مرة
  - الحد الذي قبله ايضا هو $X^2$ أي $p^4$ يكافئ صفراً

إذاً يبقى $X\cdot(1\times 2\times \dots \times (p-2) + 1\times 2\times \dots \times (p-3)(p-1) + \cdots)$

$$p^2(p-1)!\left(\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{p-1}\right) \equiv 0\ mod\ \ p^4$$

ولكننا أثبتنا من قبل أن هذا الحد مضاعف لـ $p^2$ وبالتالي انتهينا

■

**مسألة 6:**

$$2^{3n-1} \mid (2^{n+1}-1)(2^{n+1}-3)\cdot\ldots\cdot(2^n+1)-(2^n-1)(2^n-3)\cdot\ldots\cdot 3\cdot 1$$

أي جداء الأعداد الفردية بين $2^n \leftarrow 2^{n+1}$ ناقص جداء الأعداد الفردية الأصغر من $2^n$ يقبل القسمة على $2^{3n-1}$

**الإثبات:**

إن الطرف اليسار

$$A=(2^n+2^n-1)\cdot\ldots\cdot(2^n+3)(2^n+1)-(2^n-1)\cdot\ldots\cdot 3\cdot 1$$

في الطرف الأيسر لو تخيلنا $2^n=y$ ونشرنا الأقواس بنفس الطريقة التي اتبعناها في مسائل سابقة..
الحد الأول هو الجداء لكل العناصر بجانب $y$ في الاقواس الذي يتم اختصاره

الحد الثاني والثالث سنناقشهم

أما الرابع وما بعد سيحوي $2^{3k}$ "طيران"

إذا كان $X$ هو جداء الأعداد من $(2^n-1)\cdot\ldots\cdot 3\cdot 1$

$$A=2^nX\left(\frac{1}{1}+\frac{1}{3}+\cdots+\frac{1}{2^n-1}\right)+2^{2n}X\left(\sum_{i>j}\frac{1}{ij}\right)$$

نختصر على $2^nX$ لنثبت أن

$$\left(\frac{1}{1}+\cdots+\frac{1}{2^n-1}\right)+2^n\sum_{i>j}\frac{1}{ij}\equiv 0\ mod\ 2^{2n-1}$$

أي:

$$\sum_{i}^{2^n-1}\frac{1}{i}+2^n\sum_{i>j}\frac{1}{ij}\equiv 0\ mod\ 2^{2n-1}$$

والآن نجري الحركة على المجموع في اليسار لنحصل على $2^n$

$$\frac{1}{2}\sum_{1}^{2^n-1}\frac{2^n}{i(2^n-i)}+2^n\sum_{i>j}\frac{1}{ij}\equiv 0\ mod\ 2^{2n-1}$$

$$\star \frac{1}{2}\sum_1^{2^n-1}\frac{1}{i(2^n-i)}+\sum_{i>j}\frac{1}{ij}\equiv 0\ mod\ 2^{n-1}$$

والآن متطابقة

$$\frac{1}{2}\sum_1^{2^n-1}\frac{1}{i(2^n-i)}+\frac{\left(\sum\frac{1}{i}\right)^2-\sum\frac{1}{i^2}}{2}\equiv 0\ mod\ 2^{n-1}$$

نضرب بـ 2 ونلاحظ أنّ $\sum\frac{1}{i}$ هو مضاعف ل $2^n$

$$\sum_1^{2^n-1}\frac{1}{i(2^n-i)}-\sum\frac{1}{i^2}\equiv 0\ mod\ 2^n$$

والآن بما أنه جميع الاعداد $i, 2^n-i$ أعداد أولية مع $2^n$يمكننا إزالة $2^n$ من المقام وعندها

$$-2\sum\frac{1}{i^2}\equiv 0\ mod\ 2^n$$

$$\sum\frac{1}{i^2}\equiv 0\ mod\ 2^{n-1}$$ علينا إثبات

مجموعة الأعداد الفردية في المجموع على اليســـار هي تمثل كل الأعداد الأولية مع $2^{n-1}$ وبالتالي مقاليبها ستشكل نفس المجموعة الأعداد الفردية.

$$\sum\frac{1}{i^2}\equiv\sum\ i^2\ mod\ 2^{n-1}$$

ولكن نحن لا نعرف قوانين الا إذا كان المجموع لأعداد المتتالية من 1 صعودا إذاً علينا بالتعديل ...نكتب هذه المتتالية الحسابية بدلالة $n$.

( لا تستغرب فقط أشير إلى أنه ليس فقط الأعداد الفردية يمكن تعديلها وحسابها).

$$\sum_1^{2^{n-1}}(2i-1)^2=4\sum_1^{2^{n-1}}i^2+4\sum_1^{2^{n-1}}i+2^{n-1}$$

الآن بتطبيق القوانين التي نعرفها على كل حد نجد أنه المقدار فعلا مضاعف ل $2^{n-1}$ وهو المطلوب.

**مسألة 7:** $p$ عدد أولي

$$p^2 \mid \binom{p}{1} + \binom{p}{2} + \binom{p}{3} + \binom{p}{4} + \cdots + \binom{p}{\left\lfloor \frac{2p}{3} \right\rfloor}$$

حيث $\left\lfloor \frac{2p}{3} \right\rfloor$ تعني أكبر عدد صحيح أصغر من $\frac{2p}{3}$ (الفلور).

**مسألة 8:**

أوجد أصغر عدد $n$ بحيث إذا أخذنا $n$ عدد صحيح مختلف سنجد فيها 18 عدداً مجموعها مضاعف لـ 18:

كما فعلنا مع 3 أعداد مجموعها مضاعف للـ 3 والجواب هو 5 بتجريب الحالات.

الحل:

الآن 18 هي $2 \times 3^2$ إذاً من أجل وجود 9 أعداد مجموعها مضاعف للـ 9 كما عدد نحتاج ... كلما وجدنا 5 نخطف منهم ثلاثي مجموعه مضاعف للـ 3 ونحوله لعنصر واحد، لذا سنحتاج 17 عدداً ... (بالفعل بعد اختيار 4 ثلاثيات يجب أن يبقى 5 أعداد، وبالتالي $12 + 5 = 17$).

الآن تبقى للـ 18 الـ 2 فنخاف إن جمعنا تساعيتان مضاعفتان للـ 9 أن نحصل على عدد فردي.

نعيد العملية التي سمحت لنا بالانتقال من 3 إلى 9.

كم عنصراً نحتاج لنتأكد من وجود عددين مجموعهما زوجي؟ ... بالتأكيد 3، إذاً علينا أن نخطف ثلاث تساعيات.

إذاً بعد اختيار تساعيتان نريد وجود 17 عدداً لنختار منهم التساعية الثالثة، وبالتالي $(18 + 17 = 35)$، وبالفعل هو الجواب ... أي أن أي 35 عدد سنجد حتماً 18 عدداً مجموعها مضاعف لـ 18.

يمكن لتأكيد أن 35 هو أصغر ما يمكن يجب أن نبرهن أن 34 غير كافٍ، بإعطاء مثال واحد كافٍ لإنهاء الشك الهائل الذي نشأ أثناء توليد الرقم 35، والمثال هو:

17 عنصر مساوٍ للـ 5 و17 عنصر مساوٍ للـ 1.

**أما المسألة الاحترافية:**

أثبت أنه من أي $2P-1$ عدد – حيث $P$ عدد أولي – يمكن العثور على $P$ عدد مجموعها مضاعف لـ $P$:

أي كيف عرفنا أن 5 أعداد كافية للحصول على 3 أعداد مجموعها مضاعف لـ3؟ ربما بتجريب الحالات، ماذا لو أردنا التعميم؟

تخيل أننا سنعتمد في برهاننا على $Fermat$ ... نعم أعطني أي طريقة أفضل لنعامل الباقي 0 معاملة مختلفة عن كل البواقي الأخرى دون استثناء ((طبعاً طريقة حساب باقي جداء كل المجاميع أعقد بكثير)).

إذاً $(a_1 + a_2 \dots a_P)^{P-1} = 0.1$، 0 فقط إذا كان المجموع يكافئ 0 ويأخذ قيمة 1 فيما دون ذلك.

إذاً لو أردنا حساب $A \sum(a_1 + a_2 \dots a_P)^{P-1}$ يجب أن يكون $A \equiv \binom{2P-1}{P-1} modP$، ولكن $\binom{2P-1}{P-1} = 1$ (برهن ذلك)، إذاً يجب تحقق $A \equiv 1\ modP$ وفق مبدأ نقض المطلوب.

إذاً لنحسب $A$ رسمياً الآن، وهنا جوهر المسألة (مسألة بذاتها):

الآن في المنشور: $(a_1 + a_2 \dots a_P)^{P-1}$ سيوجد حدود من الشكل:

$$x_1 + x_2 + x_P = P - 1 \qquad a_1^{x_1} \dots \dots a_P^{x_P}$$

تذكر أن مجموعة الأعداد ضمن القوس $a_1, a_2 \dots a_P$ ليست بالضرورة مختلفة، فقد يتكرر الكثير منها، ولكن سنتعامل مع العنصر كرمز، لا يهمني إن كان $a_1$ يساوي $a_3$ ، إنهما مستقلان.

الآن هذا الحد $a_1{}^{P-2}a_2$ كم مرة سيتكرر ضمن الحد وكم مرة يتكرر ضمن المجموع؟

ضمن القوس $P-1$ طريقة، وهي طريقة اختيار قوس $a_2$، ولكن المجموع ضمن الحد مهم، لأنه طالما $a_1, a_2$ موجودة ضمن الحد سيتكرر $a_1{}^{P-2}a_2$ $P-1$ مرة ... إذاً المهم هو كم مرة يتكرر ضمن المجموعة ... أي تكافئ كم مرة تكون $a_1, a_2$ موجودة ضمن الحدود؟ ...

بالفعل تفرضهم موجودين ويبقى أن نبحث عن $P-2$ عنصر من $2P-3$ عنصر المتبقين لإتمام مجموعة من $P$ عنصر.

$\Longleftarrow$ يتكرر ضمن الحدود $\binom{2P-1-2}{P-2}$

و $a_1^5 a_2^3 a_3^{P-9}$ سيتكرر $\binom{2P-1-3}{P-3}$ مرة.

- إذاً ما وضع $\binom{2P-1-k}{P-k}$ في $modP$؟

لا نحتاج لاختصار من البسط والمقام لأنه ببساطة آخر حد في البسط هو $P = 2P - 1 - k - (P - k - 1)$، والمقام لا يحوي أي $P$، إذاً المقدار يكافئ $0 \cdot modP$

إذاً في المجموع سيتكرر أي حد من الشكل $a_1^{x_1}a_2^{x_2} \dots a_P^{x_P}$ عدداً مضاعفاً لـ $P$ من المرات، وبالتالي $A \equiv 0\ modP$ وهذا تناقض #.

---

مسألة سنستخدم فيها فيرما ايضا وخبرة قوية ومهارات في الحساب الطوييل على مستوى مهاري

ولكن قبل ان نصل لاستخدام الحل المعتمد على فيرما فلنناقشها كاي مسألة

**مسألة :**

ليكن $f(x_1, x_2 \dots x_n)$ كثير حدود مع أمثال صحيحة مع درجة كلية أصغر من $n$، أثبت أن عدد الـ $n$ عنصر $(x_1, x_2 \dots x_n)$ المرتبة بحيث $0 \le x_i \le 12$ بحيث:

$f(x_1, x_2 \dots x_n) \equiv 0\ mod13$ سيكون مضاعفاً لـ 13 حتماً.

**الحل:**

ستخبرني أنه لابد من أننا سنرفع لقوة 12 ونجمع من أجل كل الـ $n$ عدد المرتبة ... صحيح سنحلل بالنهاية بهذا الأسلوب، ولكن بدايةً لابد وأن مخك ممتلئ بطرق أسهل ربما تنفع في المسألة، إذاً لنوضح كل شيء:

## أولاً:

ستقول أنه أخذ كثير الحدود $x_1$ فقط، هذا لا يعطي 0 عدداً مضاعفاً لـ 13 مرة ... يكون الرد أنه إذا اعتبرت $n = 1$ عندها يجب أن تكون الدرجة 0، وإذا اعتبرت $n \ge 2$ فعندها هنالك مجاهيل أخرى يمكن أن تعطي أي قيمة من الـ 13 المتاحة ولا تتغير قيمة التابع.

إذاً $x_1$ له طريقة، و$x_2$ له 13 طريقة، وبالتالي 13 طريقة كلية لنحصل على $f \equiv 0\ mod13$ ... إذاً حتماً يجب أن تذكر كل المجاهيل.

## ثانياً:

ستقول أنني أعوض $x_1$ بأي قيمة من الـ 13 المتاحة سأحصل على تابع لها على $(x_2, \dots x_n)$ بالاستقراء يتم المطلوب.

الخلل في هذه الفكرة أنه بعد أن تعوض $x_1$ تخاف أن يبقى في $f$ حدود ذات درجة $n-1$ وهي غير مناسبة للاستقراء على $f'$ جديد على $(x_2, \dots x_n)$، أي $n-1$ عنصر (أي $n'=n-1$ والدرجة لـ $f'$ ليست أصغر من $n'$) مثلاً: $x_1^3 + x_1x_2x_3 + x_2^2x_3$

**ثالثاً:**

في المثال السابق ستقول لي أنه متجانس، أي لأي شعاع $\vec{v}\ (x_1, x_2, x_3)$ يحققها لدينا:
$\vec{v}, a\vec{v}, a^2\vec{v}, \dots a^{12}\vec{v}$، لكن انتبه!! لدينا هنا 12 مقداراً فقط.

إذاً لنتوجه إلى الحل، سنأخذ:

$$X = \sum_{0 \le x_1, x_2 \dots x_n \le 12} \left(f(x_1, x_2 \dots x_n)\right)^{12}$$

إن لم يكن عدد الأصفار مضاعفاً لـ 13 عندها $x$ البواقي الأصغرية أيضاً غير مضاعف لـ 13 لأن عدد الحدود $13^n$ ... وبالتالي المجموع $X \not\equiv 0\ mod P$.

الآن لنحسب حقيقةً ولنرى التناقض:

في منشور $f^{12}$ سنجد عدة حدود، والجميل في هذه المسألة أنها على كل قيم البواقي ودون تكرار.

