جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة بابل

كلية التربية للعلوم الصرفة

قسم الرياضيات

الاعداد الاولية

بحث تقدم به الطالبة

اسراء ثامر لفته

مقدم الى مجلس كلية التربية للعلوم الصرفة قسم الرياضيات كجزء من متطلبات ليل شهادة بكالوريوس في الرياضيات

بأشراف

أ .م .د . عقيل كتاب مزعل

2023هـ 1444هـ

﴿فَتَعَالَى اللَّهُ الْمَلِكُ الْحَقُّ ۗ وَلَا تَعْجَلْ بِالْقُرْآنِ مِن قَبْلِ

أَن يُقْضَىٰ إِلَيْكَ وَحْيُهُ ۖ وَقُل رَّبِّ زِدْنِي عِلْمًا﴾

صدق الله العلي العظيم

سورة طه: الآية 114

الإهـــــــــداء

إلى من كلله الله بالهيبة والوقار .. إلى من علمني العطاء بدون انتظار إلى من أحمل أسمه بكل افتخار ..... والدي العزيز

إلى ملاكي في الحياة .. إلى معنى الحب وإلى معنى الحنان والتفاني .. إلى بسمتي في الحياة وسر الوجود إلى من كان دعائها سر نجاحي وحنانها بلسم جراحي إلى أغلى الحبايب ...

أمي الحبيبة

إلى من هم اقرب ألي من روحي ... إلى من شاركوني حضن الأم وبهم استمد عزتي واصراري إخوتي وأخواتي

الى السراج التي اشعلت الدياجي الحالكة من عقلي الى النور الذي افاضني علماً استاذتي ومشرفة بحثي

الباحث

الشكر والتقدير

نتقدم بجزيل الشكر والتقدير الى الاستاذ المحترمين لما قدموه لنا في اربع سنوات والى كافه السادة اعضاء لجنة المناقشة في قسم الرياضيات ومشرف البحث

المحتويات

رقم الصفحة	العنوان
1	**الفصل الاول – تشفير الاعداد الأولية**
3	**المقدمة(1-1)**
5	**اهمية الاعداد الاولية (2-1)**
5	**اسهل طريقة لمعرفة العدد الاولى (3-1)**
	العنوان
8	**الفصل الثاني – النظرية الأساسية في الحساب للإعداد الأولية**
7	**المقدمة (2-1)**
8	**النظرية الاساسية في الحساب (2-2)**
18	**القاسم المشترك الاكبر والمضاعف المشترك الاصغر (2-3)**
33	**المصادر**

العدد الأولي والعدد الأول[1] هو عدد طبيعي أكبر قطعاً من 1، لا يقبل القسمة إلا على نفسه وعلى واحد فقط. يُدعى كل عدد طبيعي أكبر قطعاً من 1 وغير أولي عددا مؤلفا. على سبيل المثال، 5 هو عدد أولي لأنه لا يقبل القسمة إلا على 1 وعلى 5، بينما 6 هو عدد مؤلف لأنه قابل للقسمة على 1، وعلى 2 وعلى 3 وعلى 6.

تقيم المبرهنة الأساسية في الحسابيات الدور المركزي للأعداد الأولية في نظرية الأعداد: كل عدد صحيح طبيعي أكبر قطعا من 1 يساوي جُداء (ضَرب) مجموعة وحيدة ما من الأعداد الأولية (بغض النظر عن ترتيب هؤلاء الأعداد داخل هذهِ المجموعة). فإن هذهِ المبرهنة تستلزم إقصاء 1 من لائحة الأعداد الأولية.

لأجل تحديد هل العدد أولي أم لا؟ توجد طريقة سهلة ولكنها بطيئة، تسمى القسمة المتكررة، وتتمثل في قسمة هذا العدد على الأعداد المحصورة بين 2 والجذر التربيعي للعدد المعين. توجد خوارزميات أخرى أكثر فعالية من القسمة، تستعمل في تحديد أولية الأعداد الكبيرة، وخصوصا عندما يتعلق الأمر بأعداد ذات شكل

خاص كأعداد ميرسين الأولية

الخلاصة

يتناول هذا البحث دراسة بعض جوانب الاعداد الأولية والذي يتضمن فصلين:

الفصل الاول يتحدث عن التشفير للأعداد الاولية

_اهمية الاعداد الأولية _اسهل طريقة لمعرفة الاعداد الأولية

الفصل الثاني يتحدث عن النظرية الأساسية في الحساب للإعداد الأولية _ والقاسم المشترك الأكبر والمضاعف المشترك الأصغر

الفصل الاول

تشفير الاعداد الأولية

(1-1)مقدمة

لمده طويلة اعتبرت نظرية الاعداد بشكل عام ودراسه الاعداد الأولية بشكل خاص جزءا من الرياضيات البحته بدون أية تطبيقات بإستثناء الاهتمام الذي يوليه عالم الرياضيات الى هذه الدراسة على سبيل المثال العاملون في نظرية الاعداد من أمثال عالم الرياضيات البريطاني غودفري هارولد هاردي كانو يفتخرون بعملهم في مجال ليس لديه تطبيقات عسكرية. ولكن هاته النظرة تحطمت في سبعينات القرن العشرين .حين أعلن للعموم أن الاعداد الاوليه قد تستعمل قاعده لبناء خوارزميات التفشير باستخدام المفتاح المعلن .يستعمل الاعداد الاوليه ايضأ مولدات الاعداد شبه العشوائية

تشفير باستخدام المفتاح المعلن :

تستعمل الاعداد الاوليه في ميدان المعلومات وخاصه في علم التعميه .ومن أشهر
التطبيقات التي تستعمل الاعداد الاوليه خوارزمية أر إس إيه وتبادل مفتاح ديفي هيلمان.تعتمد خوارزمية أر فقط xyاذا كان جداؤهماy وx إس إيه أساسا على افتراض أن حساب جداء عددين صحيحين معلومين
(معروفا(مع افتراض أنها أوليين فيما بينها

،هي ارقام العد المشترك من 1 ألى ما لا نهايه بما ذلك الأرقام الأولية والأرقام N الاعداد الطبيعية:ورمزها#
الزوجيه وهي حصرأ اعداد موجبه

تشمل كافة الاعداد الصحيحة من غير الكسور سواء كانت هذه الاعداد سالبة او Z الاعداد الصحيه :ورمزها موجبة

،هي مجموعة الاعداد الطبيعية غير السالبة بدءأ من الصفر، اي من W 0الاعداد الصحية والكلية :ورمزها ، الى ما نهاية

تشمل الاعداد الصحية الموجبة والسالبة والإعداد الكسرية والإعداد العشرين، .R الاعداد الحقيقية:ورمزها لكن بدون ارقام خيالية

هي جميع الأعداد التي لا يمكن كتابتها او التعبير عنها بصورة كسور, ò الاعداد النسبية او المنطقية :ورمزها

هما عددان bg a حيث أن (a+bi) ،تعرف على أنها أي رقم يمكن كتابته بالصيغةCالاعداد المركبة:ورمزها، حقيقيان وهو الجذر التربيعي ل-1.

(1-2) أهمية الاعداد الأولية# [1]

لوهلة ما قد يبدو الآمر غير مهم، ولكن فعلآ مهم بطريقة مبالغ فيها، ويمكن تضمين ذلك في أهم شيء نستخدمه في حياتنا وهو الأجهزة الرقمية والكمبيوتر والاجهزة الذكية والهواتف وكل ماهو نحوها، فجميعها تعتمد على الخوارزميات التي تعتمد على لغة خاصة بها تستخدم الأعداد الأولية على نطاق واسع، ومن أهم ما تقدمه هذه الاعداد ايضأ هو حفاظها على الأمن السيبراني، وهذه امر بالغ الأهمية في عصرنا الحالي فكل القرصنة وسرقة المعلومات والحسابات البنكية والارضية والمعلومات الشخصية والابتزاز وغيرها الكثير

تحديد الأعداد الأولية باستخدام تحليل العدد الى عوامله

يعد تحليل العدد الى العوامل هو أفضل طريقة لإيجاد الاعداد الأولية وبشكل بسيط يتم ذلك باستخدام الخطوات المتبعة في التحليل المعروفة وهي التالي:

نبحث عن عوامل هذا العدد.

