القوى قياس p والجذور البدائية
Powers Modulo p and Primitive Roots

إذا كان a , p أوليين نسبياً، فإن نظرية فيرما الصغرى (الفصل التاسع) تخبرنا أن:

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

طبعاً من الممكن جداً أن بعض القوى الأصغر للعدد a يطابق 1 قياس p. فمثلاً، $2^3 \equiv 1 (\mathrm{mod}\ 7)$. من جهة أخرى، قد يوجد بعض قيم a التي تتطلب استخدام جميع القوى $(p-1)^{st}$. مثال، قوى 3 قياس 7 هي:

$$3^1 \equiv 3 (\mathrm{mod}\ 7), \quad 3^2 \equiv 2 (\mathrm{mod}\ 7), \quad 3^3 \equiv 6 (\mathrm{mod}\ 7),$$
$$3^4 \equiv 4 (\mathrm{mod}\ 7), \quad 3^5 \equiv 5 (\mathrm{mod}\ 7), \quad 3^6 \equiv 1 (\mathrm{mod}\ 7)$$

لذلك، كل القوة السادسة (6^{th}) للعدد 3 مطلوبة قبل أن نحصل على 1 قياس 7.

دعنا نستعرض أمثلة أكثر لنرى إذا ما كنا نستطيع اكتشاف نموذج عام. الجدول رقم (٢١,١) يستعرض أصغر قوة للعدد ٩ والذي يطابق 1 قياس p للأعداد الأولية $p = 5,7,11$ ، ولكل a بين 1 , $p-1$. هناك ملاحظتان:

(1) أصغر أس e بحيث $a^e \equiv 1 \pmod{p}$ يبدو قاسم للعدد $p-1$.

(2) هناك بعض القيم للعدد a تتطلب الأس $p-1$.

وبما أننا ندرس هذا "الأصغر أس" في هذا الفصل، فسوف نعطي له اسم.

"ترتيب a قياس p " (order of a modulo p) هو الكمية :

$$e_p(a) = \text{أصغر أس } e \geq 1 \text{ بحيث } a^e \equiv 1 \pmod{p}$$

جدول (٢١,١). أصغر قوة للعدد a الذي يساوي 1 قياس p .

$p=11$
$1^1 \equiv 1 \pmod{11}$
$2^{10} \equiv 1 \pmod{11}$
$3^5 \equiv 1 \pmod{11}$
$4^5 \equiv 1 \pmod{11}$
$5^5 \equiv 1 \pmod{11}$
$6^{10} \equiv 1 \pmod{11}$
$7^{10} \equiv 1 \pmod{11}$
$8^{10} \equiv 1 \pmod{11}$
$9^5 \equiv 1 \pmod{11}$
$10^2 \equiv 1 \pmod{11}$

$p=7$
$1^1 \equiv 1 \pmod{7}$
$2^3 \equiv 1 \pmod{7}$
$3^6 \equiv 1 \pmod{7}$
$4^3 \equiv 1 \pmod{7}$
$5^6 \equiv 1 \pmod{7}$
$6^2 \equiv 1 \pmod{7}$

$p=5$
$1^1 \equiv 1 \pmod{5}$
$2^4 \equiv 1 \pmod{5}$
$3^4 \equiv 1 \pmod{5}$
$4^2 \equiv 1 \pmod{5}$

(لاحظ أننا سمحنا فقط لقيم a التي تتناسب أولياً مع p).

بالعودة إلى الجدول 21.1، نرى على سبيل المثال، $e_5(2)=4$, $e_7(4)=3$, $e_{11}(7)=10$. نظرية فيرما الصغرى تقول إن

$a^{p-1} \equiv 1 \pmod{p}$ ؛ لذلك فنحن نعلم أن $e_p(a) \le p-1$. ملاحظتنا الأولى هي أن $e_p(a)$ يبدو على أنه قاسم للعدد $p-1$.

ملاحظتنا الثانية هي أنه يبدو دائماً وجود بعض القيم للعدد a بحيث $e_p(a) = p-1$. سنسعى الآن في فحص صحة كلتا الملاحظتين. سنبدأ بالملاحظة الأولى، وهي الأسهل بينهما.