فمثلاً الحد $x_1^{a_1}x_2^{a_2} \dots x_n^{a_n}$ سنعطيه سيغما خاصة فيه (لكل حد سيغما)، الآن هل لاحظت كيف تنتهي المسألة؟

الآن لكل حد سنجعل $n$ سيغما ... هل يمكن ذلك؟ ... نعم، ثبت قيم $x_2 \longrightarrow x_n$ وأخرجها عاملاً مشتركاً، وغيّر في قيم $x_1$، إذاً $\sum_{x_1=0}^{12} x_1^{a_1}$ن الآن هل لدينا نظريات تساعدنا في هذا المقدار؟

إذاً لنخرج بالخلاصة من حساب البواقي الطويلة هناك أشياء حتماً يجب أن تتذكرها:

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$$

$$\binom{n}{k} = \binom{n}{k-1} + \binom{n-1}{k-1}$$

$lcm$ العلاقة التي تقحم $(n+1)\binom{n}{\lfloor \frac{n}{2} \rfloor} \mid lcm\,(1, 2, \dots n)$

$$p \nmid \binom{p-1}{k}$$

$p \nmid \binom{tp-1}{k}$ لكل $p > k$ سهلة وواضحة

$p \nmid \binom{tp^a-1}{k}$ لكل $p^a > k$

$p \nmid \binom{k}{p}$ لكل $p^2 > k \geq p$ واضحة

$\binom{2^n-1}{k}$ فردي

$2^{n-k} \mid \binom{2^n}{2^k t}$ حيث $t$ فردي.

$\binom{n+1}{i} \equiv 0 \; mod \; p^{r+1}$ حيث $p^r < n+1 < p^{r+1}$

## رمز ليجيندر $\left(\frac{a}{p}\right)$

الآن سنتكلم عن موضوع كثيراً ما رأيناه في حلول المسائل والكتب وهو الرمز

وهو الذي يدل فيما إذا كان $a$ باقي تربيعي أم لا في الـ $mod\ p$.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{إذا كان } a \text{ تربيعي} \\ -1 & \text{إذا كان غير تربيعي} \end{cases}$$

الآن لنستطيع الدخول في هذا الموضوع سنستعرض حالة $a = -1$ التي أخذنا عنها الكثير ونحن جاهزون لها

$$x^2 + 1 \equiv 0\ mod\ p \Leftrightarrow x^2 \equiv -1\ mod\ p$$

أثبتنا أن $x^2 + 1$ لا يقسمه إلا عدد أولي من النمط $1\ mod\ 4$

إذاً $\left(\frac{-1}{p}\right) = -1$ إذاً كان $p \equiv 3\ mod\ 4$

وأثبتنا عن طريق ويلسون وجود $x$ بحيث

$$x^2 \equiv -1\ mod\ p \text{ إذا كان } p \equiv 1\ mod\ 4$$

إذاً $a = -1$ جاهزة سريعاً وبصماً.

من أجل $a = 2$ إثبات ما يلي أصعب من إثباتات الـ $-1$ لذا سنكتفي بوضعه جاهزاً وبصماً

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & : \quad p \equiv 1\,,7 \ mod\ 8 \\ -1 & : \quad p \equiv 3\,,5 \ mod\ 8 \end{cases}$$

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

إذا نسيت مثلاً من أجل $p \equiv 7 \ mod\ 8$ هل 2 باقي أم لا عندها جرب أي عدد أولي مثلاً الـ 7 بالفعل يوجد $(4)^2 \equiv 2 \ mod\ 7$

والآن ماذا عن $-2$ سنتجه من خلال القاعدة الظريفة التالية:

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

ولاحظ قيمته ستبقى 1 أو $-1$

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

نلاحظ سندخل حالات الـ $-1$ مع حالات الـ 2.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & : \quad p \equiv 1\,,5 \ mod\ 8 \\ -1 & : \quad p \equiv 3\,,7 \ mod\ 8 \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & : \quad p \equiv 1\,,7 \ mod\ 8 \\ -1 & : \quad p \equiv 3\,,5 \ mod\ 8 \end{cases}$$

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & : \quad p \equiv 1\,,3 \ mod\ 8 \\ -1 & : \quad p \equiv 5\,,7 \ mod\ 8 \end{cases}$$

**حيث:**

$p \equiv 1 \ mod\ 8$ تعطي $\left(\frac{2}{p}\right) = 1$ $\left(\frac{-1}{p}\right) = 1$ بالضرب نجد أنها $\left(\frac{-2}{p}\right)$ واحد

$p \equiv 3 \ mod\ 8$ تعطي $\left(\frac{2}{p}\right) = -1$ $\left(\frac{-1}{p}\right) = -1$ بالضرب نجد أنها $\left(\frac{-2}{p}\right)$ واحد

**الآن من أجل عدد أولي مكان $a$ وليكن $q$ وهو عدد أولي نعرف قيمته يمكن حينها إيجاد $\left(\frac{p}{q}\right)$ من خلال القاعدة:**

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

تسمى قاعدة المقاليب.

لإيجاد حالات $\left(\frac{3}{p}\right)$ مثلاً فإنه كالعادة الطرق الأخرى ستكون طويلة كما $\left(\frac{2}{p}\right)$ .

ولكن $\left(\frac{3}{p}\right)$ لها هذه الطريقة القصيرة

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}\times 1} = (-1)^{\frac{p-1}{2}}$$

والآن $\left(\frac{p}{3}\right)$ مقامها صـــغير ومعروف حســـابها ســـهل متى يكون $p$ باقي تربيعي في 3 ما هي البواقي التربيعية في 3 هي 1 أو 0

(انسَ الصفر) إذاً

$$\left(\frac{p}{3}\right) = 1 \quad p \equiv 1\ mod\ 3$$
$$\left(\frac{p}{3}\right) = -1 \quad p \equiv 2\ mod\ 3$$
$$(-1)^{\frac{p-1}{2}} = +1 \quad p \equiv 1\ mod\ 4$$
$$(-1)^{\frac{p-1}{2}} = -1 \quad p \equiv 3\ mod\ 4$$

إذاً لنوجد حالات $\left(\frac{3}{p}\right)$ علينا أن نقاطع حالات $\left(\frac{p}{3}\right)$ مع $(-1)^{\frac{p+1}{2}}$ في $mod\ 12$

سيكون:

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & : \quad p \equiv 7,5 \quad mod\ 12 \\ -1 & : \quad p \equiv 1,11\ mod\ 12 \end{cases}$$

وبالفعل لنجرب عدد أولي $mod\ 12$ 7 ليكن 7

لا يوجد أي $x$ يحقق $x^2 \equiv 3\ mod\ 7$

وبالعكس نجرب 13 لدينا 4تربيع تعطي الـ 3 المنشودة $(4)^2 \equiv 3\ mod\ 13$

**والآن إلى التطبيقات العملية**

**مثال1**: أثبت أنه من أجل أي عدد أولي $p$ يحقق $p \mid 2^{2^n}+1$ عندها

$$p \equiv 1 \ mod \ 2^{n+2}$$

**الحل:**

نتذكر أننا أثبتنا أنه $p \equiv 1 \ mod \ 2^{n+1}$ بطريقة **أخذ الـــ** $\boldsymbol{gcd}$ أو بنظرية الزائد ضعيف أمام الـــ 2 ولكن لن نصل لـ $2^{n+2}$.

لذا لا بد لنا من تحسين المسألة والالتفاف، هنا مهمتك التفكير بهذه الحركة.....

من الحركات التي ستفعلها هي كتابة على الشكل:

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

ولكن هذا لن يفيدك لأن مجموع مربعين فقط يعطي أنّ العدد الأولي هو $1 \ mod \ 4$.

وأي إخراج لأحد التربيعات من الأس أو إنزاله سيضر ولا ينفع، لأننا نأمل لو تزيد التربيعات واحد لا أن تنقص.

الآن من أين آتي بهذه التربيع الزائد؟!!

الآن فكر بالنظرية التي طبقناها في السطر الأول. ما الذي كان ضرورياً في نص المسألة لتحققها وما هو الشيء الموضوع عشوائياً؟!!

بالضبط الـ 2 في الأساس ... هي ليست شرطاً في عملية اخذ الـ$gcd$ هذا يدفعنا برغبة لمعرفة ضرورتها في المسألة .... إذاً يمكن أن نغيرها.

نجعل $a^2 \equiv 2 \ mod \ p$ (وهذا ممكن، لمَ؟ (لمَ 2 باقي تربيعي؟؟؟)

لأن $p$ هو $1 \ mod \ 8$ من $1 \ mod \ 2^{n+1}$ وذلك من أخذ الـ$gcd$ □.

إذاً تصبح العلاقة $a^{2^{n+1}}+1 \equiv 0 \ mod \ p \Rightarrow p \equiv 1 \ mod \ 2^{n+2}$

حسب النظرية التي طبقناها (أخذ الـ$gcd$ )ولكن هنا بشكل أقوى وتنتهي المسألة.

■

**مثال2:** أثبت أن $2^n + 1$ لا يحوي قاسم أولي من الشكل $8k + 7$ حيث $n, k$ عددان طبيعيان.

**الحل:**

الآن بالطبع سنبحث عن مربعات ولكن من أين نوجدها؟

سنأخذ حالتين:

- $n$ زوجي عندها مجموع مربعين أو $\left(\frac{-1}{p}\right) = 1 \Leftarrow p \equiv 1 \ mod \ 4$ وليس 3
- الحالة الثانية $n$ فردي

لدينا المقدار من الشكل $2k^2 + 1$

$2k^2 + 1 \equiv 0 \ mod \ p$ كيف نربط هذه المعادلة بالبواقي التربيعية

تماماً سنعدل لنعرف ما هو الرقم المقابل لمربع

$$2k^2 \equiv -1 \ mod \ p$$

هنا بدل أن نقسم على 2 لمَ لا نضرب

$$4k^2 \equiv -2 \ mod \ p$$

$$(2k)^2 \equiv -2 \ mod \ p$$

إذاً $-2$ باقي تربيعي $\Leftarrow p \equiv 1, 3 \ mod \ 8$ ولا وجود لـ $7 \ mod \ 8$ وبهذا تنتهي المسألة□.

.■

**المثال 3:** أثبت أن 16 هي القوة الثامنة لعدد ما في باقي أي عدد أولي كان

**الحل:**

المطلوب إثبات أن المعادلة $a^8 \equiv 16 \ mod \ p$ لها حل مهما كانت قيمة $p$.

كيف نبدأ؟

إنها قوة ثامنة وليست فقط ثانية لذا نتمهل في تطبيق النظرية ونحلل

$$a^8 - 16 \equiv 0 \ mod \ p$$
$$(a^4 - 4)(a^4 + 4) \equiv 0 \ mod \ p$$
$$(a^2 - 2)(a^2 + 2)(a^2 + 2a + 2)(a^2 - 2a + 2) \equiv 0 \ mod \ p$$

$(a^2 - 2)$ يوجد لها حل في كل $p \equiv 1,7 \ mod \ 8$

$(a^2 + 2)$ يوجد حل لكل $p \equiv 1,3 \ mod \ 8$

بقي الـــ $5 \ mod \ 8$ من الواضـح أنّ القوسـيين الماضـيين لا يسـتقبلانه إذاً كيف نضـمن أن القوسـيين المتبقيات دائماً تستقبله؟!!

نعم إنها تكتب بالشكل

$$(a^2 - 2)(a^2 + 2)((a + 1)^2 + 1)((a - 1)^2 + 1) \equiv 0 \ mod \ p$$

$((a)^2 + 1)((a - 1)^2 + 1)$ يوجد لها حل في أي $p \equiv 1 \ mod \ 4$ أي $1 ,5 \ mod \ 8$

وبالتالي تمت تغطية كل الأعداد الأولية ■

وهذا شيء أكثر من رائع صراحة

**والآن إليك التدريب التالي**

أوجد جميع الأعداد $n$ التي تحقق أنّ $2^n - 1 | \ 3^n - 1$

والآن إلى مثال قوي ونستخدم عدة نظريات وإبداعات

**المثال 4:** ليكن لدينا $k = 2^{2^n} + 1$ أثبت أن $k$ عدد أولي إذا وفقط إذا كان $k \mid 3^{\frac{k-1}{2}} + 1$ .

**الحل:**

سنستخدم في هذه المسألة مصطلح الـ$ord_n(a)$ الذي يعني أصغر قوة يرفع بها العدد $a$ فيعطي قيمة تكافئ $1 \ mod \ n$.

ربما استخدمنا فكرته كثيراً ولكن لم نستخدم المصطلح...ربما ليست بمشكلة.

لنبدأ إذا كان $k \mid 3^{\frac{k-1}{2}} + 1$ ونثبت أنّ $k$ أولي.

لو حللت المسألة السابقة كنت ستحاول اتباع ذات الطريقة لكن هنا $\frac{k-1}{2}$ زوجي مما لا يتيح الفرصة لـــ $-3$ لتكون باقي تربيعي.

إذاً ابحث أعمق، لدينا: $k \mid 3^{k-1} - 1$

هنا نرى الإيحاء بأن $k$ سيكون أولي ولكن هذه ليست نتيجة مباشرة لأن $k-1$ و $\emptyset(k)$ الـــ $gcd$ بينهما $d$ ربما يكون أصغر من $k-1$ وبالتالي ليس مثيراً للشك بالعدد الأولي.