.نتحقق من عدد عوامل هذه الرقم.

..نقوم بالمقارنة ،فإذا كان عدد للعوامل أكثر من اثنين.

.فهذا العدد ليس عدد أولياً

تحديد الأعداد الأولية من خلال الأدوات#

هناك عدة طرق شائعة أخرى يمكن الاستعانة بها لتجديد الاعداد الأولية من خلال الأدوات، كاستخدام الإله الحاسبة لإجراء عملية القسمة بشكل أسرع، ومن الأدوات المستخدمة هي حسابات القلم والورقة بشكل بسيط أو استخدام شجرة العوامل، وهي طريقة أشبه ماتكون بتحليل العدد ألى عوامله الأولية، ولكن باستخدام ...عوامل الضرب المتكررة

(1_3) اسهل طريقة لمعرفة العدد الاولي [2]

بأسط طريقة ممكنة لإثبات ما إذا كان الرقم عدداً أوليا، يمكن تطبيق بعض الخواص التي ذكرناها سابقا على الأعداد الأولية كمثال، نحاول اولآ تقسيمه على العدد 2لمعرفة ما اذا كنا سنحصل على عدد طبيعي دونما كسور وفواصل عشرية أو ما شأبه .واذا تم ذلك ، فهو قطعاً ليس عدد أولي ، فإذا أردنا أن نقسم العدد 5على 2، سيعطينا ناتج 2°5 وهذه عدد غير طبيعي، وبالتالي هو عدد اولي، بينما قسمه العدد 6على2 هو 3، وهذه عدد طبيعي وبالتالي هو عدد غير اولي، ومن الأشكال البسيطة للتعريف الى الاعداد الأولية ذات المرتبتين أو أكثر، هو النظر الى أول مرتبة منه فإذا كان 0او 5فهو ليس عدد أولي

الفصل الثاني

النظرية الأساسية في الحساب للإعداد الاولية

(2-1) مقدمة

تنبثق أهمية الأعداد الأولية في نظرية الاعداد وفي الرياضيات عموما من المبرهنة الأساسية في الحسابيات، والتي تنص على أن كل عدد صحيح موجب أكبر من 1، يمكن أن يكتب على شكل جداء أي (ضرب) لعدد أولي واحد أو مجموعة من الأعداد الأولية. هذه المجموعة وحيدة إذا غُض النظر إلى ترتيب الأعداد الأولية التي تُكونها. ونتيجة لذلك، هو أنه يمكن اعتبار الأعداد الأولية الأساس التي بنيت عليه الأعداد الطبيعية. على سبيل المثال،

23244= 2 · 2 · 3 · 13 · 149 =22 · 3 · 13 · 149. حيث 22 يعني مربع 2 أو القوة الثانية ل 2.

أ، 3*7=21

كما في المثال السابق، قد يتكرر نفس العامل الأولي أكثر من مرة. تسمى عملية تحليل عدد n ما إلى جداء عومل أولية :$n = p1 \cdot p2 \cdot ... \cdot p$

تحليل عدد صحيح الى عوامل

The Fundamental Theorem of Arithmetic [4] (2-2)

النظرية الأساسية في الحساب

كل عدد صحيح $n > 1$ يمكن كتابته بشكل وحيد كحاصل ضرب لقوى أعداد أولية

$p_1, p_2, \ldots, p_k$، أي

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

إيجاد gcd, lcm باستخدام التحليل.

إذا حللنا العددين الصحيحين a،b لعواملهما الأولية $a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$، $b = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$ فإن $p_1^{\min(a_1, b_1)}$ أكبر قوة ممكنة للأولي p_1 تقسم كلا من $p_1^{a_1}, p_1^{b_1}$. كذلك الحال مع بقية العوامل الأولية ولذلك

$$(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots p_k^{\min(a_k, b_k)} \qquad (*)$$

من جهة أخرى $p_1^{\max(a_1, b_1)}$ هي أصغر قوة ممكنة للأولي p_1 ليكون مضاعف للعددين $p_1^{a_1}, p_1^{b_1}$ ولذلك

$$[a, b] = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \ldots p_k^{\max(a_k, b_k)} \qquad (**)$$

إذا كان $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ تحليل العدد n لعوامله الأولية وكان m قاسم موجب للعدد n فيجب أن تكون عوامله الأولية من بين العوامل $p_1, p_2, \ldots, p_k$. السؤال هو ما هي القوة الممكنة لعامل أولي مثل p_i؟ .يمكن أن تك ون قوته $0، 1، 2، \ldots، \alpha_i$ أي أن هناك $\alpha_i + 1$ اختيار وبالتالي إذا رمزنا كانت لعدد قواسم n الموجبة بالرمز $\tau(n)$ فإن

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1)$$

<u>أمثلة:</u>

(1)اختبر ما إذا كانت الأعداد التالية أولية أم لا: 9901، $2^{11}-1$، 577، 127.

(1S) العدد 127 أولي لأنه لا يقبل القسمة على أي من الأعداد الأولية التي اقل من أو يساوي 11 وكذلك العدد 577 أولي لأنه لا يقبل القسمة على أي من الأعداد الأولية التي اقل من أو يساوي 23، بينما العدد $2047 = 2^{11} - 1$ عدد مؤلف لأنه يقبل القسمة على 23 والعدد 9901 عدد أولي لأنه لا يقبل القسمة على أي من الأعداد الأولية التي اقل من أو يساوي 97.

(2)أوجد جميع العوامل الأولية للمقدار $2^{18} - 3^{18}$

(S2)

$$3^{18}-2^{18}=(3^{-9})^2-(2^9-(2^9)=(3^9-2^9)(3^9+2^9)$$
$$=-(3^3-2)(3^3++6^3\ 2)(3^6+2)(3^{3\,6}-)6^3\ +2^6)$$
$$=-(3\ 2)(3^2++6\quad 2)(3^{26}++6^32)(3^6+2)(3^2-+6\quad 2)(3^{2-6}-+6^3\quad 2^6)$$
$$=5\times 7\times 19\times 577\times 1009$$

العدد 577 اولى من المثال (1) ويمكن التحقق كم ان 1009 عدد اولى .

(3) أوجد جميع الأعداد الأولية p بحيث كل من $1+4p^2$ و $1+6p^2$ عدد أولي.

(3S) إذا كان آحاد العدد^p إما ^{1} أو ^{9} فـإن آحـاد p^2 أيضـا ^{1} وعليـه آحـاد ^{1} + $4p^2$ يسـاوي^5، أي أن $1+4p^2$ غير أولي في هذه الحالة.

إذا كـان آح ـاد الع ـدد^p إم ـا ^{3} أو ^{7} ف ـإن آح ـاد p^2ه ـو^9 وعلي ـه آح ـاد ^{1}+ $6p^2$ يس ـاوي ^{5}، أي أن $1+6p^2$ غير أولي في هذه الحالة. الآن يتبقى إما ^{2} = p أو^5 = p:

إذا كان 2 = p فإن 17 1=+ $4p^2$ أولي بينما 25 1=+ $6p^2$غير أولي. إذا كان 5 = p فإن 101 1=+ $4p^2$ أولي ^{151} 1=+ $6p^2$ أولي أيضا. إذاً يوجد عدد أولي وحيد هو ^{5} = p عنده كل من $1+4p^2$و$1+6p^2$ عدد أولي.

(4)أثبت أن أي عدد صحيح زوجي ^{8} < n يمكن كتابته على صورة جمع ثلاثة أعداد أولية نسبيا مثنى مثنى.

(4S) أي عدد صحيح زوجي يكون على الصورة $n = 6^k$ أو ^{2} + n = 6k أو ^{4} + n = 6k حيث $k \in Z$.

إذا كان $n = 6k$، $(k \geq 2)$فان $n = 2 + 3 + (6k - 5)$.

إذا كان $n = 6k + 2$، $(k \geq 2)$فان $n = 3 + 4 + (6k - 5)$.

إذا كان $n = 6k + 4$، $(k \geq 1)$فان $n = 2 + 3 + (6k - 1)$.

(6) أثبت أنه يوجد عدد غير منتهي من الأعداد الأولية التي على الصورة ^{3} +k 4.

(6S)الحل يعتمد على فكرة أن حاصل ضرب عددين على الصورة^1+k 4 يكون على نفس الصورة.

