الفصل الثاني والعشرون

الجذور البدائية والأدلة
Primitive Roots and Indices

الجميل في الجذر البدائي g قياس عدد أولي p هو ظهور أي عدد غير صفري قياس p على أنه قوة للعدد g. لذلك لأي عدد $1 \le a < p$ ، يمكننا اختيار قوة واحدة فقط من القوى:

$$g, g^2, g^3, g^4, \ldots, g^{p-3}, g^{p-2}, g^{p-1}$$

لتكون مكافئة للعدد a قياس p.

يسمى الأس "دليل a قياس p للأساس g"

(index of a modulo p for the base g)

لنفرض أننا حددنا g, p ، نرمز للدليل بالرمز $\mathrm{I}(a)$.

مثلاً ، إذا استخدمنا الجذر البدائي 2 كأساس للعدد الأولي 13 ؛ فإن $\mathrm{I}(3) = 4$ ؛ لأن $2^4 = 16 \equiv 3 \pmod{13}$. بالمثل، $\mathrm{I}(5) = 9$ لأن $2^9 = 512 \equiv 5 \pmod{13}$. لإيجاد الدليل لأي عدد معين، مثلاً 7 ، فإننا نحسب فقط القوى $2, 2^2, 2^3, \ldots$ قياس 13 حتى نحصل على عدد مطابق للعدد 7.

طريقة أخرى هي عمل جدول لكل قوى 2 قياس 13. عندها يمكننا أن نقرأ أي معلومة نريدها من الجدول.

I	1	2	3	4	5	6	7	8	9	10	11	12
$2^{\mathrm{I}} \pmod{13}$	2	4	8	3	6	12	11	9	5	10	7	1

قوى 2 قياس 13

على سبيل المثال ، لإيجاد $\mathrm{I}(11)$ نعمل مسح للصف الثاني من الجدول حتى نجد العدد 11 ، وعندها يمكننا أن نقرأ من الصف الأول للجدول أن الدليل هو $\mathrm{I}(11)=7$.

إن هذا يقترح طريقة أخرى لتنظيم البيانات التي قد تكون أكثر فائدة. ما نفعله هو إعادة ترتيب الأعداد بحيث يصبح الصف الثاني مرتب عددياً من 1 إلى 12 وبعد ذلك نقوم بتبديل الصفين الأول والثاني. الجدول الناتج فيه الأعداد مرتبة من 1 إلى 12 في الصف الأول ، وتحت كل عدد دليله.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{I}(a)$	12	1	4	2	9	5	11	3	8	10	7	6

الأدلة قياس 13 للأساس 2

الآن من السهل قراءة دليل أي عدد ، مثل $\mathrm{I}(8)=3$, $\mathrm{I}(10)=10$.

فيما مضى ، كان الباحثون في الأعداد يؤلفون جداول الأدلة لتستخدم في

الحسابات العددية[١]. النظرية التالية تسلط الضوء على السبب في كون الأدلة مفيدة عند إجراء العمليات الحسابية.

نظرية (٢٢,١) (قوانين الأدلة)

الأدلة تحقق القوانين التالية:

(a) $\mathrm{I}(ab) \equiv \mathrm{I}(a) + \mathrm{I}(b) \pmod{p-1}$ *[قانون الضرب].*

(b) $\mathrm{I}(a^k) \equiv k\mathrm{I}(a) \pmod{p-1}$ *[قانون القوة].*

البرهان

هذه القوانين ما هي إلا قوانين الأسس المعروفة ، متلازمة مع حقيقة أن g جذر بدائي. لذلك ؛ إذا أردنا إثبات (a) نحسب:

$$g^{\mathrm{I}(ab)} \equiv ab \equiv g^{\mathrm{I}(a)} g^{\mathrm{I}(b)} \equiv g^{\mathrm{I}(a)+\mathrm{I}(b)} \pmod{p}$$