وهنا قد نحاول أخذ عدد أولي $p$ يقســـم $k$ ولكن عندها نلاحظ أن $k-1$ لا علاقة له بـــــ $p$ لكي يخلق التناقض كما في مسألة $n \mid 2^n - 1$

لذا نعيد النظر ما الذي أغفلناه من المعطيات هو أن $k = 2^{2^n} + 1$ في الأس وليس فقط في المقسوم عليه (حاولنا على الأقل أول سطر)

إذاً نلاحظ أن $k-1$ هو كله قوى لـ 2 ...لذا سنعود إلى العدد الأولي $p$ الذي يقسم $k$ الآن

$$k \mid 3^{2^{2^n-1}} + 1$$

((إياك أن تنسى أنّ مصدر إشارة الناقص كان إشارة زائد))

إذاً على $p-1$ أن يأكل كل الأس مضاف إليه اثنان مضروبةً (**حسب النظرية التي تعلمناها بشأن إشارة الموجب بدل السالب**)

$$p = k \ \Leftarrow \ \ k-1 \mid p-1 \qquad p \mid k$$

والآن الاتجاه الآخر

إذا كان $p = 2^{2^n} + 1$ أثبت أن $p \mid 3^{\frac{p-1}{2}} + 1$

$3^{\frac{p-1}{2}}$ يوحي لنا:

**هنا لدينا مثل *lemma***

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

بمعنى أن قيمة هذا المقدار الأيسر تدل إذا كان $a$ باقي تربيعي أم لا فعندما تقرأ هذا المقدار الأيسر ستصبح تقرأه كأنه $\left(\frac{a}{p}\right)$

وإثباته سهل لو كان $a \equiv b^2 \Leftarrow a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right)$

وإذا لم يكن $a$ مربع عندها نتأمل المعادلة $X^{p-1} \equiv 1 \; mod \; p$ .. $(*)$ لها $p-1$ حل

$$\left(X^{\frac{p-1}{2}} - 1\right)\left(X^{\frac{p-1}{2}} + 1\right) \equiv 0 \; mod \; p$$

الآن البواقي التربيعية تحقق القوس اليسار وعددها $\frac{p-1}{2}$ إذاً $X^{\frac{p-1}{2}} - 1$ لا تتقبل المزيد من الجذور

وبالتالي باقي الجذور للمعادلة $(*)$ ستحقق $X^{\frac{p-1}{2}} + 1 \equiv 0 \; mod \; p$ أي:

وتحقق أيضاً:

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

والآن بقي أن نعرف أنّ 3 ليست باقي تربيعي للـ $p = 2^{2^n} + 1$ ...لا سبيل إلا أن نفكر بالجدول طبعاً

بالفعل لأن $2^{2^n} + 1 \equiv 5 \; mod \; 12$ بالعودة للجدول نرى أن هذا تناقض

**مثال 5:**

- أثبت أنه لا يوجد عدد طبيعي $n$ بحيث: $2^n - 1 \mid 3^n - 1$:

**الحل:**

سنحاول كثيراً تحسين شكلها أو ان نعتمد على المتراجحات ضمن خطوات أخرى إثباتها ولكنها لن تجدي نفعاً ... لابد وأن نصل للنقطة التي تدرك أن اليمين واليسار غير مترابطين شكلياً ولا حجمياً، وكأن المسألة هي أنه هل يمكن للأعداد $2^n - 1$ الأولية أن تكون نفسها موجودة كاملةً في $3^n - 1$؟

ولكن ما هي صفات الأعداد الأولية الموجودة في $2^n - 1$؟ أولاً $n$ فردي وإلا يحتوي 3 ... كما في مسائل سابقة $2(2^{\frac{n-1}{2}})^2 - 1$ أي قاسمه الأولي $p$ سيكون 2 فيه باقياً تربيعياً، وبالتالي $p \equiv 1, 7 \ mod 8$

ماذا عن قواسم $3^n - 1$؟ أيضاً $3(3^{\frac{n-1}{2}})^2 - 1$، إذاً قاسمه $q$ سيكون 3 باقي تربيعي في $mod q$ أي $q \equiv 1, +11 \ mod 12$ (إذا نسيت جرب أمثلة، ولكن لابد أن تتذكر أنه يعتمد على $mod 12$).

إذاً عدد أولي في $2^n - 1$ لابد أن يتواجد في $3^n - 1$،

إذاً أي قاسم لـ $2^n - 1$ يجب أن يكون $1, -1 \ mod 12$.

ولأنه $n \geq 3$ فردي لدينا $2^n \equiv 8 \ mod 12 \Longleftarrow 2^n - 1 \equiv 7 \ mod 24$ وهذه الـ 7 لن نحصلها أبداً باستخدام 1 و$-1$ فقط، وبالتالي نصل للتناقض.

*_____*

إذاً الخلاصة من هذه المسائل أن البواقي التربيعية وسيلة قوية يجب أن تبقى في أذهاننا قدر المستطاع، وخاصة في حل مسائل ثانية أو خامسة، فالخبرة فيها تريحنا من أن تستنتج كل خواصها ومسائلها ضمن وقت الفحص في إيجاد نوع قواسم شكل كـ $2^4 - 1$ مثلاً، وهكذا ...

- والآن مسألة ظريفة جداً لاختبار نفسك 9.2.6:

ليكن $p$ عدداً أولياً من الشكل $4k + 3$، أثبت تكافؤ العلاقتين، $2p + 1$ هو عدد أولي $\leftrightarrow$

مع $2p + 1 \mid 2^p - 1$

### مسألة

أثبت أنه إذا لم يكن $a$ مربع كامل عندها $\left(\frac{a}{p}\right) = -1$ لعدد غير منتهٍ من الأعداد الأولية $p$:

بالفعل المطلوب من المسألة منطقي ومتوقع كما في $a = 2$، فقط الأعداد الأولية $1, 7 \ mod 8$ تقبل 2 باقياً تربيعياً (إضافة).

لو كان $a$ عدداً أولياً $a = q$ أيضاً متوقعة أكثر، فمن العلاقة:

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

لو كان $\left(\frac{q}{p}\right) = -1$ دائماً، أي عندها $\left(\frac{p}{q}\right)$ يعتمد على قيمة $p \ mod 4$ فقط، وهذا غير منطقي أبداً.

ولكن هذا الإحساس ضعيف لا يحل حالة الأولي ... عملياً ما يزعجنا هو كون $p$ عدداً أولياً، فلا نستطيع التحكم به بأريحية (لا بواقي صينية ولا غيرها).

يمكن أن نفرض $a$ خالياً من المربعات، وبالتالي $a = q_1 q_2 \dots q_n$ وبالتالي $\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right)$

الآن كلما كان $a$ يهددنا بأنه قد يحوي جداءات عن الأعداد الأولية ستصعب علينا المهمة وتحيرنا ...

سنقرر أن نجعل المقامات جداء متعدد، ولكن هنا تماماً العكس فهو سيريحنا، أي سنأخذ $q$ (بدل $a$ حاليا ..اي نحل مشكلته اذا كان $a$ اولي ثم نتوسع ) على عدة أعداد أولية (نطلق مصطلح المقامات على $b$ في $\left(\frac{a}{b}\right)$):

$$\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right)\left(\frac{q}{p_3}\right) \dots \left(\frac{q}{p_n}\right)$$

ونأخذ الجداء وإذا ساوى $-1$ تحقق المطلوب، تخيل!! ....لان صاحب المسألة هو من تكبر وجعلني افرض جدلا ان كل هذه المقادير تساقي 1

ولكن لمَ الحماس؟ فأنا لا أعرف قانوناً يحسب جداء مقامات مختلفة ..

انتظر لحظة!! يمكن تطبيق قانون المقلوب:

$$A = \prod \binom{q}{p_i} = \prod \binom{p_i}{q} (-1)^{\frac{p_i-1}{2}.\frac{q-1}{2}}$$

$$= \binom{p_1 p_2 \dots p_n}{q} (-1)^{\sum \frac{p_i-1}{2}.\frac{q-1}{2}}$$

ولكن معلومة عالخفيف وسهلة الإثبات بأن: $\sum \frac{p_i-1}{2} \equiv \frac{\prod p_i-1}{2} \ mod2$،

وذلك لان عدد الأعداد الاولية التي هي $3 \ mod4$ يحدد عدد الحدود $\frac{p_i-1}{2}$ الفردية ويحدد ايضا الجداء اذا كان $1 \ mod4$ او $3mod \ 4$وبالتالي $\frac{\prod p_i-1}{2}$ زوجي ام فردي

إذاً:

$$A = \binom{p_1 \dots p_n}{q} (-1)^{\frac{q-1}{2}.\frac{\prod p_i-1}{2}}$$

تذكر انه في عملنا لم نتطلب كون $p_1, \dots, p_n$مختلفة عن بعضها اذا عمليا $p_1 p_2 \dots p_n$ يعطي عمليا كل الاعداد b..وبالتالي نجعله يحقق الشرطيين

$$\mathrm{b} \equiv 1 \bmod 4$$

$$b \equiv s \ modq$$

حيث $s$هو اي باقي تربيعي في $modq$

ونترك البواقي الصينية لتحقق لنا الشرطيين سوية ..ونحقق المطلوب

اما $a$ حتى غير الأولية بسييط للغاية

والاهم اننا كشفنا اقوى ما قمنا به في حل هذه المسالة

(هو أخذ عدة أعداد أولية في المقام كرد فعل مناوءة لإمكانية وجود جداءات أعداد أولية في البسط).

والتعميم على $a = q_1 \dots q_m$:

$$\prod \binom{a}{p_i} = \prod \binom{q_1 \dots q_m}{p_i} = \prod \binom{q_1}{p_i} \cdot \prod \binom{q_2}{p_i} \dots \prod \binom{q_m}{p_i}$$

بمثل ما حسبنا $A$ :

$$= \binom{p_1 \dots p_n}{q_1} \cdot \binom{p_1 \dots p_n}{q_2} \dots \binom{p_1 \dots p_n}{q_m}$$

*_____*

الطريقة الأخرى: يقال عنها أنها صعب أن تخطر ولكنني أرى العكس، أنها تخطر أكثر – إذاً المطلوب اثباته ان عدد الأعداد الاولية التي لا تحقق التطابق $a \equiv b^2 \ \ modp$ لاي عدد $b$ هو غير منتهي ... أي ان جداء الاشكال $b^2 - a$ لكل $b$(من ال 1 للانهاية) سيغفل عدد غير منتهي من الاعداد الاولية ..هذا المطلوب اثباته

لو فرضنا العكس اي ان جداء الاشكال $b^2 - a$ يغفل عدد منتهي من الأعداد الاولية

وبالتالي يجب أن يصبح شعورك المعنوي تجاه مثل هذه الجملة **وكأنه** يقول كل الأعداد الأولية ستدخل في الجداء $b^2 - a$،

اذاً لو نظرنا لقدرة $b^2 - a$ على حمل هذه المسؤولية

وطبعاً $X = \prod(b^2 - a)$ عند حد معين ستصبح $(b-1)^2 < b^2 - a < b^2$.

الآن سيحوي $X$ كل الأعداد الأولية عند حد معيين، إذاً:

$$X = \prod(b^2 - a) > p_1 p_2 \dots p_t \dots$$

ولكن النظرية الكاسحة تقول أن يوجد دائماً عدد أولي $p_r$ بين $b^2$ و $(b+1)^2$ يحقق $p_r > b^2 - a$، بأخذ كل هذه الأعداد الأولية نجد أنه سيتحقق أن $X = \prod(b^2 - a) < \prod_i p_{ri}$ وهذا تناقض #.

---

**مسألة**: ليكن $a_1, a_2 \dots a_{2004}$ أعداداً صحيحة غير سالبة بحيث:

$a_1^n + a_2^n \dots a_{2004}^n$ مربع كامل لأي عدد طبيعي $n$، ما هو أصغر عدد من الـ $\{a_i\}$ يجب أن يساوي 0؟

الحل:

أولاً ما هو باعتقادك أقرب رقم؟ ستحاول أن تأخذ فكرة ... أول فكرة شيطانية أنه فقط عدد واحد يبقى، ولكن هذا خطأ، ستكتشف $4^a$ ونستفيد منها، فمثلاً 3 حدود $4^n + 2^n + 1$ لا ليست مربع لكن قريبة، $4^n + 2^n + 2^n + 1$ ... إذاً تعميم هذه الطريقة

$$a^{2n} \cdot a^{2n} \quad a^n + a^n \ldots \quad 1+1$$

$$b^2 \qquad 2bc \qquad c^2$$

سنرى أن عدد الحدود بهذه الطريقة بأعم طريقة $(b+c)^2$ وبالتالي مربع كامل ... لدينا $1936 = (44)^5$ ... يبدو أن 1936 رقم جيد لإنهاء المسألة، ولكن كيف نبرهن أن عدد الحدود مربع كامل؟ يجب أن يكون ... سنحاول الاستفادة من أهم المعلومات التي يزودها المربع الكامل، سنأخذ $mod3$ و$mod4$ و$mod5$ ومن ثم نتذكر أن الـ $n$ كيفية، وبالتالي لا نقف عند الـ 5 بل عملياً يمكن أخذ معلومة عن كل الأعداد الأولية، نعم بأخذ $n = p-1$ $\Longleftarrow$ ومن ثم $mod\ p$ لأعداد أولية غير موجودة في $a_1, a_2 \ldots a_{2004}$

$$2004 \equiv k^2\ modp \Leftarrow$$

ما معنى هذه المناقشة التي قمنا بها؟ ... نعم إنها عودة رسمية للمسألة السابقة التي توصلنا للتناقض بوجود مثل هذا الـ $a = 2004$، إذاً $a$ يجب أن تساوي مربعاً كاملاً، وبالتالي 1936 حد ... بدرجة قصوى، وبالتالي 68 حد يجب أن يحذف.

**مسألة :** أوجد عدداً بين 100 و1997 يحقق $n \mid 2^n + 2$:

حالتين: إما أن نختار $n$ فردياً أو زوجياً.

لو اخترناه فردياً عندها $n \mid 2^{n-1} + 1$، لاحظ أننا صعبنا كثيراً وجود هذا الـ $n$، لاحظ أن $n-1$ قريب جداً على نهاية الدورة الكاملة، ويزيد الطين بلة وجود الزائد ... لذا تضع $n = 2k$ بكل ثقة، $50 \leq k \leq 1000$ نبحث عن $k \mid 2^{2k-1} + 1$، الآن $k$ كل قواسمه هي $1, 3\ mod8$، هل ستنفعنا في عملنا يا ترى؟ (نضعها جانباً).

الآن لو كان $k$ عدداً أولياً $p$: $p \mid 2^{2p-1} + 1$ ، $p \mid 3$، إذاً $k = 3$ .....اصغر من 50 مرفوض .

إذاً هو مركب

الأعداد الأولية المسموحة عدا 3 هي 11 واكبر من 11 ولا نقبل 5 و7 بالاستفادة من كون الأعداد الاولية المقبولة هي $1, 3\ mod8$،

فإذاً لا يجوز أن يحوي $k$ على 3 أعداد أولية مختلفة او متساوية وإلا أصبح أكبر من 11×11×11 وبالتالي اكبر من 1000.