لنفرض أن هناك عدد منتهي $p_1\ p_2, ..., p_t$ من الأعداد الأولية التي على الصورة ^{3} +k 4. خذ العدد

$$N = 4p_1 p_2 \ldots p_t - 1 = 4(p_1 p_2 \ldots p_t - 1) + 3$$

العدد N لا يقبل القسمة على أي من p_i حيث $t\geq i \geq 1$. ولكن كل عدد صحيح موجب أكبر من 1 له قاسم أولي.أيضا العدد N فردي لذلك كل عوامله الأولية فردية وحيث أنه على الشكل 3 +m 4 فيجب أن يكون أحد عوامله الأولية على الصورة 3 +m 4 .إذا هناك قاسم أولي للعدد N ليس من ضمن $p_1\ p_2, ..., p_t$ وهذا تناقض.إذا هناك عدد لا □ائي من الأعداد الأولية على الصورة 3 +4k.

(7)برهن على أن $1og\,2$ عدد غير نسبي

(S7) بفرض العكس، أي أن $1og\,2$ عددا نسبيا وليكن $10g2 = \frac{m}{n}$ بحث $(m.n) = 1$

$$\log 2 = \frac{m}{n} \Rightarrow 10^{mn} = 2 \Rightarrow 10^{m} = 2^{n} \Rightarrow \times 2^{m} \qquad 5^{m} = 2^{n}$$

وهذا يناقض النظرية الأساسية في الحساب (الوحدانية)، إذن عكس الفرض هو الصحيح.

(8)إذا كان أحد العددين $2^n - 1$ أو $2^n + 1$ أولي فان الآخر يكون غير أولي، حيث $n \leq 3$

(S8)

الحل

العدد2^n لا يقبل القسمة على3 . إذا كان باقي قسمة 2^n على 3 يساوي 1 فان $2^n - 1$يقبل القسمة على 3 وإذا كان باقي قسمة 2^nعلى 3 يساوي 2 فان $2^n + 1$يقبل القسمة على 3وعليه أحد العددين $2^n - 1$ أو $2^n + 1$يقبل القسمة على 3، فإذا كان كل من العددين أكبر من 3 فانه لا يمكن أن يكون العددين أوليين.

تمارين

(A)إذا كان $2^n - 1$ عدد أولي فان n عدد أولي.

(B)إذا كان p العدد27000001 له أربعة عوامل أولية فأوجد مجموعهم.

(C)هل $2009^4 + 4^{2009}$ عدد أولي؟

(D) أوجد جميع الحلول الصحيحة الموجبة للمعادلة$2^{2} = 175 - 3^{2n}\,2^{m}$.

(E)إذا كان p عدد أولي أكبر من3 فإن العدد$p^2 + 2$ مؤلف و $24 \mid p^2 - 1$.

(F) أوجد جميع الأعداد الأولية p q، التي تجعل $p^2 + pq + q^2$ مربع كامل

(G) إذا كان للمعادلة $\pi^2 - 2p\pi + p^2 - 1 = 0$ جذرين صحيحين ، حيث p عدد أولي.

أوجد القيم الممكنة للعدد p.

(H) حلل العدد1001001001 إلى عوامله الأولية.

(I) أوجد جميع الأعداد الأولية p بحيث العدد$p^2 + 11$ له 6قواسم مختلفة من بينها العدد 1 والعدد نفسه.

(J) إذا كان p q، أوليان وكان $\frac{p2+q2}{p+q}$ عدد صحيح فأثبت أن r أولي .

التطابقات قياس n Congruencies modulo n

ليكن n عدد صحيح موجب. نقول أن العدد a يطابق العدد b قياس n ونرمز لذلك بالرمز

$a \equiv_n b$ أو$a \equiv b \pmod n$ إذا كان $n \mid (a - b)$ و إذا كان $n \nmid (a - b)$

فإننا نقول أن a لا يطابقb قياس n ونرمز لذلك بالرمز $a \not\equiv b \pmod n$. وبكتابة مكافئه فان

$$a \equiv b \pmod n \Leftrightarrow \exists\, k \in Z : a = b + kn$$

لاحظ أن أي عدد صحيح a يطابق باقي قسمته على n قياس العدد n وذلك لان حسب خوارزمية القسمة $a = qn + r, \quad 0 \leq r < n$ وعليه فان $a \equiv r \pmod n$.

خواص أساسية للتطابقات

لتكن $a\ b\ c\ d,\ ,\ ,\ \in Z$ و $n \in Z^+$ أعداد صحيحة

(1) $a \equiv a \pmod n$ (خاصية الانعكاس)

(2) $a \equiv b \pmod n \Leftarrow b \equiv a \pmod n$ (خاصية التناظر)

(3) $a \equiv b \pmod n$ و $b \equiv c \pmod n \Leftarrow a \equiv c \pmod n$ (خاصية التعدي)

(4) $a \equiv b \pmod m$. فان $m|n$ وكان $a \equiv b \pmod n$

(5) إذا كان فإن $a \equiv b \pmod n$ و $c \equiv d \pmod n$

$a\ c \pm \equiv b\ d \pm \pmod n$ (قانون جمع(طرح) التطابقات)

$ac \equiv bd \pmod n$ (قانون ضرب التطابقات)

(6) بشكل أعم إذا كان $a_i \equiv b_i \pmod n$ لكل $i = 1,2,\ldots,k$ فإن

$$a_1 + + + \equiv + + + a_2 \ldots\ldots a_k \equiv b_1 b_2 \ldots\ldots b_k \pmod n.$$

$$a_2\ a_1 \ldots\ldots_2\ a_k \equiv b_1 b_2\ b_k \pmod n.$$

وكحالة خاصة ، إذا كان $a \equiv b \pmod n$ فإن $a^k \equiv b^k \pmod n$ لكل $k \in Z^+$

(7) $ac \equiv bc \pmod n \Leftrightarrow a \equiv b \pmod{\frac{n}{d}}$، حيث $d = (n\ c,\ )$

(8) إذا كان $a \equiv b \pmod{n_i}$ حيث $i = 1,2,\ldots,m$ فإن $a \equiv b \pmod{[n_1\ n_2,\ldots\ldots,n_m]}$

وكحالة خاصة، إذا كانت $n\ n_1, {}_2,\cdots,n_m$ أعداد أولية نسبيا مثنى مثنى فإن $a \equiv b \pmod{n_1\ n_2 \ldots n_m}$.

(9) إذا كان m عدد صحيح موجب فإن $(an + b)^m \equiv b^m \pmod n$.

مجموع المربعين

متى يكتب العدد الصحيح الموجب على صورة مجموع مربعين لعددين صحيحين ؟، فالعدد 3 لا يمكن كتابته على صورة مجموع مربعين وبصفة عامة أي عدد صحيح موجب n بحيث $4n \equiv 3(\mathrm{mod})$ لا يمكن كتابته على صورة مجموع مربعين. العدد 5 يمكن كتابته على صورة مجموع مربعين على الصورة $5 = 1^2 + 2^2$.

نعرض بعض الخواص المتعلقة بكتابة العدد كمجموع مربعين

(1) إذا كان كل من m و n مجموع مربعين فإن mn كذلك

(2) العدد الأولي p يمكن كتابته كمجموع مربعين بطريقة وحيدة إذا وفقط إذا كان $p = 2$ أو

$p \equiv 1(\mathrm{mod}(4)$

(3) العدد الصحيح الموجب n يكون مجموع لمربعين إذا وفقط إذا كان أي قاسم أولي p للعدد n بحيث $4p \equiv 3(\mathrm{mod})$ يظهر بقوة زوجية في تحليل العدد n إلى عوامله الأولية.

سنبرهن الخاصية (1) :

بفرض $m = +a^2$ وb^2 و $n = +c^2$. عندئذ

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

ملاحظات

يمكن تعميم الخاصية (1) كما يلي: إذا كان كل من $n_1, n_2,..,nk$ ..... مجموع مربعين فإن $n_1,n_2....nk$ كذلك لكل $1 \leq k$. الخاصية (2) تزودنا باختبار لأولية العدد n ، عندما يكون$n \equiv 1(mod4)$، فمثلا العدد $n = 221$ يطابق 1 قياس 4 وعليه إذا كان أوليا فإنه n يمكن كتابته بطريقة وحيدة كمجموع مربعين . ولكن $n = 10^2 + 11^2 = 5^2 + 14^2$ وبالتالي فإن n عدد مؤلف

أمثلة:

(1) أثبت أن$13^{682} \equiv mod1\ 7$

(S1) باستخدام خاصية (9): $(an+b)^m \equiv b^m\ modn$

$$13^{682} = (2\times7 - 1)^{682} \equiv (-1)^{682} \equiv 1\ mod7$$

(2) اثبت أن $6^{n-1} + 6^{n-2} + \cdots + 6^1 + -1 - 6$ تقبل القسمة على 5 لأي عدد صحيح موجب n.