هذا يعني أن $g^{\mathrm{I}(ab)-\mathrm{I}(a)-\mathrm{I}(b)} \equiv 1 \pmod{p}$. لكن g جذر بدائي ؛ لذلك $\mathrm{I}(ab)-\mathrm{I}(a)-\mathrm{I}(b)$ يجب أن تكون من مضاعفات $p-1$. وبذلك نكون قد برهنا (a). لإثبات (b) ، نجري الحسابات المشابهة التالية:

$$g^{\mathrm{I}(a^k)} \equiv a^k \equiv \left(g^{\mathrm{I}(a)}\right)^k \equiv g^{k\mathrm{I}(a)} \pmod{p}$$

يقتضي أن $\mathrm{I}(a^k) - k\mathrm{I}(a)$ من مضاعفات $p-1$ ، وبذلك نكون قد برهنا (b).

---

(١) في عام 1839 ، قام "كارل جاكوبي" بنشر "قوانين حسابية" تضم جدول لأدلة كل الأعداد الأولية الأقل من 1000. بعد ذلك ، قام "ويستيرن" و "ميلر" بعمل جدول موسع ضم كل الأعداد الأولية حتى 50021 ، وتم نشره في "رويال سوشيتي" الصادرة عن جامعة كامبريدج وذلك سنة 1968.

إن أحد أكثر الأخطاء الشائعة عند التعامل مع الأدلة هو اختزالهم قياس p بدلاً من قياس $p-1$. من المهم أن نتذكر دائماً أن الأدلة تظهر كأسس ، وأن الأس في نظرية فيرما الصغرى هو $p-1$ وليس p . مرة أخرى :

دائماً تختزل الأدلة قياس
$$p-1$$

أريد الآن أن أشرح بشكل مختصر كيف أن قوانين الدليل وجدول الأدلة يمكن استخدامها لتبسيط الحسابات وحل التطابقات ، لتحقيق هذا الهدف ، هنا جدول أدلة العدد الأولي $p=37$ والأساس $g=2$.

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{I}(a)$	36	1	26	2	23	27	32	3	16	24

a	11	12	13	14	15	16	17	18
$\mathrm{I}(a)$	30	28	11	33	13	4	7	17

a	19	20	21	22	23	24	25	26	27	28
$\mathrm{I}(a)$	35	25	22	31	15	29	10	12	6	34

a	29	30	31	32	33	34	35	36
$\mathrm{I}(a)$	21	14	9	5	20	8	19	18

أدلة قياس 37 للأساس 2

إذا أردنا حساب $23\cdot 19 \pmod{37}$ فإننا بدلاً من ضرب 23 و 19 يمكننا جمع دليليهما. إذاً

$$\begin{aligned} I(23\cdot 19) &\equiv I(23)+I(19) \\ &\equiv 15+35 \\ &\equiv 50 \\ &\equiv 14 \pmod{36} \end{aligned}$$

لاحظ أن الحسابات أنجزت قياس $p-1$ ، أي قياس 36 في حالتنا هذه . بالنظر إلى الجدول ، نجد أن $I(30)=14$ ونستنتج أن $23\cdot 19 \equiv 30 \pmod{37}$.

"انتظر دقيقة" ، قد تعترض على ذلك ، " استخدام الأدلة لحساب الضرب $23\cdot 19 \pmod{37}$ يتطلب الكثير من الجهد ". قد يكون من الأسهل ضرب 23 , 19 ثم قسمة الناتج على 37 ، ومن ثم اخذ الباقي . إن هناك سبباً قويًّا لاستخدام الأدلة في حساب القوى. على سبيل المثال :

$$I(29^{14}) \equiv 14\cdot I(29) \equiv 14\cdot 21 \equiv 294 \equiv 6 \pmod{36}$$

من الجدول نرى أن $I(27)=6$ ، لذلك $29^{14} \equiv 27 \pmod{37}$. هنا الرقم 29^{14} له خانة 21 ؛ لذلك لا نرغب في حساب القيمة المضبوطة للعدد 29^{14} يدوياً وبعد ذلك نختزل قياس 37. من ناحية أخرى ، نحن نعلم كيف نحسب $29^{14} \pmod{37}$ بسرعة باستخدام طريقة التربيعات المتعاقبة (الفصل السادس عشر). إذاً، هل الأدلة مفيدة فعلاً لأي شيء؟ الجواب هو أن القوة الحقيقية لجدول الأدلة لا يكمن في استخدامه للحسابات المباشرة، بل في كونه أداة لحل التطابقات. وسوف نعطي مثالين لتوضيح ذلك.