إذاً $k = pq$ أو $k = 3pq$

في حالة:

$$pq \mid 2^{2pq-1}+1 \Longleftarrow \quad p \mid 2^{2q-1}+1 \quad \text{و} \quad q \mid 2^{2p-1}+1 \ \ldots\ldots \ (*)$$

الآن هناك سر ستطلع عليه أن الأعداد الأولية الصغيرة بما أنها تحقق $p \mid 2^{p-1}-1$، وبما أنها ستحقق علاقة فيها زائد (العلاقة *)

ستكون $p \mid 2^{\frac{p-1}{2}}+1$ أو حتى أحد قواسم $\frac{p-1}{2}$، ولكن ستلاحظ في الأعداد الأولية الصغيرة بالتجريب أنها لا تحقق العلاقة لأي من قواسم $\frac{p-1}{2}$ الأصغر من $\frac{p-1}{2}$، بل حصراً $\frac{p-1}{2}$ أصغر قيمة تحقق علاقة ال1+، وهذا سيبقى صحيحاً حتى الوصول للـ 41 و 43.

إذاً لو كان لدينا $p, q$ أصغر من 41 عندها:

بما أن $p \mid 2^{2q-1}+1$ وايضا $p \mid 2^{\frac{p-1}{2}}+1$ و $\frac{p-1}{2}$ اصغر قيمة تحقق ذلك نستنتج مباشرة ان $\frac{p-1}{2} \mid 2q-1$

وبالمثل $\frac{q-1}{2} \mid 2p-1$ ،

بالحل المشترك نجد $p=11$ و $q=43$ حل وحيد وهو المطلوب. $k=11\times 43$

الان لابد من انعرض مسـالة اعطيناها مهلة بعدما اخذنا دراسـة المقدار $a^2+b^2$ ..والان بما اننا عرضـنا موضوعا مشابها قليلا ...حان دورها

**مسالة :**

لنفرض وجود $x, y, z$ أعداد صحيحة موجبة بحيث: $1+z^2=xy$، أثبت وجود أعداد صحيحة $a, b, c, d$ تحقق:

$$x=a^2+b^2 \qquad y=c^2+d^2 \qquad z=ab+cd$$

الحل :

الآن من العلاقة $xy=1+z^2$: بما أن الطرف الأيمن هو مجموع مربعين كاملين عندها كل قواسم $x, y$ هي أعداد مجموع مربعين، وكما فعلنا سابقاً نركب هذه الأعداد الأولية بالاستقراء، فنجد أن $x, y$ كل منهما مجموع مربعين كاملين ... إياك أن تقع في فخ الحماس وتقول نجعل $x=a^2+b^2$ و $y=c^2+d^2$ ،

لأنك هكذا تكشف كل أوراق الطرف الأيمن. واللآن قد يقبل الطرف الأيسر الشكل المطلوب في المسألة، ولكن في نفس الوقت قد يقبل أشكالاً أخرى ... نحن دائماً نسعى وراء الخطية، لإعطائه معلومات بأقل خسائر ممكنة.

ولكن أربع مجاهيل خطية من أجل $z$ والـ 1 التي بجوارها كثير! ... كم مجهول يكفي ... نعم مجهولين. ماذا نفعل إذاً؟

سنفرض $x = a^2 + b^2$ و$y$ لا نفرضها، ونبحث عن أعداد $c, d$. إذاً مجهولان يحققان:

$$ab - cd = 1 \qquad z = ab + cd$$

بحل المعادلتين نجد أن $d$ يجب أن تكون $\frac{za+b}{a^2+b^2}$، هذه مجاهيل لا نتحكم بها، فهل تعطي عدداً صحيحاً يا ترى؟ نعم وأصبح إثبات ذلك مألوفاً لدينا نوعاً ما:

$$z^2 + 1 = (a^2 + b^2)y$$

$$z^2 + 1 \equiv 0 \quad moda^2 + b^2$$
$$a^2 + b^2 \equiv 0 \quad moda^2 + b^2$$

$$z^2 \equiv \frac{b^2}{a^2} \quad moda^2 + b^2 \iff$$

$$(za + b)(za - b) \equiv 0 \ moda^2 + b^2$$

إذا كان $za - b$ هو المضاعف لـ $a^2 + b^2$ عندها من البداية تبدل $c$ بـ $-c$ ولا يؤثر على المطلوب كلياً (فهو لم يطلب أربع مجاهيل موجبة) وإذا كان $za + b \mid a^2 + b^2$ عندها أوجدنا الأعداد الصحيحة $c, d$ بحيث: $z = ab + cd \qquad ab - cd = 1 \qquad x = a^2 + b^2$

نعوض في المعادلة نجد أن $y = c^2 + d^2$ .

- ☒ لاحظ أن هذا النوع من الالتفاف مألوف في مسائل الهندسة.
- ☒ الحل المعتمد على طريقة الحل الأصغري تحفة فنية يجب الاطلاع عليها (Euler's problem).

---

نعم لقد برهنا أن $\sum_1^{p^{-1}} x^t \equiv 0 \ modP$ وهذه تجعل كل المجاميع تكافئ 0، إذا تم أخذها على كافة قيم البواقي، وبالتالي: $X \equiv 0 \ modP$ وهذا تناقض.

## صيغة ليجندر

في إثبات صيغة ليجندر سنستخدم خاصية من خواص الفلور وهي:

$$\left\lfloor \frac{\left\lfloor \frac{n}{P} \right\rfloor}{P} \right\rfloor = \left\lfloor \frac{n}{P^2} \right\rfloor$$

✓ هل يمكنك تخيل سبب صحة هذه العلاقة؟

نعم تخيل أنك في نظام كتابة $P$ على اليسار، نزيل الآحاد ثم العشرات، على اليمين نزيل الآحاد والعشرات معاً.

صيغة ليجندر هي صيغة لحساب عدد قوى $P$ الموجود في جداء عاملي، ويرمز له $e_P(n)$ أي عدد قوى $P$ الموجودة في $n!$

$$e_P(n) = \left\lfloor \frac{n}{P} \right\rfloor + \left\lfloor \frac{n}{P^2} \right\rfloor \dots \left\lfloor \frac{n}{P^t} \right\rfloor \dots$$

لا تقلق من الحدود إلى اللا نهاية فكلها ستصبح 0 بعد حد معيين

إثباتها ومعناها واضح جداً وبديهي، ولكن هناك صيغة أخرى لـ $e_P(n)$ وهي تحتاج لإثبات، وهي ظريفة جداً ومغلقة:

$$e_P(n) = \frac{n - s_p(n)}{P - 1}$$

حيث $s_p(n)$ هي مجموع منازل العدد $n$ مكتوباً في النظام $P$ ... لإثبات الخاصية حتماً سنكتب $n$ في النظام $P$: $n = a_+P^+ + \cdots a_2P^2 + a_1P + q_0$، الآن يمكن كتابة $n$ و $s_p(n)$ بدلالة هذه الكتابة:

$$\left\lfloor \frac{n}{P^i} \right\rfloor = a_tP^{t-i} \dots a_{i+1}P + a_i$$

$$\left\lfloor \frac{n}{P^{i+1}} \right\rfloor = a_tP^{t-i-1} \dots a_{i+1}$$

لكي نحصل على الخانات لكي نصل إلى $s_p(n)$ بسهولة نأخذ:

$$\left\lfloor \frac{n}{P^i} \right\rfloor - p\left\lfloor \frac{n}{P^{i+1}} \right\rfloor = a_i$$

... العلاقة الرسمية لإيجاد المنزلة.

بالجمع التلسكوبي نجد:

$$(1-P)\sum\left\lfloor\frac{n}{P^i}\right\rfloor = n - s_p(n)$$

لاحظ أنه في التلسكوبي: كرسم توضيحي لما حصل

$$n - @$$

$$@ - \#$$

$$\# - \$$$$

$$\ldots\ldots$$

$$\ldots.. - \&$$

$$\& \quad - \quad (p\left\lfloor\frac{n}{P^{i+1}}\right\rfloor = 0)$$

---

- أثبت أن: $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ عدد صحيح:

سنقارن قوة أي عدد أولي وسنثبت أن قوة البسط أكبر أو تساوي المقام:

لدينا حسب ليجندر في البسط:

$$e_P(2m) + e_P(2n) = \sum_1^\infty\left\lfloor\frac{2m}{P^i}\right\rfloor + \sum_1^\infty\left\lfloor\frac{2n}{P^i}\right\rfloor =$$

وفي المقام:

$$\sum_1^\infty\left\lfloor\frac{m}{P^i}\right\rfloor + \sum_1^\infty\left\lfloor\frac{n}{P^i}\right\rfloor + \sum_1^\infty\left\lfloor\frac{m+n}{P^i}\right\rfloor$$

يكفي إثبات أنه لأي عدد صحيح:

$$\left\lfloor\frac{2m}{P^i}\right\rfloor + \left\lfloor\frac{2n}{P^i}\right\rfloor \geq \left\lfloor\frac{m+n}{P^i}\right\rfloor + \left\lfloor\frac{m}{P^i}\right\rfloor + \left\lfloor\frac{n}{P^i}\right\rfloor *$$

وبشكل آخر أبسط للمتراجحة:

$$\lfloor 2x\rfloor + \lfloor 2y\rfloor \geq \lfloor x+y\rfloor + \lfloor x\rfloor + \lfloor y\rfloor$$

لأي عددين نسبيين $x, y$ سننظر إلى $[x], [y]$ على أنها الأرضية الأساس، وننظر إلى $[x+y], [2y], [2x]$ كم ستزيد عن الأرضية.

لكي يزيد $[x+y]$ عن $[x]+[y]$ بمقدار 1 يجب أن يكون $x$ أو $y$ بجزء عشري أكبر من $\frac{1}{2}$ وليكن $x$ ... عندها $[2x]$ سيزيد عن $2[x]$ بـ 1 أيضاً وبالتالي فعلاً اليسار أكبر أو يساوي اليمين (أكبر تماما عندما كل من $x$ أو $y$ بجزء عشري أكبر من $\frac{1}{2}$)

الآن برهن أن ☺:

$$\frac{(3x)!\,(3y)!\,(2x+2y)!}{(2x+y)!\,(2y+x)!\,(x+y)!\,x!\,y!}$$

أيضاً إثباتها حتماً مناقشة حالات، ولكن إذا اعتمدت مبدأ الزيادة عن القاعدة ستختصر الوقت ولن تتعذب كثيراً في مناقشة كل الحالات.

---

## القسمة من خلال عدد القوى

تقول **النظرية** أنه إذا أثبتت أنه من أجل أي عدد أولي $p$ يوجد في البسط $p$ أكثر من المقام عندها البسط مضاعف للمقام أي الكسر صحيح.

أو إذا وجدت عدد أولي واحد يحقق العكس عندها البسط غير مضاعف للمقام ببساطة.

**مثال1:** أثبت أنه أي كان العددين $m, n$ عندها

$$\frac{1}{m}+\frac{1}{m+1}+\frac{1}{m+2}+\cdots+\frac{1}{m+n}$$

لا يمكن أن يكون عدداً صحيحاً.

**الحل:**

إذا كان عدد صحيح عندها

$$\frac{\sum \text{جداء الكل ما عدا واحد}}{m(m+1)(m+2)\dots(m+n)}$$

إنه جداء طويل

لا يمكن أن نأخذ $mod$ بسيط لأنه معظم الأرقام الأولية ستوجد في البسط والمقام كـ 2, 3 لذا لنلجأ لعددها في البسط والمقام أي إلى النظرية السابقة.

كما أنه نحتاج لعدد اولي واحد فقط لتنقض لذا نختار الأسهل الـ 2

الآن من الواضح أنّ كل حدود البسط تحوي أقل من المقام ولكن هذا غير كافي لأنه كما قلنا أن قوة مجموع حدود هي أصغر قوة بين الحدود إلا إذا تكررت عندها ربما بجمع الحدين المكررين أن نحصل على قوة اكبر والتي بدورها قد تجمع لقوة مساوية لها وهكذا حتى تتولد قوة في البسط أكبر من المقام. اي $2^4 + 2^4 + 2^5 = 2^5 + 2^5 = 2^6$

لذا كيف نتأكد من أن هذه الثغرة لن تكون موجودة

علينا أن نبرهن أن أصغر قوة لن تتكرر.

ماذا علينا أن نثبت؟ فكر...

نعم علي ان اثبت أن أكبر قوة لـ 2 في أحد الاعداد التالية $m, m+1, .., m+n$ لن تتكرر (أي في أعداد متتالية). (لانه تذكر ان واحدا منها سيزال في كل حد في البسط )

والان الفكرة الاقوى

بالتأكيد لن تتكرر لأن العدد الذي أكبر قوة فيه 5 مثلا والعدد التالي الذي أيضاً أكبر قوة فيه 5 بينهما عدد أكبر قوة فيه 6.

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

بينهما $2^{n+1}$

فالكلام السابق كمثال عن فكرة أنه في أعداد متتالية القوة الأكبر لـ 2 التي تظهر في هذه الأعداد تكون وحيدة حصراً.

**مثال 2:** أثبت أن

$$n! \mid (2^n - 2^0)(2^n - 2^1)(2^n - 2^2) \cdots (2^n - 2^{n-1})$$

**الحل:**

إذاً

$$n! \mid (2-1)(2^2-1)(2^3-1) \cdots (2^n-1) \cdot 2^{\frac{(n-1)n}{2}}$$

أولاً من أجل العدد الاولي 2 لنثبت أن $n!$ تحوي أقل من $\frac{n(n-1)}{2}$ من الـ 2

هذا في غاية البساطة بالطبع لا يوجد عدد من $1 \rightarrow n$ يحوي أكثر من $n-1$ من "2"

وهنالك $\frac{n}{2}$ عدد زوجي ....خالصة.

والآن فكر بأي عدد أولي آخر،، $p$

فكر أن أي قوة لـ $p$ توجد في عدد ما من $1 \rightarrow n$ ضمن العاملي وليكن $p^k t = m$.. كيف سنوجد ما يغني عنها في أحد $2^a - 1$ حيث $a$ من $1 \leftarrow n$

بما ان $m = p^k t$ نختار $2^{p^{k-1}(p-1)t} - 1$ ليعوض عنها.