(2S)بما أن $6 \equiv 1(mod5)$ فإن $6^m \equiv 1^m = 1(mod5)$ حيث m صحيح موجب، إذا

$$6^{n-1} + 6^{n-2} + \cdots + 6^1 + -1n \equiv (1+1+\cdots+1+1) - n$$
$$\equiv n - n \equiv 0\ (mod5).$$

(3) أثبت أن $3^{4n} + 2 + 5^{2n+2} + 5^{2n} + 1$ يقبل القسمة على 14 حيث $0 \leq n$.

(S3)لهذه المسألة عدة طرق منها الاستقراء الرياضي، لكن باستخدام التطابق نصل للجواب سريعا. لاحظ أن

$$3^{4n+2} + 5^{2n+1} = 9(81)^n + 5(25)^n$$

ولكن $25 \equiv -3\ (mod14)$, $81 \equiv -3\ (mod14)$ إذا

$$(81)^n \equiv -(3)^n (mod14), (25)^n \equiv (-3)^n (mod14)$$

وبالتالي

$$3^{4n+2} + 5^{2n+1} \equiv 9(-3)^n + 5(-3)^n \equiv 14(-3)^n \equiv 0\ (mod14)$$

(4) أثبت أن في المتتابعة $a_n = 2^n - 3$ حيث $0 \leq n$ عدد لا نهائي من الحدود قابلة للقسمة على5 وكذلك عدد لا نهائي من الحدود قابلة للقسمة على 13 ولكن ليس فيها أي حد يقبل القسمة على5 و 13.

(S4) بما أن $2^3 \equiv 3(mod\ 5)$ وبما أن $2^4 \equiv 3(mod5)$ فإن

$$2^{4k+3} - 3 \equiv (2^4)^k \cdot 2^3 - 3 \equiv 1.3 - 3 \equiv 0(mod5).$$

بما أن $2^r \equiv 3(mod5)$ متحققة فقط عندما $r = 3$ من بين الأعداد 0،1،2،3،4 وعليه فان $5|a_n$ فقط عندما $n = 4k + 3$.

بالمثل $2^4 \equiv 3 \pmod{13}$ و $3 \equiv 1 \bmod 13 \equiv {(2^4)}^3$ ولذلك

$2^{12m} + 4 - 3 \equiv (2^{12})^m .\ 2^4 - 3 \equiv 1.3-3 \equiv 0 \pmod{13}$.

وحيث $2^r \equiv 3 \pmod{13}$ إذا وإذا فقط $r = 4$ لكل $0 \leq r < 13$ فإن $13 | an$ فقط عندما $n = 12m + 4$. بما أنه لا يوجد عدد صحيح له الصورة $n = 12m + 4$ والصورة $3n = +4k$ فإنه لا يوجد حد من المتتابعة يقبل القسمة على 5 و 13.

(5) ليكن $x\ y, \in Z$. $3 | x2 + y2 \Leftrightarrow 3 | x, 3 | y$

(S 5) إذا كـان $3|x ,3|y$ فـإن وضـوحا $3 | 2x^2 + y$. نلاحظ أن $3x2 \equiv 0$ or $1 \pmod{}$ وعليـه إذا كـان $| x2 + y$ فان $3|y$, $3 | 2x2$ وعليه $3 | x, 3 | y$.

ملاحظة

التمرين السابق لا يتحقق لأي عدد أولي فمثلا $5^2 + 2^2 | 1$ بينما 1 5و2 5. هل يتحقق التمرين السابق للعدد الأولي $p = 7$؟ .

(6)أثبت أنه إذا كان $a \equiv b \pmod n$ فإن $a^n \equiv b^n \pmod{n^2}$.هل العكس صحيح؟

(S6)بما أن $a \equiv b \pmod n$ ، إذن $a = b + qn$ لعدد صحيح q . الآن من نظرية ذات الحدين

$$a^n - b^n = (b+bn)^n - b^n$$

$$\begin{aligned} a^n - b^n &= (b+qn)^n - b^n \\ &= \binom{n}{1} b^{n-1} qn + \binom{n}{2} b^{n-2} q^2 n^2 + \cdots + \binom{n}{n} q^n n^n \\ &= n^2 \left(b^{n-1} q + \binom{n}{2} b^{n-2} q^2 + \cdots + \binom{n}{n} q^n n^{n-2} \right) \end{aligned}$$

وعليه $a^n \equiv b^n \pmod{n^2}$. العكس غير صحيح، فمثلا $34 \equiv 1^2 \pmod{4^2}$ بينما $3 \not\equiv 1 \pmod 4$.

حل آخر

لدينا $\alpha^n - bn = (\alpha\ b\ \alpha^n - 1 + \alpha^n -^2 b + + \cdots + \alpha^{bn-2} + b^{n-1})$ وحيث أن

$a^{n-1-i}\, b^i \equiv \alpha^{n-1-i}\, \alpha^i \equiv \alpha^{n-1} \pmod n$

$(\alpha^{n-1-i} b^{-i} + \alpha^{n-1-i-} \alpha^i \equiv \alpha^{n-1} \equiv 0 \pmod n$،

اي ان, $(\alpha^{n-1} + \alpha^n -^2 b \ldots\ldots + \alpha b^{n-2} + b^{n-1}) \equiv n\alpha^{n-1} \equiv 0 \pmod n$

(7)أكتب العدد 2009 كمجموع مربعين

(S 7)بتحليل العدد 2009 إلى عوامله الأولية نجد أن $2009 = 7^2 \times 41$، إذن يمكن كتابته على صورة مجموع مربعين $2009 = 7^2 \times 41 = 7^2 (4^2 + 5^2) = 28^2 + 35^2$.

نختم هذا الجزء بنظرية برهانها يعتمد على مواضيع سوف نتطرق إليها في الجزء الثاني من هذا العمل إنشاء الله وذلك لاستخدامها في إثبات أنه يوجد عدد غير منتهي من الأعداد الأولية التي على الصورة $4k + 1$.

نظرية

ليكن p عدداً أوليا. عندئذ يوجد حل للتطابق $x^2 \equiv -1 (\bmod p)$ إذا وفقط إذا كان

$p \equiv 1(\bmod 4)$. وعلاوة على ذلك إذا كان $p \equiv 1(\bmod 4)$ فإن ! $\pi = \left(\frac{p-1}{2}\right)$ حلاً للتطابق.

تمارين

(A)أوجد آخر رقمين(خانتي الآحاد والعشرات) من العدد 7^{2010} .

(B) أثبت أن $2222^{5555} + 5555^{2222}$ يقبل القسمة على 7.

(C)أوجد آخر رقمين من العدد$37^{10}+229^{10}$.

(D) أوجد آخر رقمين من العدد 2^{999}.

(E) إذا كان p عدداً أولياً و k عدد صحيح بحيث k عدد صحيح بحيث $1 \le k < p$ فأثبت أن $p \left| \binom{p}{k} \right.$ ، ثم استنتج أنه إذا كان

b،a عددين صحيحين فإن $(\alpha + b)^p \equiv a^p + b^p (\bmod p)$.

(F)حل المعادلة التالية في الأعداد الصحيحة $x^2 + y 2 = 3^{2008}$

(G) **عين الأعداد الصحيحة الموجبة m بحيث يكون $m!+ 5$ مكعب كامل.**

(H) **أثبت أنه يوجد عدد غير منتهي من الأعداد الأولية التي على الصورة $4 k+1$.**

(I)أثبت أن $2^{11 \times 31} \equiv 11(\bmod 2\times 31)$.