نظرية (٢١,١). (خاصية ترتيب قابلية القسمة)

ليكن a عدداً صحيحاً لا يقبل القسمة على العدد الأولي p ، وافرض أن $a^n \equiv 1 \pmod{p}$. عندئذ الترتيب $e_p(a)$ يقسم n.

بشكل خاص، الترتيب $e_p(a)$ دائماً يقسم $p-1$.

البرهان

تعريف الترتيب $e_p(a)$ يخبرنا أن $a^{e_p(a)} \equiv 1 \pmod{p}$ ، ولنفرض أن $a^n \equiv 1 \pmod{p}$. ليكن $G = \gcd(e_p(a), n)$ ، وليكن (u,v) هو الحل الصحيح الموجب للمعادلة :

$$e_p(a)u - nv = G$$

(نظرية المعادلة الخطية الواردة في الفصل السادس تقول إن هناك حلاً).

سنحسب الآن المقدار $a^{e_p(a)} \equiv 1 \pmod{p}$ بطريقتين مختلفتين :

$$a^{e_p(a)u} = \left(a^{e_p(a)}\right)^u \equiv 1^u \equiv 1 \pmod{p},$$

$$^{e_p(a)u} = a^{nv+G} = \left(a^n\right)^v \cdot a^G \equiv 1^v \cdot a^G \equiv a^G \pmod{p}$$

إن هذا يبين أن $a^G \equiv 1 \pmod p$. لكن $e_p(a)$ هي أصغر قوة للعدد a تطابق 1 قياس p ؛ لذلك فإن $G \geq e_p(a)$. من ناحية أخرى، $G = \gcd\left(e_p(a), n\right)$ ، وعليه فإن G تقسم كل من $e_p(a)$, n. كحالة خاصة $G \leq e_p(a)$. الاحتمال الوحيد هو $G = e_p(a)$ ، إذاً $e_p(a)$ تقسم n.

أخيراً، نظرية فيرما الصغرى (الفصل التاسع) تخبرنا أن $a^{p-1} \equiv 1 \pmod p$ ، وبأخذ $n = p-1$ نستنتج أن $e_p(a)$ تقسم $p-1$.

مهمتنا القادمة هي النظر إلى الأعداد التي لها أكبر ترتيب ممكن: $e_p(a) = p-1$. إذا كانت a من هذه الأرقام، فإن القوى:

$$a\,,\ a^2\,,\ a^3, \ldots,\ a^{p-3},\ a^{p-2},\ a^{p-1} \pmod p$$

يجب أن تكون جميعها مختلفة قياس p.

[إذا لم تكن جميع القوى مختلفة، فإن $a^i \equiv a^j \pmod p$ لبعض الأسس $1 \leq i < j \leq p-1$ ، وهذا يعني أن $a^{j-i} \equiv 1 \pmod p$ ، حيث إن الأس $j-i$ أقل من $p-1$]. الأعداد التي تتطلب أكبر أس مهم جداً أن نعطيها اسم.

العدد g الذي له أكبر ترتيب

$$e_p(g) = p-1$$

يسمى جذراً بدائيًّا قياس p

primitive root modulo p

بمعاودة النظر إلى جداول رقم $p = 5,7,11$ ، نرى أن 2 , 3 جذور بدائية قياس 5 ، و 3 , 5 جذور بدائية قياس 7 و 2 , 6 , 7 , 8 جذور بدائية قياس 11.

سنأتي الآن لأهم نتيجة في هذا الفصل.

نظرية (٢١,١). (نظرية الجذور البدائية)

كل عدد أولي له جذر بدائي. بشكل أكثر دقة، هناك $\phi(p-1)$ جذر بدائي قياس p.