وهكذا نضمن أن البسط يحوي أكثر من المقام لكل الأعداد الأولية. ■

**ملاحظة:** هذه المرة اســتطعنا التعامل مع العدد الأولي في $n!$ دون اســتخدام صــيغة ليجندر لكن سنحتاجها حتماً في مسائل أخرى ..

**المسألة الثالثة:**

أثبت أنه من أجل عدد طبيعي $n$ تتحقق العلاقة:

$$(n+1)(lcm\left(\binom{n}{0},\binom{n}{1},\dots\dots\dots,\binom{n}{n}\right) = lcm(1,2,\dots,n+1)$$

**الحل:**

رائعة جداً المسألة وطريقة حل صاحب المسألة كانت تعتمد على خاصتين للتوافيق **هامتين جداً** حيث عندما أُضــيف $n+1$ إلى الجداءات المتتالية في البســط الخاص ب$\binom{n}{k}$ نريد تحويل هذا الحد إلى توافيقات أخرى فمرة أضفنا $k+1$ إلى المقام ومرة أخرجنا $n-k+1$ من نهاية البسط (اصغر الجداءات)

فنحصل على علاقات هي كالتالي:

$$(n+1)\binom{n}{k} = (n-k+1)\binom{n+1}{k} = (k+1)\binom{n+1}{k+1}$$

فائدة هذه العلاقات انه اذا ادخلنا$n+1$ الى داخل ال $lcm$ نحصــل على الطرف الايسرــ من العلاقات السابقة $(n+1)\binom{n}{k}$

ومن ثم جاء بفكرة اضافية اقوى وهي بان $\binom{n+1}{i} \not\equiv 0 \ mod\ p^{r+1}$ حيث $p^r < n+1 < p^{r+1}$

بالعودة لطريقتنا في الحل نشــير أنه من الممكن أن تتم **بطريقة ابتدائية دون معرفة صــيغة –ليجندر** أكثر بالاعتماد على الفكرة التالية

- <u>هاام جدا</u>ا أكبر قوة في جداء أعداد متتالية $p^k$ تكون مثل الزعيم بعده تكون بداية جديدة.

وكأننا بدأنا من الصفر (يكون بمثابة الصفر) وذلك من ناحية عدد الـ $p$ الموجودة في الأعداد التي بعده

بدايةً من أجل أن نثبت المساواة في مثل هذه المسألة يجب أن نثبت أن قوة أي عدد أولي $p$ هي نفسها في الطرفين فإذاً لنأخذ $k$ الذي يحقق

الآن في المثال $p^k < n < p^{k+1}$

**مثلاً** في حالة $p^{k+1} = n+1$ أي عندما تأخذ الـ $n+1$ أكبر قوة في الأعداد من $n+1 \rightarrow 1$ لذا الـ $lcm$ أكبر قوة فيه لـ $p$ هي $k+1$ أما الطرف الأيسر فيحوي على $n+1$ وبالتالي يحوي على $k+1$ قوة للـ $p$ إذاً بقي أن نثبت أنّ $p$ لا تقسم $\binom{p^{k+1}-1}{k}$ ليتحقق شرط المساواة ...بالفعل

$$\left(\frac{p^{k+1}-1}{i}\right) = \frac{(p^{k+1}-1)(p^{k+1}-2)\dots(\,)}{1\cdot 2\cdot 3\cdots i}$$

وبالتالي بالتأكيد لا يوجد $p$ في الكسر هذا ... لأن $p^{k+1}-r$ تحوي نفس عدد الـ $p$ في $r$ لأن $p^{k+1}$ أكبر قوة حتى قبل الـ $p^{k+1}$ كأننا بدأنا من جديد.

- تذكير عندما قلت لك أنه هناك أخطار عند أخذ $mod\ p$ لكسر حيث لا يمكن أن تأخذ $mod\ p$ البسط لوحده والمقام لوحده.
- صراحةً يمكنك أخذ $mod\ p$ على كل شيء غير مضاعف لـ $p$ أما المضاعف لـ $p$ لا يمكنك ذلك لأنه تخيل عددين في البسط والمقام مضاعفين لـ $p$ مثل $\frac{5p}{3p}$ كلاهما نفس القيمة في الـ $mod\ p$ أي $0$ ولكن تذكر أنه كسر لذا تختصر الـ $p$ $\frac{5}{3}$ وبالتالي اختلفت النتيجة بال $mod\ p$

الآن تتمة المسألة نفرض $p^r || n+1$ حيث $r < k+1$.... علينا أن نثبت أن $\binom{n}{i}$ تحوي **أقل أو يساوي** $k-r$ من قوى الـ $p$ (تذكر أنّ الـ $k$ هي القوة الحاصرة للـ $n$) ونجد أنّ $lcm$ الطرف الأيمن يحوي $k$ من $p$ .

الآن البسط نعرف بدايته لا نعرف نهايته

$$(p^r t-1)\dots.(p^s+1)\,p^s\dots$$

ولكن نفرض أنه في البسط أكبر قوة كانت $s$ (ليس بالضرورة أن يصل لـ $k$).

الآن المقام يصبح $1\times 2\times 3\dots(p^r t-p^s)\dots i$

كما قلنا ما بعد الـ $p^s$ بداية جديدة في البسط لذا يختصر مع الاعداد من 1 إلى $p^r t-p^s-1$ في المقام

الآن ما قبل $p^s$ في البسط أيضاً أصبح من $1 \leftarrow t$ ستبدأ كأنها من الـ 0.

وبعد $p^r t-p^s$ في المقام جداء $t$ عدد متتالي إذاً

إما $\boldsymbol{s \le r}$ عندها القوة في هذا الحد هي s وهذا ممتاز لأن الـ $t$ عدد متتالي سيبدؤون من الصفر أيضاً.

وبالتالي معاً يشكلان توافيق ولكن بالمقلوب إذا البسط يحوي تماما نفس قوة المقام. وبالتالي في هذه الحالة الكسر بشكل كامل

أما حالة $s > r$ عندها الحد $p^r t - p^s$ سيحوي قوة $r$

والأعداد الـــ $t$ المتتالية في المقام هي لن تبدأ من الـــ 0 نسبة ل $p^s$ بل **ستبدأ بأفضلية** $+p^r t + 1$ لذا جداء الـ $t$ عدد في المقام سيحوي قوى أكبر أو تساوي قوى جداء ال $t$ عدد في البسط

إذاً كمحصلة

الحد $p^s / p^r t - p^s$ سيحوي $s - r$ قوة للـ $p$ والكسر باكمله سيحوي $s - r$ قوة أو اقل حسب جداء الـ $t$ عدد في المقام

والســـطر الختامي الاهم والمريح اننا نختار $s = k$ و نختار ال $i$ تســـاوي $p^r t - p^s$ لكي ينتهي الجداء في المقام عند هذا الحد بالذات وألا ارهق نفسي بالتعامل مع الاعداد التي كانت تاتي بعده

وبالتالي قوة ال $p$ الموجودة في هذه الحالة هي $k - r$

$\binom{n}{i}$ تحوي أقل **أو يساوي** $k - r$ من قوى الـ $p$ ..... (حيث $s$ أكبر ما يمكن أن تكون هو $k$)

وهو المطلوب

الآن ربما عرضـــت لك كل المهارات التي يمكن أن تتعلمها من هذا القســـم وهي أفكار احترافية للغاية ...ويبقى الحل باســتخدام التوافيق أبســط ولكن وجب عرض هذا الحل لأنه يعرض قدرتك على الـــ *brutal force* اي سلك الطريق الطويل لانه مضمون

**خلاصة الأفكار:** عندما تأخذ أكبر قوة لـ $p$ في جداء أعداد متتالية فأنت تخلق قبلها وبعدها جزئين كلاهما جداء أعداد من 1 حتى عدد معيين في قواها بالنسبة ل $p$

وان جداء أعداد متتالية **بدءاً من 1** إلى عدد معيين $t$ تمثل **مقام كسر التوافيق** لذا هي تقســـم جداء أي $t$ عدد متتالي بالنسبة لقوى الـ $p$ طبعاً ...هذا فقط 👌

**المسألة الرابعة:**

أثبت أنه من أجل أي صحيح موجب $n$, $2^n$ لا يقسم $n!$

**الحل:**

ببساطة علينا إثبات أن $n!$ لا يحوي $n$ من الـ 2 ولكن كيف نحسب كم $n$ موجودة في $2^n$؟!!

**هناك قاعدة مخصّصة لذلك تدعى ليجندر *Legendre* تقول:**

$$v_2(n!) = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n}{8} \right\rfloor + \cdots + \left\lfloor \frac{n}{2^k} \right\rfloor + \cdots = \sum_{1}^{\infty} \frac{n}{2^i}$$

واللانهاية ليست شيء عظيم لأنه بعد عدد محدود ستتحول كل الحدود إلى 0 لماذا؟

بالعودة إلى المسألة علينا إثبات أنّ:

$$A = \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{4} \right\rfloor + \left\lfloor \frac{n}{8} \right\rfloor + \cdots + \left\lfloor \frac{n}{2^k} \right\rfloor < n$$

وذلك واضح لأن

$$A < \frac{n}{2} + \frac{n}{4} \ldots . \frac{n}{2^k}$$
$$= n\left(\frac{1}{2} + \frac{1}{4} \ldots . . \frac{1}{2^k}\right)$$
$$n\left(1 - \frac{1}{2^k}\right) < n$$

## المسألة الخامسة :

من اجل اي عدد طبيعي $k$ اثبت انه يتحقق لدينا

$$2^{3k} \mid \binom{2^{k+1}}{2^k} - \binom{2^k}{2^{k-1}}$$

في هذ المسألة لو تابعنا بنفس منوال المسائل التي تسبقها والتي تحوي على طرح في قسم حساب بواقي طويلة نفك التوافيق وربما نزيل المقامات ... ثم نلاحظ الفخ المعدّ في هذه المسألة.

نعم إننا نتعامل في $mod2^n$ أي $mod$ قوى الـ 2 ولم يحتوي الطرف الأيمن على أعداد فردية فقط ... هنا تبدأ المشاكل، فمثلاً لو رغبنا بإكمال أسلوبنا لضربنا بالمقام، ولكن تذكر أن المقام يحوي الكثير من الـ 2، لو ضربنا بالمقام نضطر لأن نزيد قوى الـ 2 الموجودة فيه إلى $2^{3k}$ – وقوى الـ 2 في المقام (أي $2^k$ !) هي $\frac{k(k+1)}{2}$ حسب ليجندر وإذا ضربناها ب $2^{3k}$ سنشوه شكل المسألة لذا يجب أن نحافظ على المقامات، وبتوحيد المقامات مثلاً سنحاول عديداً أن نفك ونعدل على شكل $2^k + i$ ولكنها ليست بالشكل الجميل الذي يعدل، لذا سنبدأ باعتبار كل حد على حدا، خصوصاً أن لكل منها نفس الشكل عملياً ... الآن:

$$A = \binom{2^{k+1}}{2^k} = \frac{2^{k+1}(2^{k+1}-1)\,(2^{k+1}-2)\dots(2^k+1)}{2^k\,(2^k-1)\dots(1)}$$
$$= 2 \cdot \frac{(2^{k+1}-1)\,(2^{k+1}-2)\dots(2^k+1)}{(2^k-1)\,(2^k-2)\dots 2\times 1}$$

المعلومات التي نعرفها مباشرة عن المقدار الأخير أنه عدا الـ 2 على اليسار لا يحوي أي 2 أخرى لأن حدود البسط هي المجاورة لأكبر قوة في البسط وهي $2^{k+1}$ فنعطي وكأنها تبدأ من ال1...

وبالتالي حتماً لا يوجد 2 والأكثر من ذلك داخلياً علمنا أن كل حد من المقام يحوي نفس عدد الـ2 الموجود في الحد الذي يقع أعلاه في البسط ... لذا سنشعر ربما أنه يمكننا أن نختصر على الـ 2 وننتهي منها ونعود لأسلوبنا السابق ...

لكن تظهر لنا المشكلة بأن كل حد سيختصر مع الحد أعلاه على قوة مختلفة لـ 2 وبالتالي لن يحافظ الجداء على شكله وانتظامه ...

ولكن نهايةً يجب أن نفعل شيئاً تجاه هذه القوى الـ 2.

سنبدأ نعم على اختصارها جميعاً على 2 فقط (الحدود الزوجية طبعاً)، وبالتالي نحافظ على الأعداد الفردية في الجداء كما هي (حدود نحب التعامل معها).

ماذا عن الحدود الزوجية بعد الاختصار؟ ماذا تعطي؟

$$A = 2 \cdot \frac{(2^{k+1}-1)!!}{(2^k-1)!!} \cdot \boxed{\frac{(2^k-1)\,(2^k-2)\dots(2^{k-1}+1)}{(2^{k-1}-1)\,(2^{k-1}-2)\dots(1)}}$$

هنا التعريف: $(x)!! = x(x-2)(x-4)\dots 1/2$

(إذاً ما يصبح جداء الأعداد الزوجية المتتالية جميل بعد القسمة على 2)

الآن بالفعل نلاحظ أن المقدار:

$$A = \frac{(2^{k+1}-1)!!}{(2^k-1)!!} \cdot \binom{2^k}{2^{k-1}}$$

بالطبع لاحظت كيف يفيد هذا الشكل لـ A

$$= \binom{2^k}{2^{k-1}} \left( \frac{(2^{k+1}-1)!!}{(2^k-1)!!} - 1 \right)$$

والآن من مسألة سابقة نجد أن القوس الأيمن مضاعف لـ $2^{3k-1}$ ويكتمل الإثبات #.

**المسألة 6:** $n \in \mathbb{N}$ أثبت أن هذه الأعداد

$$\binom{2^n-1}{0}, \binom{2^n-1}{1}, \binom{2^n-1}{2} \dots \binom{2^n-1}{2^{n-1}-1}$$

تعطي جميع البواقي الفردية في $mod\ 2^n$

أولاً هل نحن متأكدون أن هذه الأرقام فردية حتماً؟ يجب حتماً أن نثبت ذلك لأن $2^{n-1}$ عدد وهو عدد البواقي الفردية المطلوب تأمينها ... طبعاً إثبات أنها فردية لم يعد تحدياً بعد الآن فقد تعمد وضع $2^n - 1$ (الحد المجاور لأكبر قوة لـ2) لكي تثبت بسهولة أنها فردية.