(J) أوجد المربعات الكاملة في المتتابعة

أوجد()K 1!، 1!+2!، 1!+ +2! 3!،1!+ + +2! 3!4!، …، 1!+ + + +2! 3! ⋯ …n!،.......،

باقي قسمة . $17 + 177 + 1777 + \cdots + 1\underbrace{77\cdots7}_{20}$ على 7

الحلول

قابلية القسمة

(A) **إذا كان x y، عددين صحيحين فاثبت أن** **$17 \mid 2x + 3y \Leftrightarrow 17 \mid 9x + 5y$.**

الحل

" ⇒ "

$$17 \mid 2x + 3y \Rightarrow 17 \mid 13(2x + 3y) = (17x + 34y) + (9x + 5y)$$
$$\Rightarrow 17 \mid 9x + 5y$$

" ⇐ "

$$17 \mid 9x + 5y \Rightarrow 17 \mid 4(9x + 5y) = (34x + 17y) + (2x + 3y)$$

$$\Rightarrow 17 \mid 2x + 3y$$

(B) اثبت أن $n^3 +(n+1)^3 +(n+2)^3$ يقبل القسمة على 9.

الحل

ضع $S = n3 +(n +1)3 +(n + 2)3$.

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

$= n^3 +(n^3 + 3n^2 + 3n +1)+(n^3 + 6n^2 +12n + 8)$

$= 3n^3 + 9n^2 +15n + 9 = 3n3 +15n + 9(n2 +1)$

$= 3n^3 - 3n +18n + 9(n2 +)1$

$= (3n\ n^2 -1)+ 9(n^2 + 2n +)1$

واضح أن كل من حدي المعادلة الأخيرة يقبل القسمة على9 ، الحد الأول يتكون من العدد3 مضروبا في ثلاثة أعداد صحيحة متتالية والثاني وضوحا يقبل القسمة على 9 .

(C) ليكن nعدد صحيح موجب، لماذا $n5 - n$ يقبل القسمة على 5 دائما؟

الحل

ضع $S = n^5\text{-}n$

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

أي عدد صحيح موجب n يكون على الصورة $4n = +5k\ i, 0 \le i \le$ حيث $k \in Z$.

إذا كان n يس3اوي k5 أو $k\ 5+ 1$ أو $n = +5k$ فان $S|5$. أما إذا كان $n = +5k+2$ او $n = 5k+3$ فان $S|5$ وذلك لان $n^2 + 1 | 5$. أكثر من ذلك يمكن إثبات أن $S|30$ وإذا كان n عدد فردي فان $S|240$.

(D)أوجد جميع الأزواج الصحيحة الموجبة $(m\ n،)$ التي تحقق المعادلة $m^2 - n! =780$.

الحل

إذا كان هناك حل فان $n \le 5$ لأنه إذا كان $5\ \ n > $ فان $3 + n!\ 780$ و$3|780$ $m\ n!2=+ 780|9$ وبالتعويض بـ $n = 1،2،3،4،5$ نجد أن $n = 5$ و $m = 30$ هو الحل الوحيد.

(E)إذا كان $a\ b, \in Z$ فأثبت أن $4\ |\alpha^2 - b^2$ إذا وإذا فقط كان α, b كلاهما زوجيان أو فرديان.

الحل

افرض أن احدهما وليكن α فردي و b زوجي عندئذ $(\alpha+ b)(\alpha - b)$ $\alpha^2 - b^2$ عبارة عن حاصل ضرب فرديين وبالتالي $4 \nmid \alpha^2 - b^2$. الآن افرض أن كلاهما فرديان أو كلاهما زوجيان إذا $\alpha + -b, \alpha\text{-}\ b$ زوجيان وبالتالي $\alpha^2 - b^2= (\alpha +b)(\alpha - b)$ يقبل القسمة على 4.

(F) هل توجد كثيرة حدود $p(x)$ معاملاتها أعداد صحيحة بحيث $p(1) = 2$ و $p(3) = 5$ ؟

الحل

بفرض توجد كثيرة حدود $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ حيث $a_i \in \mathbb{Z}, \quad i = 0,1,\cdots,n$ و $p(1) = 2, \quad p(3) = 5$.

$$p(1) = 2 \Rightarrow a_n + a_{n-1} + \ldots + a_1 + a_0 = 2$$

$$p(3) = 5 \Rightarrow 3^n a_n + 3^{n-1} a_{n-1} + \ldots + 3a_1 + a_0 = 5$$

بالطرح، نحصل على

$(3^n - 1)a_n + (3^{n-1} - 1)a_{n-1} + \ldots + (3 - 1)a_{10} = 3$ ، تناقض، 2 تقسم الطرف الأيسر لان: $2 \mid 3^i - 1$ لكل $i = 1,2,\cdots,n$ بينما 2 لا قسم 3 (الطرف الأيمن). إذاً لا توجد مثل هذه كثيرة الحدود.

لاحظ أن $a - b \mid p(a) - p(b)$ لكل $a, b \in \mathbb{Z}$ و $a \neq b$.

(G) أثبت أنه لكل $n > 11$ فان العدد $n^2 - 19n + 89$ ليس مربعا

الحل

سوف نثبت أن العدد $n^2 - 19n + 89$ يقع بين عددين مربعين متتاليين لكل $n > 11$.

$$n^2 - 19n + 89 = n^2 - 18n + 81 - (n - 8) = (n - 9)^2 - (\underbrace{n - 8}_{>0}) < (n - 9)^2$$

$$n^2 - 19n + 89 = n^2 - 20n + 100 + n - 11 = (n - 10)^2 + \underbrace{n - 11}_{>0} > (n - 10)^2$$

أي أن $(n - 10)^2 < n^2 - 19n + 89 < (n - 9)^2$.

(H) إذا كان nمكعب كامل فأثبت أن $n2 + 3n + 3$ ليس مكعب كامل.

الحل

بفـرض العكس أن $n^2 + 3n + 3$ عدد مكع ـب كام ـل وحي ـث أن n مكعب كامـل إذاً ،

$n(n^2 + 3n + 3)$ مكعب كامل، ولكن $n(n^2 + 3n + 3) = n^3 + 3n^2 + +1)^3 -1$

وهذا تعارض لان $(n + 1)^3 -1$ لا يمكن أن يكون عدد مكعب كامل.

(I) ليكن $a\ b\ c, , \in Z$، أثبت أن $6|a3 + b3 + c3 \Leftrightarrow 6|a + b + c$.

الحل

لاحظ أن $a^3 + b^3 + c^3 - (a + b + c) = 6k$ حيث $k \in Z$. وينتج المطلوب مباشرة.

(J)أثبت أن العدد $\underbrace{11\cdots1}_{2011}\underbrace{55\cdots5}_{2010}6$ عدد مربع

الحل

ليكن $N = \underbrace{11\cdots1}_{2010}\underbrace{55\cdots5}_{2009}6$

$$N = \underbrace{11\cdots1}_{2011}\times10^{2011} + \underbrace{55\cdots5}_{2010}\times10 + 6$$

$$= \frac{1}{9}(10^{2011}-1)\times10^{2011} + \frac{5}{9}(10^{2010}-1)\times10+6$$

$$= \frac{1}{9}[(10^{4022}-10^{2011}+5\times10^{2011}+4]$$

$$= \frac{1}{9}[(10^{4022}+4\times10^{2011}+4]$$

$$= (\frac{10^{2011}+2}{3})^2 = (\frac{1\underbrace{00\cdots0}_{2010}2}{3})^2 = (\underbrace{33\cdots3}_{2010}2)^2$$

(2-3) [5] القاسم المشترك الأكبر والمضاعف المشترك الأصغر

(A) ليكن $m, n \in \mathbb{Z}$. أوجد $\gcd(2^n, 2m+1)$ ، $\gcd(6, 2m+1)$ ،
$\gcd(2n+2, 2n+6)$ ، $\gcd(2^n-1, 2^n+1)$

الحل

$\gcd(2^n, 2m+1) = 1$ و $\gcd(6, 2m+1) | 3$ و

$$\gcd(2n+2, 2n+6) = \gcd(2n+2, 2n+6-2n-2) = \gcd(2n+2, 4) = 2 \ or \ 4$$

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

(B) أثبت أن الكسر $\dfrac{21n+4}{14n+3}$ في أبسط صورة لكل $n \in \mathbb{Z}^+$ $(IMO\ 1959)$.