على سبيل المثال، نظرية الجذر البدائي تقول إن هناك $\phi(10)=4$ جذراً بدائيًّا قياس 11، ورأينا أن الجذور البدائية قياس 11 هي الأعداد $2, 6, 7, 8$. نفس الشيء، فإن النظرية تقول إن هناك $\phi(36)=12$ جذراً بدائيًّا قياس 37. وأن هناك $\phi(9906)=3024$ جذراً بدائيًّا قياس 9907. في الحقيقة، الجذور البدائية قياس 37 هي 12 عدد:

$$2,5,13,15,17,18,19,20,22,24,32,35$$

لن نبدد السطور في عرض 3024 جذر بدائي قياس 9907. إن إحدى سلبيات نظرية الجذور البدائية هي أنها لا تعطي طريقة محددة لإيجاد الجذور البدائية قياس p.

كل ما نستطيع عمله هو البدء بفحص $a=2$، $a=3$، $a=5$، $a=6$، ... حتى نجد قيمة العدد a بحيث $e_p(a)=p-1$.

(هل تعرف لماذا العدد 4 لا يمكن أن يكون جذراً بدائيًّا؟) على كل حال، إذا أوجدنا جذراً بدائيًّا واحداً قياس p، فليس من الصعب أن نجد البقية (انظر تمرين 21.6).

برهان نظرية الجذر البدائي

سنبرهن نظرية الجذر الأولى باستخدام أكثر الطرق فاعلية في نظرية الأعداد: "العد". قد تستغرب كيف أن أسلوب العد فعّال جداً. فهو أول أساليب التفكير في

مرحلة رياض الأطفال. ما سنفعله هو أخذ مجموعة معينة من الأعداد. سوف نحصي كم عدداً في المجموعة بطريقتين مختلفتين.

إن فكرة عد أشياء بطريقتين مختلفتين ثم مقارنة النتائج لها تطبيقات واسعة في نظرية الأعداد وفي الرياضيات بشكل عام.

لكل عدد a بين 1 و $p-1$ ، نعلم أن ترتيب $e_p(a)$ يقسم $p-1$. لذلك، لكل عدد a يقسم $p-1$ ، قد نسأل كم a ترتيبها $e_p(a)$ يساوي d. نسمي هذا العدد $\psi(d)$.

بمعنى آخر:

(عدد الـ $a's$ بحيث $1 \le a < p$, $\psi(d) = \left(e_p(a)\right) = d$). وبشكل خاص، $\psi(p-1)$ هو عدد الجذور البدائية قياس p.

ليكن n أي عدد يقسم $p-1$ ، وليكن $p-1 = nk$. إذاً يمكننا تحليل كثير الحدود $X^{p-1}-1$ كما يلي:

$$\begin{aligned} X^{p-1}-1 &= X^{nk}-1 \\ &= \left(X^n\right)^k - 1 \\ &= \left(X^n-1\right)\left(\left(X^n\right)^{k-1} + \left(X^n\right)^{k-2} + \cdots + \left(X^n\right)^2 + X^n + 1\right) \end{aligned}$$

سنحسب كم جذراً لكثيرة الحدود هذه قياس p.

أولاً نلاحظ أن

$X^{p-1}-1 \equiv 0 \pmod p$ لها بالضبط $p-1$ حل،

لأن نظرية فيرما الصغرى تخبرنا أن $X = 1,2,3,\ldots,p-1$ جميعها حلول.

من جهة أخرى:

$$X^n - 1 \equiv 0 \pmod{p}$$

لها n حل على الأكثر،

$$(X^n)^{k-1} + (X^n)^{k-2} + \cdots + X^n + 1 \equiv 0 \pmod{p}$$

ولها على الأكثر $nk - n$ حل. بشكل عام، إذا كان $F(X)$ كثيراً من الدرجة D معاملاته أعداد صحيحة، فإن التطابق $F(X) \equiv 0 \pmod{p}$ له على الأكثر D حل قياس p. سنترك هذه الحقيقة كتمرين لك لتقوم بإثباتها.