الآن أيضاً لأن عدد الحدود يساوي عدد البواقي المطلوب تأمينها ... يكفي أن نثبت أن أي حدين غير متساويين في $mod 2^n$

نلاحظ من طريقة كتابة الحدود:

$$\binom{2^n-1}{1} = \frac{2^n-1}{1}$$

$$\binom{2^n-1}{2} = \frac{2^n-1}{1} \cdot \frac{2^n-2}{2}$$

$$\binom{2^n-1}{4} = \frac{2^n-1}{1} \cdot \frac{2^n-2}{2} \cdot \frac{2^n-3}{3} \cdot \frac{2^n-4}{4}$$

لكي يتساوى حدّان، مثلاً الحد 1 والحد 4، عندها القطعة المشار إليها في الأعلى يجب أن تكافئ 1 في $mod2^n$ وهكذا ...

إذاً لنثبت المطلوب علينا أن نثبت أن كل القطع لا تكافئ 1.

نأخذ قطعة بدايتها $i$ ونهايتها $j$

$$A \equiv \frac{2^n-i}{i} \cdot \frac{2^n-(j-1)}{j-1} \dots \frac{2^n-j}{j} \quad mod2^n$$

نلاحظ المشكلة نفسها التي عانينا منها في المسألة السابقة، أنه يوجد فردي وزوجي ... وكالعادة الحدود الفردية (أي البسط والمقام فرديان) $\frac{2^n-t}{t} \equiv -1$ ، أما الزوجي فلا يحسب مباشرة، بل يعتمد على قوة 2 المختصرة.

إذاً من الحكمة تعديل $A$ بحيث نعوض الحدود الفردية ب $-1$ وأما الأعداد الزوجية فماذا نفعل بها؟ نعم نختصر على 2 واحدة فقط.

**سنسميها العملية نجمة**

$$A \equiv (-1)^t \frac{2^{n-1} - \left\lfloor \frac{i}{2} \right\rfloor}{\left\lfloor \frac{i}{2} \right\rfloor} \dots \frac{2^{n-1} - \left\lceil \frac{j}{2} \right\rceil}{\left\lceil \frac{j}{2} \right\rceil}$$

$mod2^n$

نلاحظ أنه لا يمكننا تعويض الحدود الفردية الآن بـ $-1$ بعد هذه الخطوة لأنه لدينا $2^{n-1}$ في البسط... هل أغلقت المسألة أبوابها هنا؟

بالعكس تماماً – الاكتشاف الأقوى هو أن التعامل مع المقدار الآن أصبح أسهل – سنكمل بـ $mod2^{n-1}$ فإذا كان المقدار لا يكافئ 1 في $mod2^{n-1}$ عندها حتماً لا يكافئ 1 في $mod2^n$... إذاً وضوحاً بالاستقراء – فماذا يصبح الفرض الاستقرائي إذاً؟ ...

بالاستقراء على $n$ أنه من أجل أي عددين $i < j < 2^{n-1}$ المقدار: $\frac{2^n-i}{i} \dots \frac{2^n-j}{j}$ لا يكافئ 1 في $mod2^n$ ولكن هناك قيمة غير الـ 1 قد تسبب إشكالاً نظراً لآخر شكل وصلنا له في $A$، نعم الـ $-1$ لأنه لو

كان $(-1)^t = -1$ والمقدار على يمينه (الذي يمثل الخطوة الاستقرائية $n - 1$) لا يمكن عندها ان نسمح له أن يكون $\equiv -1$،

للوقاية من ذلك

نضيفها إلى الفرض الاستقرائي ان المقدار هذا لايمكن ان يعطي $-1, 1$، وطبعا عند الاضافة الى الفرض الاستقرائي يترتيب علينا ضرائب ..وهي ان نثبت ما اضفناه على الحالات الابتدائية فقط

والآن ما هي خطوة البدء الاستقرائية (سنتخيل لو رجعنا عدة مرات من $n \leftarrow n - 1$ وهكذا)

ستكون خطوة البدء ب3او 2 لاننا فرضنا ان $i < j$حد لكي نثبتها في هذه الحالات نطبق العملية نجمة مرة اخيرة

ما هو الحد الذي سيبقى؟ ... (جرب أرقام إذا ضيّعت) ... بالفعل آخر خطوة سنزيل الحدود الفردية ويبقى حد زوجي $\frac{2^a - 2k}{2k}$ وحيد ... هل نقسمه على 2؟ ... يمكن أن نقسمه، ولكن سنناقش في $mod 2^{a-1}$

$$\frac{2^{a-1} - k}{k} \equiv 1 \ mod \ 2^{a-1}$$

نجد أنه مستعد لأن يأخذ قيم 1 و $-1$ فإذاً سنناقش على $mod 2^a$ لأنه بالأصل كنا ننتقل إلى $mod 2^{a-1}$ لصعوبة الحسابات فقط ...

الآن:

$\frac{2^{a-1} - k}{k} \equiv 1 \ mod \ 2^{a-1}$ فرقنا البسط والمقام لأنها حركة شرعية بكل الأحوال.

$$\frac{2^{a-1}}{k} - 1 \equiv 1 \ mod \ 2^{a-1}$$

$$\frac{2^{a-1}}{k} \equiv 2 \ mod \ 2^{a-1}$$

$$k \equiv 2^{a-2} \ mod \ 2^{a-1} \Leftarrow$$

$\Leftarrow 2k = 2^{a-1}$ أي الحد الأخير الذي يمكن أن يسبب مشاكل هو: $\frac{2^a - 2^{a-1}}{2^{a-1}}$ ، لكن كي يبقى هذا الحد للنهاية دون أن يعوض ب $-1$ نتذكر بأنه تم اختصار 2 من البسط والمقام $n - a$ مرة، وبالتالي في خطوة $\left(\frac{2^n - i}{i} \dots \frac{2^n - j}{j}\right)$ كان هذا الحد يساوي $\frac{2^n - 2^{n-1}}{2^{n-1}}$، وهذا تناقض واضح لأن $i, j < 2^{n-1}$

**هنالك الكثير من المسائل تتطلب منا التعامل مع التوابع الشهيرة جبريا .. ونستفيد من خواصها طبعا وهنا مسالة على تابع اخذناه مسبقا وتعاملنا معه..**

مسالة :

لدينا المتتالية $a_n = \tau\ (n^2 + 1)$ من اجل كل الأعداد الموجبة ... أثبت أنها لن تصبح متزايدة تماما بعد حد $a_N$ حيث $N$ عدد طبيعي

الحل:

الآن هناك نسختان من المسألة، الأولى متزايدة تماماً (وهي المقصودة)،

حيث لو فرضنا انها عند حد معيين تصبح متزايدة تماما ..نلاحظ أن المتتالية ستزيد بكم من حد لحد؟؟

نعم ستزيد بقيمة "2" وليس 1 لأن كل الحدود فردية (**علل**).

وبهذه الزيادة ستصبح الحدود كبيرة نسبيا ..كما يلي

$$-\tau\ (n^2 + 1) \geq 2(n - N)$$

إحساساً أو رياضياً المقدار $2(n - N)$ سيصبح حتماً أكبر من $n$،..وذلك عندما $n$ تتجاوز $2N$ هل هذا مقبول ان يصبح $\tau\ (n^2 + 1) \geq n$

؟ **لا** – أثبت ذلك –

كيف اثبت ان عدد قواسم عدد اصغر من جذر هذا العدد

إذا تخلصنا من التزايد التام على شكل خطي الذي تغلب على $\tau$ الnتربيع+1،

أما في نسخة التزايد غير التام ... لابد أن نوجد شكلاً ضعيفاً أمام الـ + ...اي جزء كبير منه يكون عددا اوليا واحدا

وشكلاً قوياً أمام الزائد ((كلما تحلل المقدار داخل الـ $\tau$ أعطى $\tau$قيماً أكبر))

كل هذه تنبؤات عن طريقة حل مثل هذه المسالة

## التوابع الشهيرة في نهاية الأعداد

- **تابع عدد قواسم عدد صحيح $T$:**

إذا كان لدينا عدد صحيح $n$ يكتب بالشكل $n = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ عندها يكون عدد قواسمه أي $T(n)$:

$$T(n) = (a_1 + 1)(a_2 + 1) \dots (a_n + 1)$$

برهان هذه الصيغة سهل للغاية ... لكي يكون العدد قاسماً لـ $n$ يجب أن تكون قوى كل أعداده الأولية أصغر أو تساوي قوى الـ $n$.

للقوة $P_i$ يوجد $a_i + 1$ احتمالاً متضمناً $a$ حسب النظرية الأساسية في الحساب.

- **إتمام فكرة التابع الضربي:**

**تعريفه**: هو تحقيق التابع أنه من أجل أي عددين $n, m$ أوليين فيما بينهما فإن: $f(mn) = f(m) \cdot f(n)$ أي كما استقل $n, m$ فالـ $f$ يحافظ أيضاً على الاستقلالية، وعملياً أكثر نجد أن الـ $f$ يعامل كل قوة لـ $P_i$ لوحدها باستقلال.

وبالفعل كل توابعنا التي سنناقشها تحقق الضربية $\emptyset(n), T(n)\ \sigma(n)$ ← سنأتي في شرحه، لكن الفكرة الأقوى أن التابع التجميعي لأي تابع ضربي هو تابع ضربي.

التابع الجمعي هو كما في الآتي:

$\sum_{d_i} f(d_i)$ حيث $\{d_i\}_1^{T(n)}$ تمثل مجموعة كل قواسم $n$.

كثيراً ما سيمر معك في المسائل هذه السيغما على قواسم العدد، هنا إشارة واضحة إلى التابع الجمعي.

الآن يجب أن نأخذ فكرة عن كيفية إثبات أن التابع التجميعي لتابع ضربي هو ضربي:

$n = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ نلاحظ أن مجموعة $d_i$ تشمل جداء قوى مختلفة ل $p_i$ أصغر أو يساوي $a_i$، والاستفادة من أن $F$ ضربي:

$$F(n) = \sum_{d_i} f(d_i)$$

$$= \sum_{d_i} f(p_1^{b_1} p_2^{b_2} \dots p_+^{b_+})$$

$$= \sum_{0 \le b_1 \le a_1} \sum_{0 \le b_2 \le a_2 \dots} f\left(p_1^{b_1}\right) f\left(p_2^{b_2}\right) \dots f\left(p_+^{b_+}\right)$$

الآن حسب خواص السيغما:

$$F(n) = F\left(p_1^{a_1}\right) \cdot F\left(p_2^{a_2}\right) \cdot \dots F\left(p_n^{a_n}\right)$$

إذاً حتماً التابع التجميعي هو تابع ضربي.

**ملاحظة:** إن كان لديك شك بخواص السيغما جربها على أرقام صغيرة، أن يكون لديك عدة أدلة لتوابع مضروبة باستقلال عن بعضها (حتماً ستخرج عامل مشترك).

الآن لنرى كيف يمكن أن نستفيد من فكرة الضربية؟

☒ أثبت الخاصية التالية، حيث $\{d_i\}$ هي مجموعة قواسم الـ $n$:

$$\left(\sum_{d_i} T(d_i)\right)^2 = \sum_{d_i} T^3(d_i)$$

**الإثبات:** لاحظ أن هذه الخاصة تشابه كثيراً خاصية جمع الأعداد من $1 \leftarrow n$ ... لذا تبدو هذه الخاصة مهمة جداً ((كيف للتابع $T$ أن يحققها أيضاً)) لنفحص ذلك:

على اليسار لدينا التابع التجميعي لـ $T(d_i)$ الضربي، إذاً فالتجميعي ضربي، فإذا كان $n = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$:

$$LHS = \left(\sum_{d_i \mid n} T(d_i)\right)^2 = \prod_{p_i}\left(\sum_{d_i \mid p_i^{a_i}} T(d_i)\right)^2$$

يجب أن نصل لمرحلة أن نتخيل هذه الخطوة قبل كتابتها:

$$LHS = \prod\left(\sum_{0}^{a_i} i + 1\right)^2$$

أما الطرف الأيمن فهل $T^3(n)$ ضربي؟ ... حتماً ضربي، إذاً التابع التجميعي له ضربي:

$$RHS = \sum_{d_i \mid n} T^3(d_i) = \prod\left(\sum_{d_i \mid p_i^{a_i}} T^3(d_i)\right) \Leftarrow$$

$$= \prod_{p_i}\left(\sum_{0}^{a_i} (i+1)^3\right)$$

$$RHS = LHS \Leftarrow$$

والآن نجد وضوحاً لمَ تحقق نفس خاصية الأعداد من $n \leftarrow 1$، والفكرة أننا لو جربنا $n = p_i^t$ في البداية كنا لاحظنا كيف ستحقق نفس الخاصية تماماً.

- **تابع $\boldsymbol{M\ddot{o}bius}$:**

هو التابع الرابع في التوابع الضربية الشهيرة، غالباً ما يتم إهماله من بين الـ 4 رغم مواجهتنا لصعوبة تطبيق فكرته في بعض المسائل دون أن نعلم أنه $M\ddot{o}bius$ ..كما في إثبات خاصية مهمة سنتطرق لها...

$$\mu(n) = \begin{cases} (-1)^k & \text{إذا كان } n = P_1 P_2 \dots P_k \text{، أي كل عدد أولي يعطي } (-1) \\ 0 & \text{إذا كان } P^2 \mid n \text{، أي أنه يحزن إذا دخل فيه مربع} \\ 1 & \text{فقط لتغطية حالة } n = 1 \end{cases}$$

$$\mu(2^2.3) = 0 \qquad \mu(15) = 1 \qquad \mu(30) = -1$$

وبوضوح إنه تابع ضربي حيث

.. سيبقى التربيع موجوداً مهما فرقنا $n$ إلى أعداد أولية فيما بينها ((قوة العدد الأولي لا تفررق)) وبالتالي تبقى النتيجة 0.

وبالنسبة للسطر الأول ... كل عدد أولي سيعطي $1-$ وبالتالي الضربية واضحة.