الحل

المطلوب إثبات أن $\gcd(21n+4, 14n+3) = 1$.

بما أن $(21n+4)(-2) + (14n+3) \times 3 = 1$ إذا $\gcd(21n+4, 14n+3) = 1$.

(B) أثبت أن الكسر $\dfrac{21n+4}{14n+3}$ في أبسط صورة لكل $n \in \mathbb{Z}^+$ $(IMO\ 1959)$.

الحل

المطلوب إثبات أن $\gcd(21n+4, 14n+3) = 1$.

بما أن $(21n+4)(-2) + (14n+3) \times 3 = 1$ إذا $\gcd(21n+4, 14n+3) = 1$.

(C) إذا كان $\gcd(a, b) = 1$ فاثبت أن $\gcd(a+b, a^2-ab+b^2) | 3$.

الحل

بفرض $d = \gcd(a+b, a^2-ab+b^2)$ ،

$$d \,\Big|\, (a+b)^2 - a^2 + ab - b^2 = 3ab$$

أيضا $d \,\Big|\, 3b(a+b)$ ومنها $d \,\Big|\, 3b^2$ وبالمثل $d \,\Big|\, 3a^2$ وعليه

$$d \,\Big|\, (3a^2, 3b^2) = 3(a^2, b^2) = 3(a, b)^2 = 3 .$$

(D) أثبت أن $\gcd(5a+3b, 13a+8b) = \gcd(a,b)$.

الحل

بفرض $d_1 = \gcd(a,b)$ و $d_2 = \gcd(5a+3b, 13a+8b)$.

بما أن

$$d_1 \mid a, \quad d_1 \mid b \Rightarrow d_1 \mid 5a+3b, \quad d_1 \mid 13a+8b \Rightarrow d_1 \mid d_2 \cdots (1)$$

أيضا

$$d_2 \mid 5a+3b, \quad d_2 \mid 13a+8b \Rightarrow d_2 \mid 8(5a+3b) - 3(13a+8b) = a,$$
$$d_2 \mid (-13)(5a+3b) + 5(13a+8b) = b$$
$$\Rightarrow d_2 \mid d_1 \cdots (2)$$

من (1) و (2) ينتج المطلوب.

(E) إذا كان $A = 2n + 3m + 13, \quad B = 3n + 5m + 1, \quad C = 6n + 8n - 1$ فاثبت أن $\gcd(A,B,C) | 77$.

الحل

ليكن $d = \gcd(A,B,C)$. إذا d كان هو القاسم المشترك الأكبر للأعداد A, B, C فإن d يقسم كل من

$$E = 3A - C = m + 40,$$
$$F = 2B - C = 2m + 3$$

وأيضا يقسم $G = 2E - F = 77$ ومن ثم d يجب أن يكون قاسما لـ 77.

(F)احسب $\gcd(n!+1,(n+1)!+1)$ حيث n عدد صحيح موجب.

الحل

$$\begin{aligned}\gcd(n!+1,(n+1)!+1) &= \gcd(n!+1,(n+1)!+1-(n+1)(n+1))\\ &= \gcd(n!+1,n) = 1\end{aligned}$$

(G)ليكن n عدد صحيح أكبر من 2 ، أثبت انه يوجد ضمن الكسور $\frac{1}{n},\frac{2}{n},\cdots,\frac{n-1}{n}$ عدد زوجي من الكسور غير القابلة للتحليل.

الحل

الفكرة في أن الكسر $\frac{k}{n}$ غير قابل للتحليل إذا وفقط إذا كان الكسر $\frac{n-k}{n}$ غير قابل للتحليل، وذلك لان $\gcd(k,n)=\gcd(n-k,n)$. إذا كان الكسرين $\frac{k}{n}$ و $\frac{n-k}{n}$ مختلفين لكل k فإن مجموع الكسور غير القابلة للتحليل زوجي.إذا كان $\frac{k}{n}=\frac{n-k}{n}$ لـ $k\in\mathbb{Z}^+$ فان $n=2k$ وعليه $\frac{k}{n}=\frac{k}{2k}=\frac{1}{2}$ كسر قابل للتحليل وتؤول هذه إلى الحالة الأولى.

(H)حاصل ضرب أربعة أعداد صحيحة موجبة متتالية لا يمكن أي يكون قوي لعدد صحيح موجب.

الحل

بفرض $n(n+1)(n+2)(n+3)=m^k$ حيث $n,m,k\in\mathbb{Z}^+$ و $k>1$

$$n(n+1)(n+2)(n+3)=(n^2+3n)(n^2+3n+2)=m^k$$

بمـــا أن $\gcd(n^2+3n,n^2+3n+2)=2$ ، إذن $\gcd(\frac{n^2+3n}{2},\frac{n^2+3n+2}{2})=1$

وعليه $\frac{n^2+3n}{2}=a^k$ و $\frac{n^2+3n+2}{2}=b^k$ ومنها $b^k-a^k=1$ ولا يوجد عددين موجبين الفرق بين قواهما يساوي 1.

ملاحظة إذا أضفنا لهذا الضرب العدد 1 فان العدد يصبح مربع كامل.

$$\begin{aligned}n(n+1)(n+2)(n+3)+1&=(n^2+3n)(n^2+3n+2)+1\\&=(n^2+3n)^2+2(n^2+3n)+1\\&=((n^2+3n)+1)^2\end{aligned}$$

(I) أوجد القاسم المشترك الأكبر للأعداد

$.2^{2^2}+2^{2^1}+1,\ 2^{2^3}+2^{2^2}+1,\dots,2^{2^{n+1}}+2^{2^n}+1,\dots$

نفرض أن yx هو رقم الهاتف حيث x رقم مكون من أربع خانات و y رقم مكون من ثلاث خانات. من المعطيات $2(y\times 10000+x)+1=x\times 1000+y$ ومنها نجد أن $998x-19999y=1$. الآن، نبحث عن القاسم المشترك الأكبر للعددين 998 و 19999:

$$19999=20\times 998+39$$

$$998\quad=25\times 39+23$$

$$39\quad=1\times 23+16$$

$$23\quad=1\times 16+7$$

$$16\quad=2\times 7+2$$

$$7\quad=3\times 2+1$$

$$2\quad=2\times 1+0$$

وعليه $\gcd(998,19999)=1$ ، نستخدم خوارزمية إقليدس لإيجاد x,y ، بإجراء عملية عكسية لما تم أعلاه نجد أن $998\times 8717-19999\times 435=1$ وعليه يكون $x=8717,\quad y=435$ ويكون رقم الهاتف هو $435-8717$.ملاحظة هذا الرقم وحيد: لان جميع الحلول x,y تعطى من نتيجة 3 وتكون على الصورة

$$x=8717-19999k$$

$$y=435-998k$$

حيث $k\in\mathbb{Z}$ ويكون كل من x,y موجبين إذا كان $k\leq 0$ والحالة الوحيدة التي يكون فيه الرقم x يتكون من أربع خانات و y من ثلاث خانات هي عندما $k=0$.

الأعداد الأولية والنظرية الأساسية في الحساب

(A) إذا كان 2^n-1 عدد أولي فان n عدد أولي.

الحل

الإثبات بواسطة المكافئ العكسي. ليكن $n=mt$ عدد مؤلف حيث $1<m,t<n$ ونجد أن $2^n-1=2^{mt}-1=(2^m)^t-1=(2^m-1)k$ ومنهـــــــــــــــا $2^m-1|2^n-1$ و $2^n-1>1$ عدد مؤلف، لاحظ أن $k>1$.

(B) إذا كان p العدد 27000001 له أربعة عوامل أولية فأوجد مجموعهم.

الحل

$$\begin{aligned}27000001 &= 27\times10^6+1\\ &= (3\times10^2)^3+1\\ &= (300+1)(300^2-300+1)\\ &= 301(300^2+2\times300+1-3\times300)\\ &= 7\times43((300+1)^2-30^2)\\ &= 7\times43(301-30)(301+30)\\ &= 7\times43\times271\times331\end{aligned}$$

ويمكن التحقق من أن كل من 271 و 331 عدد أولي. ويكون مجموعهم مساويا 652.

(C) هل $4^{2009}+2009^4$ عدد أولي؟

الحل

بتطبيق متباينة صوفي جيرمين للمقدار $2009^4+4\times(4^{502})^4$.