لذلك نعرف الآن أن:

$$\underbrace{X^{p-1} - 1}_{\substack{\text{exactly } p-1=nk \\ \text{roots mod } p}} = \underbrace{X^n - 1}_{\substack{\text{at most n} \\ \text{roots mod } p}} \times \underbrace{\left((X^n - 1)(X^n)^{k-1} + (X^n)^{k-2} + \cdots + X^n + 1\right)}_{\text{at most } nk-n \text{ roots mod } p}$$

وهذا صحيح فقط إذا كان $X^n - 1$ له بالضبط n جذراً قياس p؛ لأن غير ذلك لن يكون للطرف الأيمن عدد كافٍ من الجذور. وهذا يثبت الحقيقة المهمة التالية:

إذا n قسم $p-1$، فإن التطابق

$$X^n - 1 \equiv 0 \pmod{p}$$

له بالضبط n حل عندما $0 \le X < p$

دعنا الآن نحسب عدد حلول $X^n - 1 \equiv 0 \pmod{p}$ بطريقة مختلفة. إذا كان $X = a$ حلاً، فإن $a^n \equiv 1 \pmod{p}$، إذاً من خاصية ترتيب القسمة، نعلم أن $e_p(a)$ يقسم n. لذلك إذا نظرنا إلى قواسم n وإذا أخذنا لكل قاسم d للعدد n قيم a بحيث $e_p(a) = d$، عندئذ سنحصل على كل الحلول للتطابق $x^n - 1 \equiv 0 \pmod{p}$. بمعنى، إذا كانت $d_1, d_2, \ldots, d_r$ قواسم n، فإن عدد

حلول $x^n-1\equiv 0\pmod p$ يساوي :

$$\psi(d_1)+\psi(d_2)+\cdots+\psi(d_r)$$

الآن نكون قد حسبنا عدد حلول $x^n-1\equiv 0\pmod p$ بطريقتين مختلفتين. في الأولى رأينا أن هناك n من الحلول ، وفي الثانية رأينا أن هناك $\psi(d_1)+\cdots+\psi(d_r)$ حلاً. هذان العددان هما نفس العدد، لذلك من خلال حسابنا لعدد الحلول، نكون قد برهنا الصيغة الجميلة التالية :

ليكن n قاسم للعدد $p-1$ وليكن $d_1,d_2,\ldots,d_r$ قواسم n بما فيها 1 و n ، فإن :

$$\psi(d_1)+\psi(d_2)+\cdots+\psi(d_r)=n$$

تبدو هذه الصيغة مألوفة لدينا ، إنها تماماً نفس الصيغة التي برهنّاها لدالة فاي لأويلر في الفصل العشرون .

سنستخدم الآن حقيقة أن ϕ و ψ كليهما يحقق هذه الصيغة لإثبات أن ϕ و ψ متساويان.

إن أولى ملاحظاتنا هي أن $\phi(1)=1$ و $\psi(1)=1$ ، إذاً الدالتان متساويتان عند $n=1$. سنعمل الآن على اختبار فيما إذا كان $\phi(q)=\psi(q)$ عندما $n=q$ ، حيث q عدد أولي. قواسم q هي 1 , q ، لذلك $\phi(q)+\phi(1)=q=\psi(q)+\psi(1)$ ولكن نعلم أن $\phi(1)=\psi(1)=1$ ، بطرح 1 من الطرفين ينتج أن $\phi(q)=\psi(q)$.

ماذا عن الحالة $n=q^2$ ؟ قواسم q^2 هي 1 , q , q^2 إذاً :

$$\phi(q^2)+\phi(q)+\phi(1)=q^2=\psi(q^2)+\psi(q)+\psi(1)$$

وبما أن $\phi(q)=\psi(q)$, $\phi(1)=\psi(1)$ إذاً $\phi(q^2)=\psi(q^2)$.

بشكل مشابه، إذا كان $n=q_1q_2$ حيث q_1 , q_2 عددين أوليين مختلفين، فإن قواسم n هي 1 , q_1 , q_2 , q_1q_2 ، إذاً :

$$\phi(q_1q_2)+\phi(q_1)+\phi(q_2)+\phi(1)=q_1q_2$$
$$=\psi(q_1q_2)+\psi(q_1)+\psi(q_2)+\psi(1)$$

بحذف الحدود المتساوية من الطرفين ينتج أن $\phi(q_1q_2)=\psi(q_1q_2)$.