في مثالنا الأول ، ليكن لدينا التطابق $19x \equiv 23 \pmod{37}$.

إذا كانت x حلاً، فان دليل $19x$ يساوي دليل العدد 23. باستخدام قانون الضرب وأخذ قيم من جدول الأدلة ، يمكننا حساب :

$$\mathrm{I}(19x) \equiv \mathrm{I}(23)$$

$$\mathrm{I}(19) + \mathrm{I}(x) \equiv \mathrm{I}(23) \pmod{36}$$

$$35 + \mathrm{I}(x) \equiv 15 \pmod{36}$$

$$\mathrm{I}(x) \equiv -20 \equiv 16 \pmod{36}$$

لذلك ؛ فان دليل الحل هو $\mathrm{I}(x) = 16$ ، وبالنظر مرة أخرى للجدول، نجد أن $x \equiv 9 \pmod{37}$. يجب أن نقارن هذا الحل للتطابق $19x \equiv 23 \pmod{37}$ مع الطرق المرهقة المعروضة في الفصل الثامن. بالطبع ، فإن طريقة الدليل لا تكون مجدية إلا إذا كان لديك جدول أدلة جاهز ؛ لذلك فإن نظرية التطابق الخطي الواردة في الفصل الثامن تفرض نفسها .

بالنسبة لمثالنا الثاني سوف نقوم بحل مسألة تحتاج إلى كثير من الحسابات الشاقة حتى هذه اللحظة. سوف نبحث عن كل الحلول للتطابق :

$$3x^{30} \equiv 4 \pmod{37}$$

سنبدأ بأخذ الدليل للطرفين، ونستخدم الضرب وقوانين القوة.

$$\mathrm{I}\left(3x^{30}\right) = \mathrm{I}(4)$$

$$\mathrm{I}(3) + 30\mathrm{I}(x) \equiv \mathrm{I}(4) \pmod{36}$$

$$26 + 30\mathrm{I}(x) \equiv 2 \pmod{36}$$

$$30\mathrm{I}(x) \equiv -24 \equiv 12 \pmod{36}$$

لذلك سوف نحتاج حل التطابق $30\mathrm{I}(x) \equiv 12 \pmod{36}$ لإيجاد $\mathrm{I}(x)$.

[تحذير: لا تقسم الطرفين على 6 لتحصل على $5\mathrm{I}(x) \equiv 2 \pmod{36}$ ، سوف تفقد بعض الإجابات]. رأينا في الفصل الثامن كيف نحل تطابقاً من هذا النوع. بشكل عام، التطابق $ax \equiv c \pmod{m}$ له $\gcd(a,m)$ حلاً إذا كان $\gcd(a,m)$ يقسم c ، خلاف ذلك لا يكون لها حل. في حالتنا هذه $\gcd(30,36) = 6$ والذي يقسم 12 ، إذاً يجب أن يكون هناك 6 حلول. باستخدام الطرق الواردة في الفصل الثامن، أو بالمحاولة والخطأ نجد أن:

$$30\mathrm{I}(x) \equiv 12 \pmod{36}$$

إذاً

$$\mathrm{I}(x) \equiv 4, 10, 16, 22, 28, 34 \pmod{36}$$

أخيراً، نرجع إلى جدول الأدلة لنحصل على القيم المقابلة للمجهول x .

$$\mathrm{I}(16) = 4, \qquad \mathrm{I}(25) = 10, \qquad \mathrm{I}(9) = 16,$$
$$\mathrm{I}(21) = 22, \qquad \mathrm{I}(12) = 28, \qquad \mathrm{I}(28) = 34$$

وعليه؛ فإن التطابق $3x^{30} \equiv 4 \pmod{37}$ له ستة حلول:

$$x \equiv 16, 25, 9, 21, 12, 28 \pmod{37}$$

إن الإيجابيات الحسابية لاستخدام أدلة يمكن صياغتها بسهولة. قوانين الأدلة تحول الضرب إلى جمع والأسس إلى ضرب.