متطابقة صوفي جيرمين Sophie Germain :

$$\begin{aligned}a^4+4b^4 &= a^4+4a^2b^2+4b^4-4a^2b^2\\ &= (a^2+2b^2)^2-(2ab)^2\end{aligned}$$

(D) أوجد جميع الحلول الصحيحة الموجبة للمعادلة $2^{2m}-3^{2n}=175$

الحل

واضح أن $m>n$. فكرة الحل التحليل ومناقشة الحالات تبعا للنظرية الأساسية في الحساب

$$2^{2m}-3^{2n}=(2^m-3^n)(2^m+3^n)=7\times5^2$$

لاحظ أن $(2^m-3^n)<(2^m+3^n)$ وعليه يكون لدينا الحالات:

$$(2^m-3^n)=1,\quad (2^m+3^n)=175\cdots(1)$$

$$(2^m-3^n)=5,\quad (2^m+3^n)=35\cdots(2)$$

$$(2^m-3^n)=7,\quad (2^m+3^n)=25\cdots(3)$$

ونجد أن المعادلة (3) فقط التي لها حل هو $m=4$ و $n=2$.

(E) إذا كان p عدد أولي أكبر من 3 فإن العدد p^2+2 مؤلف و $24|p^2-1$

الحل

أي عدد أولي أكبر من 3 يكون على الصورة $6k\pm1$ حيث $k\in\mathbb{Z}^+$ وعليه يكون

$p^2+2=36k^2 \pm 12k+3$ ، أي أن $3 \big| p^2+2$

وأيضا $p^2-1=12k(3k\pm1)$ وحيث أن $k(3k\pm1)$ عدد زوجي لجميع $k \in \mathbb{Z}^+$، إذن $24 \big| p^2-1$.

(F) أوجد جميع الأعداد الأولية p,q التي تجعل p^2+pq+q^2 مربع كامل

الحل

بفرض $p^2+pq+q^2=n^2$ حيث n عدد صحيح موجب

$$p^2+pq+q^2=n^2 \Rightarrow (p+q)^2-pq=n^2 \Rightarrow (p+q)^2-n^2=pq$$
$$\Rightarrow (p+q-n)((p+q+n)=pq$$

إذن $((p+q+n)=pq$, $(p+q-n)=1$ لان $p+q-n \neq p,q$

ومنها $2p+2q=pq+1$ وعليه $pq-2p-2q+4=3$

ومنها $(p-2)(q-2)=3$ ويكون $p=3$ و $q=5$ أو العكس.

(G) إذا كان للمعادلة $x^2-2px+p^2-5p-1=0$ جذرين صحيحين ، حيث p عدد أولي أوجد القيم الممكنة للعدد p .

الحل

$$x_{1,2}=\frac{2p\pm\sqrt{4p^2-4(p^2-5p-1)}}{2}$$

$$= p \pm \sqrt{5p+1}$$

لكي يكون للمعادلة جذرين صحيحين لابد أن يكون $5p+1$ مربع كامل. ليكن $5p+1 = n^2$ حيث n عدد صحيح موجب. $5p = (n-1)(n+1)$ وعليه $n-1=5$ أو $n+1=5$ ونجد أن p يساوي 3 أو 7 .

(H) حلل العدد 1001001001 إلى عوامله الأولية.

الحل

$$\begin{aligned}1001001001 &= 1001\times10^6+1001\\ &= 1001(10^6+1)\\ &= 7\times11\times13((10^2)^3+1)\\ &= 7\times11\times13\times101\times9901\end{aligned}$$

(I) أوجد جميع الأعداد الأولية p بحيث العدد p^2+11 له 6 قواسم مختلفة من بينها العدد 1 والعدد نفسه

الحل

إذا كان p عدد أولي أكبر من 3 فإن $p = 6k \pm 1, \quad k \in \mathbb{Z}$

$$\Rightarrow p^2 = 36k^2 \pm 12k + 1$$

$$\Rightarrow p^2 + 11 = 36k^2 \pm 12k + 12$$

$$\Rightarrow 12 \mid p^2 + 11$$

وحيث أن $12 < p^2 + 11$ و العدد 12 له 6 قواسم هي $1,2,3,4,6,12$. إذن p^2+11 له أكثر من 6 قواسم.

يتبقى حالتين هما $p=2$ و $p=3$:

إذا كان $p=2$ فإن $p^2+11=15$ له أربعة قواسم فقط.

إذا كان $p=3$ فإن $p^2+11=20$ له ستة قواسم بالضبط. إذاً $p=3$ هو الحل الوحيد.

(J) إذا كان p,q أوليان وكان $r = \dfrac{p^2+q^2}{p+q}$ عدد صحيح فأثبت أن r أولي.

الحل

إذا كان $p=q$ واضح أن $r = \dfrac{p^2+q^2}{p+q} = \dfrac{p^2}{2p} = p$ وهو أولي. لنفرض الآن أن $p \neq q$ أن

$r = \dfrac{p^2 + q^2}{p + q}$ عدد صحيح. بما أن $p^2 + q^2 = (p+q)^2 - 2pq$ فإن $p + q \mid 2pq$ ولكن $(p+q, pq) = 1$ لأن $(p+q, q) = 1, (p+q, p) = 1$. إذا $p + q \mid 2$ وهذا مستحيل.

التطابقات قياس n

(A) أوجد آخر رقمين(خانتي الآحاد والعشرات) من العدد 7^{2010} .

الحل

بما أن $7^4 = 49^2 = (50-1)^2 \equiv 1 \pmod{100}$

إذا $7^{2010} = (7^4)^{502} \times 7^2 \equiv 1^{502} \times 49 \equiv 49 \pmod{100}$ **وعليه فإن آخر رقمين هما** 49

(B) أثبت أن $2222^{5555} + 5555^{2222}$ يقبل القسمة على 7

الحل

$$2222 \equiv 3 \pmod 7$$

$$3^3 = 27 \equiv -1 \pmod 7$$

$$2222^{5555} \equiv 3^{5553+2} \equiv 3^{3k+2} \equiv (-1)^k \cdot 3^2 \equiv -9 \equiv -2 \pmod 7$$

لاحظ أن k عدد فردي. بالمثل

$$5555 \equiv 4 \pmod 7$$

$$3^3 = 27 \equiv -1 \pmod 7$$

$$5555^{2222} \equiv 4^{2220+2} \equiv 4^{3m+2} \equiv (-1)^m \cdot 4^2 \equiv 16 \equiv 2 \pmod 7$$

لاحظ m زوجي. بالجمع نصل للمطلوب.

(C)أوجد آخر رقمين من العدد $229^{10} + 37^{10}$.

الحل

سنستخدم الخاصية: إذا كان $a \equiv b \pmod n$ فإن $a^n \equiv b^n \pmod{n^2}$.

$$229 \equiv 29 \equiv -1 \pmod{10} \Rightarrow 229^{10} \equiv (-1)^{10} \equiv 1 \pmod{100}$$

$$37 \equiv 7 \pmod{10} \Rightarrow 37^{10} \equiv 7^{10} \equiv (50-1)^5 \equiv 250 - 1 \equiv 49 \pmod{100}$$

إذا $229^{10} + 37^{10} \equiv 1 + 49 \equiv 50 \pmod{100}$ والباقي يكون 50.

(D) أوجد آخر رقمين من العدد 2^{999}.

الحل

الحل

لاحظ أولا أن: $2^{10} \equiv -1 (\bmod 25)$ وعليه فان

$$2^{997} = (2^{10})^{99}.2^{7} \equiv (-1).3 (\bmod 25) \equiv 22 (\bmod 25)$$

ومنها نجد أن

$$2^{2}.2^{997} \equiv 4.22 (\bmod 100) \equiv 88 (\bmod 100)$$

لاحظ استخدمنا: $a \equiv b (\bmod n) \Leftrightarrow am \equiv bm (\bmod mn)$ لكل $m \in \mathbb{Z}^{+}$.

حل آخر: $2^{12} \equiv -4 (\bmod 100)$ ومنها $2^{72} = (2^{12})^{6} \equiv -4 (\bmod 100)$ وأيضا $2^{432} = (2^{72})^{6} \equiv -4 (\bmod 100)$ وعليه $2^{864} \equiv 16 (\bmod 100)$.