هذه الأمثلة توضح كيف نبرهن أن $\phi(n)=\psi(n)$ لكل n بالبدء من القيم الصغيرة للعدد إلى القيم الأكبر له. يمكننا كذلك أن نعطي برهاناً بالاستقراء الرياضي. (ربما ترغب بالعودة إلى برهان النظرية الأساسية للحساب الواردة في الفصل السابع لتعطي برهاناً آخر باستخدام الاستقراء الرياضي). لذلك لنفرض أننا برهنا أن $\phi(d)=\psi(d)$ لكل الأعداد $d<n$ ، وأننا نحاول إثبات أن $\phi(d)=\psi(d)$. ليكن $d_1,d_2,\ldots,d_r$ قواسم n كالمعتاد. أحد هذه القواسم هو n نفسه، من الملائم أن نفرض أن $d_1=n$. باستخدام صيغة الجمع للدالتين ϕ , ψ ، نجد أن:

$$\phi(n)+\phi(d_2)+\phi(d_3)+\cdots+\phi(d_r)=n$$
$$=\psi(n)+\psi(d_2)+\psi(d_3)+\cdots+\psi(d_r)$$

لكن كل الأعداد $d_2,d_3,\ldots,d_r$ أقل من n ، لذلك فإن فرضنا يخبرنا أن $\phi(d_i)=\psi(d_i)$ لكل $i=2,3,\ldots,r$. لذلك يمكننا حذف القيم المتساوية من طرفي المعادلة، وبالتالي سنحصل على المساواة المطلوبة $\phi(n)=\psi(n)$.

خلاصة ما سبق، برهنا أن لكل عدد n يقسم $p-1$ يوجد بالضبط $\phi(n)$ من الأعداد a ، حيث $e_p(a)=n$. بأخذ $n=p-1$ ، نرى أنه يوجد $\phi(p-1)$

عدد a بحيث $e_p(a)=p-1$. لكن قيم a حيث $e_p(a)=p-1$ هي تماماً جذور بدائية قياس p ، وبذلك نكون قد برهنا وجود $\phi(p-1)$ جذر بدائي قياس p . وحيث إن العدد $\phi(p-1)$ دائماً أكبر من أو يساوي 1 ، فإننا رأينا أن كل عدد أولي له على الأقل جذر بدائي واحد. وبذلك نكون قد أكملنا برهاننا على نظرية الجذر البدائي.

إن نظرية الجذر البدائي تخبرنا أنه يوجد الكثير من الجذور البدائية قياس p ، وبشكل دقيق، فإن عددها في الحقيقة يساوي $\phi(p-1)$. لسوء الحظ، أنها لا تعطينا أي معلومة ألبتة عن ماهية هذه الجذور البدائية. لنفرض أننا قلبنا السؤال، لنأخذ a عدداً ثابتاً، ولنسأل عن أي الأعداد الأولية التي يكون عندها a جذراً بدائيًّا. فمثلاً، لأي الأعداد الأولية يكون 2 جذراً بدائيًّا؟ نظرية الجذر البدائي لا تعطينا أي معلومة عن الجواب!

هنا قائمة عن الترتيب $e_p(2)$ لكل الأعداد الأولية حتى العدد 100. كتبنا e_p بدل $e_p(2)$ للاختصار.

$e_3=2$	$e_5=4$	$e_7=3$
$e_{11}=10$	$e_{13}=12$	$e_{17}=8$
$e_{19}=18$	$e_{23}=11$	$e_{29}=28$
$e_{31}=5$	$e_{37}=36$	$e_{41}=20$
$e_{43}=14$	$e_{47}=23$	$e_{53}=52$
$e_{59}=58$	$e_{61}=60$	$e_{67}=66$
$e_{71}=35$	$e_{73}=9$	$e_{79}=39$