الآن المكان الذي خلق فيه $M\check{o}bius$، ليكن $f$ **تابع ضربي،** إذا كان $n = P_1P_2 \dots P_n$ :

$$A = \big(1 - f(p_1)\big)\big(1 - f(p_2)\big) \dots \big(1 - f(p_n)\big) =$$

ماذا يساوي فك هذا المقدار؟

نريد أن نقول أنه بعدد الأعداد الأولية التي ضُرِبَت ببعضها نحدد إشارة كل $f$ في المنشور، أما بعد ولادة $M\check{o}bius$ تحول الكلام إلى رمز:

$$A = \sum_{d \mid n} \mu(d)\, f(d)$$

بما أن التابع ضربي فهو يقحم الأعداد الأولية ضمن نفس الـ $f$ فيتشكل بوضوح أحد قواسم $n$، أما إشارة السالب يتولى أمرها $\mu$.

---

ليكن $f(n)$ تابع لا نعرف إذا كان ضربياً أم لا، وليكن $F(n)$ تابعه التجميعي، أثبت أن:

$$f(n) = \sum_{d \mid n} \mu(d)\, F(\frac{n}{d})$$

هذه هي الخاصة المدمرة، تتطبقها دون أن تشعر بمبدأ الإقصاء والتضمين، حيث تجمع وتطرح دوائر كبيرة لتحصل على قطعة صغيرة في النهاية، ولاحظ أن $f$ أصبحت تحسب بتابع تجميعي ... و $M\check{o}bius$ هو الذي خلق هذه الحلقة.

الآن لنثبت الخاصية: سأكتبها مثل الحل الرسمي مع توضيح التفاعل مع سيغما ليصبح بإمكانك استخدام هكذا كتابات بنفسك:

$$\sum_{d\mid n}\mu(d)\,F(\frac{n}{d})=\sum_{d\mid n}\mu(d)\left(\sum_{c\mid\frac{n}{d}}f(c)\right)=\sum_{d\mid n}\left(\sum_{c\mid\frac{n}{d}}\mu(d)f(c)\right)$$

في هذه الخطوة فقط أدخلنا العامل المشترك $\mu(d)$ على المجموع الخاص ب$F(n)$لنرى الكل مضروب بالكل.

$$=\sum_{c\mid n}\left(\sum_{d\mid\frac{n}{c}}\mu(d)f(c)\right)$$

في هذه الخطوة الاخيرة توجد الفحوى، فبعد أن أظهرنا أن الكل مضروب بالكل سنغير،

اولا لاحظ ان $f$ ديما المجهول الذي نضعه ضمنه هو $c$ ...وضمن التابع $\mu$ دائما d

الان تخيل معي التغيير ...بدل ان نعرضهم على شكل $\tau(n)$ مجاميع كبار ..في كل منهم يتغير ال $c$

**سنسحب قيمة ثابتة ل $c$ من كل مجمع** ونضعها في مجمع ..فنلاحظ الصيغة الجديدة انه الان في كل مجمع كبير قيمة ال$c$ ثابتة ..وضمن المجمع تتغير قيم ال $d$

والان

$$=\sum_{c\mid n}f(c)\sum_{d\mid\frac{n}{c}}\mu\,(d)$$

في اخر خطوة أخرجنا عاملاً مشتركاً $f(c)$ إلى دليله

$$=\ f(n)$$

حيث حسب الخاصية $\sum_{d\mid\frac{n}{c}}\mu(d)=0$ في حال $n\neq c$،اي حالة $\frac{n}{c}\neq 1$ وذلك لأننا جمعنا 1 مع $-1$ ثم 1 مع $-1$ كما كان يحدث في الإقصاء والتضمين.

والآن جاهزون للخاصية الهامة بأنه إذا كان $F$ التابع التجميعي للتابع $f$ وكان $F$ ضربي عندها $f$ ضربي.

الإثبات سهل: $f(n)=\sum_{d\mid n}\mu(d)\,F(\frac{n}{d})$

$F$ ضربي و $\mu$ ضربي $\Longleftarrow F\cdot\mu$ ضربي، و $f$ هو التابع التجميعي لـ $F$ $\mu$.

والآن مع تابع مجموع القواسم ... لفرد لإثبات بعض الخواص الجبرية لهذه التوابع:

1) أثبت أن: $\sigma(n) < n \mid n(n)$:

استفادة من الخاصة $\frac{1}{1}+\frac{1}{2}\dots\frac{1}{k} < 0.81 + ln\, k$

الفكرة الأقوى هي القسمة على $n$، ونذكر أن $\sigma(n)$ هو مجموع القواسم

$$\frac{\sigma(n)}{n} < ln\, n$$

$$\frac{\Sigma(d_i)}{n} < ln\, n$$

$$\Sigma\, \frac{1}{d_i} < ln\, n$$

لدينا:

$$\Sigma\, \frac{1}{d_i} < \frac{1}{1}+\frac{1}{2}\dots\frac{1}{T(n)}$$

$$< 0.81 + ln\big(T(n)\big)$$

كيف زبط $T(n)$ بـ $n$؟ الخاصة الأوضح والأجمل $2\sqrt{n} \geq T(n)$

$$\Sigma\, \frac{1}{d_i} < 0.81 + ln(2\sqrt{n})$$

$$< 0.81 + ln\, 2 + \frac{1}{2}\, ln\, n$$

$$< ln\, n$$

الأخيرة محققة على $n \geq 20$، ونجرب كل الأرقام تحت 20 فقط لنؤمن على تواجد هذه الخاصية.

$$\big(\sigma(n)\big)^2 \geq n\big(T(n)\big)^2$$

$$(\Sigma d_i)^2 \geq n\big(T(n)\big)^2$$

$$(\Sigma d_i)(\Sigma d_i) \geq n\big(T(n)\big)^2$$

$$(\Sigma d_i)\left(\Sigma \frac{n}{d_i}\right) \geq n\big(T(n)\big)^2$$

$$(\Sigma d_i)\left(\Sigma \frac{1}{d_i}\right) \geq \left(T(n)\right)^2$$

والتي هي كوشي شوارتز.

الآن أثبت $\sigma(n) < n\sqrt{2T(n)}$، هذه المرة $\sigma$ أصغر، أي تشبه الأولى.

استخدم الخاصية: $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} \ldots \frac{1}{n^2} \ldots = \frac{*^2}{6} < 2$:

أثبت أن $\sum_{d \mid n} \emptyset(d) = n$:

المسألة سهلة بالفعل، التابع على اليسار هو تابع ضربي، نحسبها من أجل $p^a$ نجدها محققة بالجمع التلسكوبي.

ولكن تعمدت وضعها آخر مسألة لأنه لا أسلوب آخر في الحل ظريف جداً يعتمد على الـ $bijection$.

سنقابل الأعداد من $1 \leftarrow n$ على الحدود $\{\emptyset(d)\}_{d \mid n}$، ليس بالضرورة أن نقابل مع الحد $\emptyset(t)$ الأعداد الأصغر من $t$ والأولية معه (بل سنقابل مع عناصر لها نفس العدد، وهنا ستكمن فكرة الحل).

أحد طرق تحديد عدد ما $x$ أصغر من $n$ هو أن نعرف قسمه المشترك مع $n$ وقسمه الأولي مع $n$.

مثلاً نأخذ قسمه المشترك هو $d$ أحد القواسم طبعاً، الآن حددنا القسم المشترك مع $n$ وبالتالي من $\frac{n}{d}$ يجب ألا يأخذ $x$ أي شيء = (أولي مع $\frac{n}{d}$)، وبالتالي لنعد الأعداد $1 \leftarrow n$ بطريقة أخرى نجد:

$$A = \sum_{d} \emptyset\left(\frac{n}{d}\right)$$

القسم المشترك — القسم غير المشترك

عدد اولي مع n/d

equation here.

$$A = n \Longleftarrow$$

$$\sum_{d} \emptyset\left(\frac{n}{d}\right) = n$$

## Rational numbers*

كيف نتعامل مع الأعداد النسبية:

عندما نريد حل معادلة ديوفانتية ولكن بأعداد نسبية **لدينا المبادئ التالية:**

$x = \frac{a}{b}$ حيث $a, b$ صحيحان أو الأفضل:

$x = \frac{m}{n}$ حيث $n, m$ صحيحان $(n, m) = 1$ وهو الشكل المختزل لأي عدد نسبي وهو الأكثر استخداماً

## معادلات ديوفانتية غريبة

عندما نتأمل معادلة من الشكل

$$x, y > 0 \quad x^2 + y^2 + 1 = xyz$$

والتي هي بالأصل مسألة قسمة

$$xy \mid x^2 + y^2 + 1$$

مما يجعل الـ $mod$ طريقة سيئة للمعادلة.

وهي لا تحل بالمتراجحات لأن الطرفين درجة ثانية في القسمة.

إذاً هناك إشارة لوجود عدد غير منته من الحلول وبالتالي لابد أن نلجأ لطريقة أخرى.

ما سنفعله في هذه المسائل يتمحور حول فكرة أننا:

- سنناقش أصغر الحلول ضمن العدد الغير منته من الحلول وهو موجود لأن $x, y > 0$ وأعداد صحيحة حصراً

الفكرة الرئيسية في المعادلة السابقة أننا يمكننا كتابة المسألة على الشكل:

$$x^2 - (yz)x + y^2 + 1 = 0$$

نفترض أن $y, z$ ثوابت والمعادلة السابقة هي معادلة تربيعية بدلالة $x$ عندها إذا كان $x_1$ حل ⇐

حل $x_2 = yz - x_1$

هذه هي الفكرة الرئيسية

**فمثلاً:**

في حال $x = y = 1 \ , \ z = 3$

$$x^2 + y^2 + 1 = 3xy$$

$(1,1)$ حل واضح، $(13,5)$ أيضاً حل ايضا بالتجريب.

ولكن لو استفدنا من فكرة المعادلة التربيعية يمكننا أن نحصل على عدد غير منته من الحلول

$(13,5)$ حل لو ثبتنا 13 عندها

⇐ $(13,13 \times 3 - 5)$ حل أيضاً $(13,34)$

نثبت 34هذه المرة

حيث بسبب تناظر المسألة نفس ما ينطبق على $x$ ينطبق على $y$.

$$(89,34) = (3 \times 34 - 13, 34)$$

إذاً حصلنا على عدد غير منته من الحلول ولكن يمكننا أن ننزل أيضاً بالحلول ليس فقط أن نصعد بها

وذلك نثبت 5 في $(13,5)$ وليس 13 هذه المرة كي نهبط $(2,5)$

نثبّت 2 فنحصل على $(2,1)$

لاحظ أنه إذا ثبّتنا عدداً مرتين نعود لنفس الثنائية لذلك لا نفعل ذلك.

الآن لو فكرنا أنه بدءاً بأي حل بالدنيا لو نزلنا كثيراً ما هو الحل الأصغري؟!! الحل الأصغري بحيث تبقى $x, y$ أعداداً موجبة، سنناقش حالة هذا الحل فقط.

ماذا سيحدث لو طبقنا نفس العملية عليه $3x - y$ ماذا سيحصل

- سيكون الحل الجديد حتماً مخالفاً للشروط فهو:
  - إما سالباً،
  - أو أكبر من الحل الأصغري

وفي الحالتين نكسب متراجحة من العدم(المتراجحة إما أن تأتي من فكرة اما الحل الجديد سالب(وبالتالي اصغر من صفر) أو أكبر من الحل الاصلي (الحل الأصغري)

**نعود للمسألة**

$$x^2 + y^2 + 1 = xyz$$

كما فعلنا في الصفحة السابقة نثبّت $z$ أي ندرس جميع الثنائيات $(x, y)$ التي تحقق المعادلة من أجل قيمة واحدة (صراحة فقط قيمة $z = 3$ سيكون عندها حلول)

لنحل المسألة

$$x^2 - x(yz) + y^2 + 1 = 0 \ \ldots.(*)$$

الـ $z$ نتخيله عدداً ثابتاً (مثل الـ 3 قبل قليل).

هنا معادلة تربيعية وكأن المجهول $x$ والثابت هو $y$

إذا كان $(x, y)$ حل عندها $(yz - x, y)$ حل أيضاً

الآن إذا كان $(x_1, y_1)$ الحل الأصغري (أنت تضع الشروط بطريقة ما ترضيك وترضي المسألة)

- $x$ أصغر ما يمكن
- $x, y > 0$

والآن الحل $(y_1 z - x_1, y_1)$

والآن بما أن $x_1$ , $x_2 = y_1 z - x_1$ هما جذرا المعادلة في الأعلى (حيث $y_1$ ثابتة) جداءهما يساوي الحد الثابت

$$x_1 x_2 = y_1^2 + 1 > 0$$

$\Leftarrow x_2$ موجب لا يمكن أن يكون سالب إذا حصراً يجب أن يكون $x_2 \geq x_1$ (لأن $x_1$ هو العدد الأصغري)

$$y_1^2 + 1 \geq x_1^2$$

هنا:

يمكننا أن نفرض دون المس بعمومية المسألة أن $x_1 \geq y_1$ وذلك بسبب التناظر أو لأننا يمكننا أن نناقش بالعكس أي أن نثبت $x_1$ ونغير $y_1$

نفرض هذه المتراجحة حسب ما نحتاجه عندما نصل إلى آخر متراجحة، ولكن في الحل يجب أن نضعها عند $(*)$ من أجل جودة الحل وكأننا نعرف مسبقاً

الآن $x_1 \geq y_1$ إذا $x_1 \neq y_1$ عندها $x_1 \geq y_1 + 1$

$$y_1^2 + 1 \geq (y_1 + 1)^2$$

تناقض.

إذاً $x_1 = y_1$ (أي في الحل الأصغري يجب أن تكون الإكسات تساوي الوايات)

نعوض لأننا لا ننسى ما هو الحل الأصغري بالأصل.

$$2x_1^2 + 1 = x_1^2 z$$
$$\Rightarrow x_1 = 1 \ , \qquad z = 3$$

هنا استنتجنا أنه لا حلول إلا عندما $z = 3$ (حتماً) وفي حالتها الحل الأصغري $(1,1)$ ولا يوجد حالة أخرى للحل الأصغري.

الآن لنوجد العدد الغير منتهي من الحلول العملية $(x, y) \xleftarrow{\text{نثبّت } y} (3y - x, y)$

$$\ldots\ldots (13, \underline{34}) \leftarrow (\underline{13}, 5) \leftarrow (2, \underline{5}) \leftarrow (\underline{2}, 1) \leftarrow (1, \underline{1})$$

نلاحظ أنه لا نثبت بنفس الجهة مرتين لأننا سنعود للحل السابق.