أيضا $2^{60} \equiv -24 (\bmod 100)$ ومن ثم $2^{999} \equiv 88 (\bmod 100)$.

(E) إذا كان p عدداً أولياً و k عدد صحيح بحيث $1 \leq k < p$ فأثبت أن $p \left| \binom{p}{k} \right.$.

الحل

بما أن $k\binom{p}{k} = p\binom{p-1}{k-1}$، إذن $p \left| k\binom{p}{k} \right.$ وحيث أن $\gcd(k,p) = 1$ أذن $p \left| \binom{p}{k} \right.$، الجزء الثاني ينتج مباشرة من نظرية ذات الحدين واستخدام الجزء الأول.

(F) حل المعادلة التالية في الأعداد الصحيحة $x^{2} + y^{2} = 3^{2008}$.

الحل

بما أن $x^2 + y^2 \equiv 3^{2008} \equiv 0 \pmod 3$ وحيث أنه لأي عدد صحيح a فان $a^2 \equiv 0 \ or\ 1 \pmod 3$ وعليه $x^2 + y^2 \equiv 0 \pmod 3$ إذا وإذا فقط $3 \mid x, y$. إذا افرض أن $x = 3x_1$ و $y = 3y_1$ وبالتعويض في المعادلة والقسمة على 3^2 نستنتج أن $x_1^{\,2} + y_1^{\,2} = 3^{2006}$.

بتكرار نفس الإجراء مرات متعاقبة يتولد متتابعة $(x_k)_{k=1}^{1004}$ وأخرى $(y_k)_{k=1}^{1004}$ بحيث $x = 3^{1004} x_{1004}$ و $y = 3^{1004} y_{1004}$ و $x_{1004}^{\ \ 2} + y_{1004}^{\ \ 2} = 1$ وهذه لها الحلول الأربعة $(0, \pm 1), (\pm 1, 0)$.

إذا المعادلة الأصلية لها الحلول $(0, \pm 3^{1004}), (\pm 3^{1004}, 0)$.

(G) حدد الأعداد الصحيحة الموجبة m بحيث يكون $m! + 5$ مكعب كامل.

الحل

دراسة هذه المسألة قياس 7 سيكون مناسب جدا، وهذه إستراتيجية مهمة.

بما أن $m \equiv 0,1,2,3,4,5,6 \pmod 7$ نريد أن نرى بواقي m^3 لذلك سنكتب بواقي القسمة على 7 بالشكل $m \equiv 0, \pm 1, \pm 2, \pm 3 \pmod 7$ حتى يسهل حساب المكعبات.

بالتكعيب وفقا للخاصية $a^k \equiv b^k \pmod n$ نجد أن $m^3 \equiv 0, \pm 1 \pmod 7$. إذا باقي مكعب أي عدد لدى قسمته على 7 هو 0 أو ± 1. لذلك إذا كانت $m \geq 7$ فإن $m! + 5$ ليس مكعب كامل لأن

$$m! + 5 \equiv 0 + 5 \equiv 5 \pmod 7$$

يبقى فقط فحص $m!+5$ عندما $m<7$:

$$m=6,\ m!+5=5(6\cdot4\cdot3\cdot2+1)=5\cdot145=5^2\cdot29$$

$$m=5,\ m!+5=5(4\cdot3\cdot2+1)=5\cdot25=5^3$$

عندما $m=4,3,2,1$ فإن $m!+5=29,11,7,6$ على الترتيب. إذا $m!+5$ مكعب كامل فقط عندما $m=5$.

(H) أثبت أنه يوجد عدد غير منتهي من الأعداد الأولية التي على الصورة $4k+1$.

الحل

بفرض يوجد عدد منتهٍ من الأعداد الأولية التي على الصورة $4k+1$، هي $p_1<p_2<\ldots<p_t$. خذ العدد $N=(2p_1p_2\ldots p_t)^2+1$. بما أن $N>1$ عدد فردي، إذا يوجد له قاسم أولي $p>2$. أي أن $(2p_1p_2\ldots p_t)^2\equiv-1(\bmod p)$ وعليه p يجب أن يكون على الصورة $4n+1$ حيث $n\in\mathbb{Z}^+$ و بما أن $p_1,p_2,\ldots,p_t$ هي جميع الأعداد التي على الصورة $4k+1$ فإن $p=p_i$ حيث $1\le i\le t$ وبالتالي $p|N$ و $p\left|(2p_1p_2\ldots p_t)^2\right.$ وعليه $p\left|N-(2p_1p_2\ldots p_t)^2\right.=1$ وهذا مستحيل. إذن عكس الفرض هو الصحيح.

(I) أثبت أن $2^{11\times 31} \equiv 2(\bmod 11\times 31)$

الحل: باستخدام الخاصية (8): $a \equiv b(\bmod n_1),\ a \equiv b(\bmod n_2)$ إذا وإذا فقط

. $a \equiv b(\bmod [n_1, n_2])$

نستنتج أن

$2^{11\times 31} \equiv 2(\bmod 11\times 31)$ إذا وإذا فقط $2^{11\times 31} \equiv 2(\bmod 11)$ و $2^{11\times 31} \equiv 2(\bmod 31)$. بما أن $2^5 \equiv 32 \equiv -1\ (\bmod 11)$ فإن

$$2^{11\times 31} \equiv 2^{5(68)+1} \equiv (-1)^{68}\cdot 2^1 \equiv 2 \bmod 11$$

بالمثل حيث أن $2^5 \equiv 1(\bmod 31)$ نستنتج أن $2^{11\times 31} \equiv 2(\bmod 31)$ ويثبت المطلوب.

(J) أوجد المربعات الكاملة في المتتابعة

$$1!,\ 1!+2!,\ 1!+2!+3!, 1!+2!+3!+4!,\ \ldots,\ 1!+2!+3!+\cdots+n!,\ \ldots$$

الحل

بفرض $S_n = 1!+2!+3!+\cdots+n!$

من خلال الحساب يتضح أن الحدود من S_1 إلى S_4 ليس بينها مربع كامل سوى S_1, S_3 .

الآن افرض $n \geq 5$. لدينا $S_n = (1!+2!+3!+4!)+5!+\cdots+n! = 33+5!+\cdots+n!$

$S_n - 3 = 30+5!+\cdots+n!$ كل حد من حدود $5!+\cdots+n!$ يقبل القسمة على 5 وعليه

فإن $S_n - 3$ يقبل القسمة على 5 . بمعنى آخر $S_n \equiv 3(\bmod 5)$. هذا التطابق قياس 5 مستحيل

التحقق عندما يكون S_n مربع كامل وذلك لان لأي عدد طبيعي k فإن $k \equiv 0, \pm 1, \pm 2 \pmod 5$ وعليه فإن $k^2 \equiv 0, 1, 4 \pmod 5$ إذا S_n ليس مربع كامل لكل $n \geq 5$.

(K)أوجد باقي قسمة $17 + 177 + 1777 + \cdots + 1\underbrace{77\cdots 7}_{20}$على 7 .

الحل

ضع $S = 17 + 177 + 1777 + \cdots + 1\underbrace{77\cdots 7}_{20}$.

$$S \equiv \sum_{k=1}^{20} 10^k \pmod 7 \equiv 3(3+2+6+4+5+1)+3+2 \equiv 5 \pmod 7$$

المصادر

1. M. E. Lines, "Anumber for your Thoughts" Adam Hilger (1989). 7. Y. I. Manin and A. A. Panchishkin," Introduction to Mondern

Number Theory" 2nd Edition Springer (2005)

2. L. Moser, "An Introduction to the Theory of Numbers" Trillia Group, Indiana (1975).

3. I. Niven and H. S. Zuckerman: "An Introduction to the Theory of

Number" 4th Edition, John wiley and Sons (1980).

4. O. Ore: "Number Theory and its History", Dover Publications (1980). 11. A. J. Perttofrezzo and D. R. Byrkit," Elements of Number

Theory", Prentice Hall Inc. (1970).

5. H. S. Rose, "A Course in Number Theory" Oxford Science

Publications (1988). 13. K. A. Rosen, "Elementary Number Theory" 4th Edition, Addison- wesley (2000).

6. J. P. Serre, "A Course in Arithmetic" Springer International

student Edition (1973).

7 .15. Starke, "An Introduction to Number Theory" MTT Press (1984.(