$e_{83}=82$	$e_{89}=11$	$e_{97}=48$

بالنظر إلى هذه القائمة ، نرى أن 2 جذر بدائي للأعداد الأولية :

$$p=3,5,11,13,19,29,37,53,59,61,67,83$$

هل تلاحظ أي نمط؟ لا تجعل الإحباط يتسلل إلى نفسك إذا لم تلاحظ نمطاً ما، لا يوجد أحد حتى الآن اكتشف أي نمط. على كل حال، في عشرينات القرن العشرين قام "إميل آرتين"Emil Artin بوضع التخمين التالي :

تخمين (٢١,٣) (تخمين آرتين)

يوجد عدد لا نهائي من الأعداد الأولية p ، بحيث يكون العدد 2 جذراً بدائيًا قياس p .

طبعاً، لا يوجد شيء يميز العدد 2 عن غيره؛ لذلك قام آرتين أيضاً بوضع التخمين التالي :

تخمين (٢١,٤) (تخمين آرتين العام)

ليكن a أي عدد صحيح ليس مربعاً كاملاً ولا يساوي -1. عندئذ هناك عدد لا نهائي من الأعداد الأولية p بحيث يكون a جذراً بدائيًا قياس p .

حتى الآن، لم نبرهن حدسية (تخمين) آرتين، على الرغم من التقدم الكبير الذي حصل عليها في السنوات الأخيرة. فعلى سبيل المثال، في عام 1967 أثبت "كريستوفر هولي" Christopher Hooley أنه إذا كانت "حدسية عبارة ريمان العامة" صحيحة فإن "حدسية آرتين العامة" صحيحة أيضاً. وبأهمية مماثلة، قام "راجيف جوبتا" ، "م. رام مورتي"، و "روجر هيث – بروان" في عام 1985 بالبرهان على أنه يوجد على

الأكثر ثلاثة أزواج من الأعداد الأولية نسبياً كقيم للعدد a تكون عندها "حدسية آرتين العامة" غير صحيحة. بالطبع، هذه القيم الثلاث الافتراضية "السيئة" قد تكون غير موجودة، لكن لا يعرف أحد حتى الآن كيف يبرهن عدم وجودها. ولا يوجد أحد حتى الآن قادر على إثبات أن $a=2$ قيمة صالحة؛ لذلك حتى حدسية آرتين الأصلية تبقى بدون برهان!

تمارين

(٢١,١) ليكن p عدداً أوليًّا.

(a) ما قيمة $1+2+3+\cdots+(p-1) \pmod p$ ؟

(b) ما قيمة $1^2+2^2+3^2+\cdots+(p-1)^2 \pmod p$ ؟

(c) لأي عدد صحيح موجب k، أوجد قيمة:

$$1^k+2^k+3^k+\cdots+(p-1)^k \pmod p$$

وبرهن أن إجابتك صحيحة.

(٢١,٢) لأي عددين صحيحين a , m حيث $\gcd(a,m)=1$، سنفرض أن $e_m(a)$ هو أصغر أس $e \geq 1$ حيث $a^e \equiv 1 \pmod m$. نسمي $e_m(a)$ ترتيب a قياس m.

(a) احسب القيم التالية للعدد $e_m(a)$:

(i) $e_9(2)$ (ii) $e_{15}(2)$

(iii) $e_{16}(3)$ (iv) $e_{10}(3)$

(b) بيّن أن $e_m(a)$ دائماً يقسم $\phi(m)$.

(٢١,٣) في هذا التمرين سوف تبحث عن قيمة $e_m(2)$ للأعداد الصحيحة الفردية

m. للاختصار كتبنا e_m بدل $e_m(2)$ ؛ لذلك فإن e_m في هذا التمرين هي أصغر قوة للعدد 2 يطابق 1 قياس m.

(a) احسب قيمة e_m لكل عدد فردي $11 \le m \le 19$.

(b) هنا جدول يعطي قيم e_m لكل الأعداد الفردية بين 3 و 149 [ما عدا $11 \le m \le 19$ والتي قمت بالعمل عليها في الفرع (a)].