إن هذه العبارة مألوفة لدينا؛ لأنها تماماً مثل القوانين المطبقة على اللوغاريتمات:

$$\log(ab) = \log(a) + \log(b),$$

$$\log\left(a^k\right) = k\log(a)$$

لهذا السبب، يسمى الدليل أيضاً باللوغاريثم المنفصل. وتماماً كما استخدمت جداول اللوغاريثم في الزمن القديم لإجراء الحسابات، وذلك قبل ظهور الآلات الحاسبة الرخيصة، كذلك استخدمت جداول الأدلة لإجراء الحسابات في نظرية الأعداد.

في هذه الأيام، ومع توفر أجهزة الكمبيوتر، أصبحت جداول الدليل تستخدم بشكل قليل في الحسابات العددية، ولكن الأدلة ما زالت تحتفظ بمكانتها كأداة نظرية.

على كل حال، هناك سمة أخرى للوغاريتمات المنفصلة تجعلها مهمة للغاية في الأساليب الحديثة لكتابة الرسائل بالشيفرة. افرض أنك أُعطيت عدداً أوليًّا كبيراً p وعددين a , g قياس p. إن مسألة اللوغاريتم المنفصل (Discrete Logarithm Problem) (DLP) هي مسألة إيجاد الأس k بحيث $g^k \equiv a \pmod p$. بمعنى آخر، مسألة اللوغاريتم المنفصل تطلب منك إيجاد دليل a قياس p للأساس g. كما رأيت في الفصل السادس عشر، من السهل حساب $g^k \pmod p$ إذا عرفت g , k. على كل حال، إذا كان p عدداً كبيراً، فإنه من الصعب جداً إيجاد قيمة k حتى لو أُعطيت قيمة $g^k \pmod p$. إن هذا الفصل يمكن استخدامه لإنشاء التعمية ذات المفتاح المعلن، نفس فكرة صعوبة تحليل الأعداد التي استخدمت لإنشاء نظام التعمية RSA في الفصل الثامن عشر. سنصف مثل هذا الإنشاء في التمرين 22.6.

تمارين

(٢٢,١) استخدم جداول الأدلة قياس 37 لإيجاد جميع الحلول للتطابقات التالية :

(a) $12x \equiv 23 \pmod{37}$ (c) $x^{12} \equiv 11 \pmod{37}$

(b) $5x^{23} \equiv 18 \pmod{37}$ (d) $7x^{20} \equiv 34 \pmod{37}$

(٢٢,٢) (a) أنشئ جدول أدلة قياس 17 باستخدام الجذر البدائي 3.

(b) استخدم جدولك لحل التطابق $4x \equiv 11 \pmod{17}$

(c) إستخدم جدولك لإيجاد جميع حلول التطابق $5x^6 \equiv 7 \pmod{17}$.

(٢٢,٣) (a) إذا حقق a , b العلاقة $ab \equiv 1 \pmod{p}$ ، كيف يرتبط الدليلان $\mathrm{I}(a)$, $\mathrm{I}(b)$ ببعضهما البعض؟

(b) إذا حقق a , b العلاقة $a+b \equiv 0 \pmod{p}$ ، كيف يرتبط الدليلان $\mathrm{I}(a)$, $\mathrm{I}(b)$ ببعضهما البعض؟

(c) إذا حقق a , b العلاقة $a+b \equiv 1 \pmod{p}$ ، كيف يرتبط الدليلان $\mathrm{I}(a)$, $\mathrm{I}(b)$ ببعضهما البعض؟

(٢٢,٤) (a) إذا كان k يقسم $p-1$. بيّن أن التطابق $x^k \equiv 1 \pmod{p}$ له بالضبط k حلاً مختلفاً قياس p .

(b) بشكل عام، ليكن لدينا التطابق $x^k \equiv a \pmod{p}$.أوجد طريقة سهلة لاستخدام القيم k , p والدليل $\mathrm{I}(a)$ لتحدد كم عدد حلول هذا التطابق.