**ملاحظة:** وضعناً خطاً تحت العدد الذي تم تثبيته)، وفق عملياتنا نحن نصعد إلى الأعلى لو ثبتنا العدد الآخر سنهبط إلى الأسفل.

وهذه السلسلة ستحوي جميع الحلول، لأنه إذا خرج حل عن السلسلة السابقة ننزل به إلى حله الأصغري ولكن بما أنه لا يوجد إلا حل أصغري وحيد لذلك يجب أن ينتمي إلى السلسلة السابقة حصراً.

** إذا عدد سلاسل الحلول يساوي عدد الحلول الأصغري. □

**المسألة الثانية:**

$$x^2 + y^2 + x + y + 1 = xyz$$

درب نفسك على ذات الطريقة.

- ما نلاحظه هو أننا نفرض شروط للحل لأصغري بحيث يناقضها الحل الجديد وهذه الشروط دقيقة جداً.

  فمثلاً $x, y > 0 \quad x \geq y$ , $y$ أصغر ما يمكن

  هذا ما قمنا به في المسألتين الماضيتين واستطعنا فعل ذلك لأن $x$ يبقى ثابتاً.

ولكن في المسألة التالية سيتغير العددين في الحل الجديد وبالتالي سنلجأ لمعيار آخر مثل $x + y$ أصغر ما يمكن وهكذا

**مسألة 3:**

أوجد حلول المعادلة $x^2 - 5y^2 = -4$ حيث $x, y \in \mathbb{N}$

**الحل:** سنبدأ بخطوة مساعدة:

إذا كان $(x, y)$ حل عندها $\left(\frac{3x-5y}{2}, \frac{3y-x}{2}\right)$ حل أيضاً يجب أن تستنتج مثل هذه الصيغة لوحدك فيما بعد

ومثل هذه الخطوات قوية جداً لحل مثل هذه المسائل ذات العدد الغير منته من الحلول.

**تتمة الحل:** إذا فرضنا أن $(x_1, y_1)$ الحل الأصغري $x_1, y_1 > 0$ (1) بحيث $x_1 + y_1$ أصغر ما يمكن (2)

عندها $\left(\frac{3x_1-5y_1}{2}, \frac{3y_1-x_1}{2}\right)$ حل ولكن فقط يجب أن نثبت أنهما صحيحان.

بالفعل هما صحيحان لأن $x_1, y_1$ يحققان $x_1^2 - 5y_1^2 = -4$ وبالتالي لهما نفس الـ **parity**

الآن نناقش الحالات التالية

- العددين كلاهما موجب تحقق (1) عندها يجب أن يكون مجموعهما $x_1 - y_1$ أكبر من $x_1 + y_1$ حسب (2) وهذا تناقض واضح.
- والآن أحدهما إذاً يجب أن يكون سالباً.

$$\frac{3y_1 - x_1}{2} \leq 0 \Rightarrow x_1 \geq 3y_1$$

$$9y_1^2 - 5y_1^2 \leq x_1^2 - 5y_1^2 = -4$$

$$\Rightarrow y_1^2 \leq -1$$

تناقض

$$\frac{3x_1 - 5y_1}{2} \leq 0 \Rightarrow 3x_1 \leq 5y_1$$

$$5x_1^2 = 25y_1^2 - 20$$

$$\geq 9x_1^2 - 20$$
$$\Rightarrow 5 \geq x_1^2$$

إما $x_1 = 1 \Leftarrow y_1 = 1$ حصلنا أخيراً على حل أصغري.

أو $x_1 = 2$ نعوض في الأساسية تناقض.

إذاً يوجد حل أصغري وحيد مما سبق

$$(1, 1)$$

إذاً لدينا سلسلة واحدة من الحلول ننشأ هذه السلسلة بدءاً من $(1,1)$ والعلاقة المعاكسة لـ $(x, y) \rightarrow$ $\left(\frac{3x-5y}{2}, \frac{3y-x}{2}\right)$

لربما ما زال الشخص يشكك بوحدانية هذه السلاسل كحلول لذا يفيد التأكيد.

**إن أي حل للمعادلات السابقة يمكن النزول به حتى الحل الأصغري يعني أحد الحلول الأصغرية.**

وبالتالي عند إنشاء السلاسل بدءاً من جميع الحلول الأصغرية لابد من المرور عليه.

### المسألة الرابعة

$$(n^2 - mn - m^2)^2 = 1 \quad m, n \in \mathbb{N}$$

**الحل:**

من الواضح أن: $m \leq n$ $(*)$

وذلك لأن $-mn$ سالب إذاً $n^2 - m^2$ يجب أن يكون موجب حتى يصبح المجموع 1 أو $-1$ وبما أنّ $n, m$ موجبان عندها $m \leq n$

أول ما سيزعجنا في المسألة هو موضوع التناظر. إنها غير متناظرة ولكن ليس كثيراً إذا بدلنا $n$ مكان $m$ تصبح:

$$(m^2 - mn - n^2)^2 = (n^2 + mn - m^2)^2$$

إذا بدلنا $m$ بـ $-m$ في الجديدة نحصل على نفس المقدار $(n^2 - mn - m^2)^2$ وبالتالي على حل جديد.

الآن بالعودة إلى كونها معادلة تربيعية إذا كان $(n, m)$ حل عندها إذا ثبتنا $m$ يكون $(m - n, m)$

نطبق عليها ما سلف أي أن نبدل مكان $m$ و $n$ ونبدل إشارة "العملية" نجمة يكون:

$(m, n - m)$ حل إذاً $(n, m) \rightarrow (m, n - m)$

الآن نأخذ الحل الأصغري $n_1, m_1 > 0$ بحيث يكون **المجموع** أصغر ما يمكن (لاحظ الخباثة فأنا لاحظت أنّ المجموع سيكون أصغر في الحل الجديد ...ولاحظت لما قمنا ب)

- إذا كان $n - m > 0$ تناقض لأن المجموع أصغر من $m + n$
- إذاً $m = n \quad n = m = 1 \quad (1,1)$
- إذا كان $m > n$ تناقض واضح من $(*)$

لاحظ أنّ مثل علاقة * كنّا ممكن أن نستنتجها عندما نصل إلى هذه المرحلة - من خلال جداء الجذريين وهكذا - وليس في البداية ولكن استنتاجها من البداية نبّهنا على عدم وجود التناظر

الآن من $(1,1)$ والعلاقة العكسية ل $(n, m) \rightarrow (m, n - m)$ هي

$$(F_{n+1}, F_n) = (n, m)\ , (m + n, n) \leftarrow (n, m)\ , (5,3) \leftarrow (3,2) \leftarrow (2,1) \leftarrow (1,1)$$

الأمثلة السابقة كانت تقودنا إلى تناقض مباشر بعد متراجحة الأكبر من الحل الأصغري.

ماذا لو تعذبنا قليلاً لإيجاد التناقض

**المسألة الخامسة**: (الطريقة الأولى غريبة قليلاً)

أثبت أنه إذا كان $\frac{a^2+b^2}{ab+1} = k$ عندها $k$ مربع كامل حيث $a, b, k \in \mathbb{N}$.

**الحل:**

ليكن $(a_1, b_1)$ أصغر حل بحيث $b$ أصغر ما يمكن (يمين القوس)

$$a_1^2 + b_1^2 = k a_1 b_1 + k$$
$$a_1^2 - a_1(kb_1) + b_1^2 - k = 0$$

عندها $(kb_1 - a_1, b_1)$ **وأيضاً** $(\boldsymbol{b_1, kb_1 - a_1})$ **حل** وهذه سنستخدمها كعلاقة التحول من حل لآخر لاحظ الغريب فيها أنّ $b_1$ لا يتغير ولكن يبدل موقعه

إذا كان $kb_1 - a_1 < 0$ لنصل إلى التناقض هنا ننظر إلى جذور المعادلة بشكل عام

$$a^2 + b^2 = k\, ab + k$$

$ab > -1$ نستفيد من كون $a, b$ صحيحة $ab \geq 0$ إذاً $ab \geq 0$ أي أن الثنائية دائماً لهما نفس الإشارة وبالتالي في الثنائية $(kb_1 - a_1, b_1)$ هي حل للمعادلة السابقة، بالنهاية استنتجناه بأيدينا ولو عوضت اليسار في $a$ واليمين في $b$ لتحققت المساواة مية بالمية.. إذاً في الثنائية نصل لنقص الحالة.

قد يقترح البعض أن أفرض $b_1 \geq a_1$ لنقض الحالة في الأعلى ولكن انظر للأسفل استخدمت المترجحة المعاكسة لنقض حالة أصعب تتطلب هذا الفرض حصراً حتى تحل

إذا كان $ka_1 - b_1 = 0 \Leftarrow b_1^2 = k$ وبالتالي تحقق المطلوب

إذا كان $kb_1 - a_1 > 0$ إذاً يجب أن يكون $kb_1 - a_1 \geq b_1$

$$k \geq \frac{a_1 + b_1}{b_1}$$

**نفرض** $\boldsymbol{b_1 \leq a_1}$

لاحظ أننا فرضنا هذه المتراجحة عند احتياجنا لها ومع ذلك **أؤكد أنه في الحل الرسمي يفضل كتابتها من الأول**

$$\frac{a_1+b_1}{b_1} \le k = \frac{a_1^2+b_1^2}{a_1b_1+1} \le \frac{a_1^2+a_1b_1}{a_1b_1+1} < \frac{a_1^2+a_1b_1}{a_1b_1} = \frac{a_1+b_1}{b_1}$$

تناقض. **علماً أن هذه الطريقة لا داعي لها استخدام جداء الجذريين يفي بالغرض مباشرة جرب ذلك.**

**طريقة أخرى.**

نفرض $(a_1, b_1)$ الحل مع $a_1, b_1 > 0$ بحيث $a$ أصغر ما يمكن

$$a_1^2 + b_1^2 = ka_1b_1 + k$$
$$a_1^2 - a_1(kb_1) + b_1^2 - k = 0$$
$$(kb_1 - a_1, b_1)$$

حل أيضاً

- إذا كان $kb_1 - a_1 < 0$ لن نصل للتناقض عن طريق علاقة الجداء هذه المرة بل سنناقش الثنائية $(a, b)$ بشكل عام التي تحقق $\frac{a^2+b^2}{ab+1} = k$ بغض النظر عن شروط المسألة $(a, b > 0)$ لأنه عند إجراء "الانتقال إلى حل اخر" قد تتغير.

بما أن $k$ موجب (لأننا فرضنا وجود حل مع $a_1, b_1 > 0$ ) وكذلك $a^2 + b^2$ إذاً $ab + 1 > 0$ موجب من أجل أي $a, b$ هذه المرة.

$ab \ge 0 \Leftarrow$ إذاً عنصرين الثنائية لهما نفس الإشارة وبالتالي في الثنائية $(kb_1 - a_1, a_1)$

الطريقة السابقة ذكية جداً وفعالة "أن نناقش بشكل عام أي ثنائية حلول"

- إذا كان $kb_1 = a_1$ $\Leftarrow$ نعوض $k = b_1^2$ انتصرنا.

هنا يمكننا إيجاد السلسلة لكن لا يهمنا وهنا عدد غير منته إذ من أجل أي $k$ يوجد حل ليس فقط 3

- إذا كان $kb_1 - a_1 > 0$ عندها من الأصغرية:

$$kb_1 - a_1 \ge a_1$$

من جداء الجذور والاستفادة من متراجحة الأصغرية مباشرة:

$$a_1^2 \le b_1^2 - k$$

نفرض $b_1 \le a_1$

نصل للتناقض. ■

## المسألة السادسة:

أوجد $n$ بحيث يوجد حل للمعادلة التالية في الأعداد الموجبة الصحيحة

$$(x+y+z)^2 = nxyz$$

**الحل:**

لو نظرنا إليها نظرة عامة، نلاحظ أنها أو أن الـ $n$ يقضي على احتمالات حل عديدة الـ $mod$ والتحليل ومن ثم نرى أنه إذا وجد حل من أجل قيمة معينة لـ $n$ يوجد عدد غير منته.

- لذا سنناقش الحل الأصغري
- وماذا عن المتراجحات؟!! إنها تشبه نمط المعادلات التي تحل بالتراجح مثل:

$$xyz = xy + yz + zx$$

$$1 = \frac{1}{z} + \frac{1}{x} + \frac{1}{y}$$

نقسم على $xyz$

$$\frac{x}{yz} + \frac{z}{xy} + \frac{y}{xz} + \frac{2}{x} + \frac{2}{y} + \frac{2}{z} = n \quad \dots (*)$$

إذا كان $x \le y \le z$ نعوض تراجحياً كل ما يؤدي إلى اختصار جيد وأراعي الإشارة السليمة طبعاً

$$n \le \frac{1}{z} + \frac{z}{xy} + \frac{1}{x} + \frac{2}{x} + \frac{2}{y} + \frac{2}{z}$$

هناك شيء ناقص (بالطبع فمن أجل أي حل $(x,y,z)$ لا يوجد أي تناقض تراجحي).

نبحث عن متراجحة اعتماداً على فكرة الحل الأصغري لنتابع اخر متراجحة وصلناها

نفرض أن $x_1 \le y_1 \le z_1$ الحل الأصغري أي بحيث $z_1$ أصغر ما يمكن وطبعاً كل الأعداد موجبة.

إذا ثبتنا $x, y$ طبعاً نعمل على المعادلة الأصلية للحل وليس على المتراجحة ☐

نلاحظ أن جداء الجذرين $z_1 z_2 = (x_1 + y_1)^2$ من الموضح أن $z_2$ موجب

إذاً $z_2 \le z_1$

$$\Rightarrow z_1 \leq x_1 + y_1$$

نعوض في الحد الذي لم نستطع تغيره في الأعلى:

$$n \leq \frac{3}{y_1} + \frac{4}{x_1} + \frac{3}{z_1} \leq 10$$

نناقش الآن بضع حالات ونوجد $n$ ثم على أساس قيمتها نعتمد على الطرف الأيسر من المتراجحة في الأعلى بل وأيضاً يمكن إيجاد الحلول الأصغرية من العلاقة $(*)$ وبالتالي كل السلاسل.*