$e_3 = 2$	$e_5 = 4$	$e_7 = 3$	$e_9 = 6$
$e_{11} = **$	$e_{13} = **$	$e_{15} = **$	$e_{17} = **$
$e_{19} = **$	$e_{21} = 6$	$e_{23} = 11$	$e_{25} = 20$
$e_{27} = 18$	$e_{29} = 28$	$e_{31} = 5$	$e_{33} = 10$
$e_{35} = 12$	$e_{37} = 36$	$e_{39} = 12$	$e_{41} = 20$
$e_{43} = 14$	$e_{45} = 12$	$e_{47} = 23$	$e_{49} = 21$
$e_{51} = 8$	$e_{53} = 52$	$e_{55} = 20$	$e_{57} = 18$
$e_{59} = 58$	$e_{61} = 60$	$e_{63} = 6$	$e_{65} = 12$
$e_{67} = 66$	$e_{69} = 22$	$e_{71} = 35$	$e_{73} = 9$

$$e_{75}=20 \qquad e_{77}=30 \qquad e_{79}=39 \qquad e_{81}=54$$

$$e_{83}=82 \qquad e_{85}=8 \qquad e_{87}=28 \qquad e_{89}=11$$

$$e_{91}=12 \qquad e_{93}=10 \qquad e_{95}=36 \qquad e_{97}=48$$

$$e_{99}=30 \qquad e_{101}=100 \qquad e_{103}=51 \qquad e_{105}=12$$

$$e_{107}=106 \qquad e_{109}=36 \qquad e_{111}=36 \qquad e_{113}=28$$

$$e_{115}=44 \qquad e_{117}=12 \qquad e_{119}=24 \qquad e_{121}=110$$

$$e_{123}=20 \qquad e_{125}=100 \qquad e_{127}=7 \qquad e_{129}=14$$

$$e_{131}=130 \qquad e_{133}=18 \qquad e_{135}=36 \qquad e_{137}=68$$

$$e_{139}=138 \qquad e_{141}=46 \qquad e_{143}=60 \qquad e_{145}=28$$

$$e_{147}=42 \qquad e_{149}=148$$

باستخدام هذا الجدول أوجد (بمعنى خمَّن) صيغة للعدد e_{mn} بدلالة e_m , e_n و عندما $\gcd(m,n)=1$.

(c) استخدم صيغتك التخمينية من (b) لإيجاد قيمة e_{11227} . (لاحظ أن

$.(11227 = 103.109$

(d) برهن أن صيغتك التخمينية في (b) صحيحة.

(e) استخدم الجدول لتخمين صيغة للعدد e_{p^k} بدلالة e_p ، p ، k حيث p عدد فردي أولي.

استخدم صيغتك لإيجاد قيمة e_{68921} . (لاحظ أن $68921 = 41^3$).

(f) هل تستطيع إثبات أن صيغتك التخمينية لحساب e_{p^k} في (e) صحيحة؟

(٢١,٤) (a) أوجد جميع الجذور البدائية قياس 13.

(b) لكل عدد d يقسم 12 ، أوجد قيم a عندما $1 \le a < 13$ و $e_{13}(a) = d$.

(٢١,٥) (a) ليكن:

$$F(X) = X^D + A_1X^{D-1} + A_2X^{D-2} + \cdots + A_{D-1}X + A_D$$

كثير حدود معاملاته $A_1, A_2, \ldots, A_D$ أعداد صحيحة.

ليكن p عدداً أوليًّا بيّن أن التطابق $F(X) \equiv 0 \pmod p$ له على الأكثر D حلاً حيث $0 \le X < p$.

(b) كم حلاً للتطابق $X^4 + 5X^3 + 4X^2 - 6X - 4 \equiv 0 \pmod{11}$ حيث $0 \le X < 11$ ؟ هل لها أربعة حلول أو أقل من أربعة حلول؟

(c) كم حلاً للتطابق $X^2 - 1 \equiv 0 \pmod 8$ ، حيث $0 \le X < 8$ ؟ بما أن هذا التطابق له أكثر من حلين ، لماذا هنا لا يبرهن أن الفرع (a) غير صحيح.

(٢١,٦) (a) إذا كان g جذراً بدائيًّا قياس 37 ، أي الأعداد $g^2, g^3, \ldots, g^8$

جذر بدائي قياس 37 ؟

(b) إذا كان g جذراً بدائيًّا قياس p ، اشتق قانوناً بسيطاً يمكن استخدامه لتحديد فيما إذا كان g^k جذراً بدائيًّا قياس p ، وبرهن أن قانونك صحيح.

(c) افرض أن g جذر بدائي قياس العدد الأولي $p = 21169$. استخدم قانونك في (b) لتحديد أي الأعداد $g^2, g^3, \ldots, g^{20}$ جذور بدائية قياس 21169.

(٢١,٧) (a) أوجد كل الأعداد الأولية الأصغر من 20 التي يكون 3 جذراً بدائيًّا لها.

(b) إذا كنت قادراً على عمل برنامج كمبيوتر، أوجد كل الأعداد الأولية الأقل من 100 التي يكون 3 جذراً بدائيًّا لها.

(٢١,٨) إذا كان $a = b^2$ مربع كامل و p عدداً أوليًّا فرديًّا، وإشرح لماذا لا يمكن أن يكون a جذراً بدائيًّا قياس p .

(٢١,٩) ليكن p عدداً أوليًّا ، وليكن k عدداً لا يقبل القسمة على p ، وليكن b عدداً له k^{th} جذراً قياس p . أوجد صيغة توجد عدد الجذور k^{th} للعدد b قياس p وبرهن أن صيغتك صحيحة. (مساعدة: صيغتك يجب أن تعتمد على p , k وليس على b).

(٢١,١٠) اكتب برنامجاً لحساب $e_p(a)$ ، والذي يمثل أصغر أس موجب e بحيث $a^e \equiv 1 \pmod{p}$. [كن متأكداً من استخدامك لحقيقة أنه إذا كان $a^e \not\equiv 1 \pmod{p}$ لكل $1 \le e < p/2$ ، فإن $e_p(a)$ تلقائياً يساوي $p-1$].

(١٢,١١) اكتب برنامجاً يوجد أصغر جذر بدائي لعدد أولي معطى p . اعمل قائمة

لكل الأعداد الأولية الواقعة بين 100 و 200 والتي يكون العدد 2 جذراً بدائيًّا لها.

(٢١,١٢) اكتب برنامجاً يأخذ كثير الحدود $f(X)$ (معاملاته أعداد صحيحة) و m كمدخلات ويعطي كمخرجات جميع الحلول للتطابق:

$$f(X) \equiv 0 \pmod{m}$$

(لا تكن خيالياً، فقط عوض في $X = 0,1,2,\ldots,m-1$ وانظر أي القيم تمثل الحل).

(٢١,١٣) إذا كان a أوليًّا نسبياً مع كل من m , n ، وإذا كان $\gcd(m,n)=1$ ، أوجد صيغة لإيجاد $e_{mn}(a)$ بدلالة $e_m(a)$, $e_n(a)$.

(٢١,١٤) لأي عدد $m \geq 2$ ، ليس بالضرورة أن يكون أوليًّا، نقول إن g جذر بدائي قياس m إذا كانت أصغر قوة للعدد g المطابقة للعدد 1 قياس m هي القوة $\phi(m)^{th}$.

بمعنى آخر ، g جذر بدائي قياس m إذا كان

$$\gcd(g,m)=1 \quad , \quad g^k \not\equiv 1 \pmod{m}$$

لكل القوى $1 \leq k < \phi(m)$.

(a) لكل عدد $2 \leq m \leq 25$ ، حدد فيما إذا كان يوجد أي جذور بدائية قياس m.

(إذا كان لديك كمبيوتر، اعمل نفس الشيء لكل $m \leq 50$).

(b) استخدم البيانات التي حصلت عليها من (a) لعمل تخمين تحدد من خلاله أي قيم m لها جذور بدائية وأيها ليس لها.

(c) برهن أن تخمينك فيه صحيح.