(c) العدد 3 هو جذر بدائي قياس العدد الأولي 1987. كم عدد حلول التطابق $x^{111} \equiv 729 \pmod{1987}$ ؟ (مساعدة : $3^6 = 729$).

(٢٢,٥) اكتب برنامجاً يأخذ كمدخلات عدد أولي p ، جذر بدائي g للعدد p ، وعدد a ، ويعطي الدليل $\mathrm{I}(a)$ كمُخرج. استخدم برنامجك لعمل جدول أدلة للعدد الأولي $p=47$ والجذر البدائي $g=5$.

(٢٢,٦) في هذا التمرين نَصف نظام تعمية ذات مفتاح معلن يسمى نظام التعمية ElGamal، وهو مبني على صعوبة حل مسألة لوغاريتم منفصل. ليكن p عدداً أوليًّا كبيراً وليكن g جذراً بدائيًّا قياس p. السؤال هنا هو كيف ستتمكن "ألس" Alice من إنشاء مفتاح ومن ثم يرسل لها "بوب" Bob رسالة.

أول خطوة ستقوم بها "ألس" هي اختيار عدد k ليكون مفتاحها السري. هي ستحسب العدد $a \equiv g^k \pmod{p}$. ستقوم "ألس" بنشر هذا الرقم a ، والذي هو المفتاح العام الذي سيقوم "بوب" (أو أي أحد آخر) باستخدامه لإرسال رسالة لها.

الآن افرض أن "بوباً" يريد إرسال الرسالة m لـ "ألس" ، حيث m عدد بين 2 , $p-1$. هو سيختار بشكل عشوائي عدد r ويحسب العددين:

$$e_1 \equiv g^r \pmod{p} \quad , \quad e_2 \equiv m a^r \pmod{p}$$

"بوب" يرسل لـ "ألس" زوج الأعداد (e_1, e_2).

أخيراً، تحتاج "ألس" لفك الشيفرة.

في البداية سوف تستخدم مفتاحها السري k لحساب $c \equiv e_1^k \pmod{p}$. بعد ذلك ستحسب $u \equiv c^{-1} \pmod{p}$. [أي أنها توجد حل $cu \equiv 1 \pmod{p}$ في u ، باستخدام الطريقة الواردة في الفصل الثامن]، أخيراً، ستقوم "ألس" بحساب $v \equiv u e_2 \pmod{p}$. يمكننا تلخيص حسابات "ألس" بالصيغة:

$$v \equiv e_2 \cdot \left(e_1^k\right)^{-1} \pmod{p}$$

(a) بيّن أنه عندما تنهي "ألس" حساباتها فإن العدد v الذي تحسبه يساوي رسالة "بوب" m.

(b) بين أنه إذا قام شخص ما بمعرفة كيف يحل مسألة اللوغاريتم المنفصل للعدد الأولي p والأساس g ؛ فإنه سيستطيع قراءة رسالة "بوب".

(٢٢.٧) في هذا التمرين، استخدم نظام التعمية ElGamal الموضح في التمرين 22.6.

(a) يريد "بوب" استخدام مفتاح "ألس" العام $a = 22695$ للعدد الأولي $p = 163841$ والأساس $g = 3$ ليرسل لها الرسالة $m = 39828$. اختار "بوب" الرقم العشوائي ليكون $r = 129381$. احسب الرسالة المشفرة (e_1, e_2) التي أرسلها "بوب" لـ "ألس".

(b) افرض أن "بوب" أرسل نفس الرسالة لـ "ألس"، ولكنه اختار قيمة مختلفة للعدد r. هل ستكون الرسالة المشفرة نفسها؟

(c) اختارت "ألس" المفتاح السري $k = 278374$ للعدد الأولي $p = 380803$ والأساس $g = 2$. استلمت "ألس" الرسالة (تحتوي ثلاث رسائل منفصلة):

$$(61745, 206881), \quad (255836, 314674), \quad (108147, 350768)$$

من "بوب". فك شيفرة الرسالة وحولها إلى أحرف باستخدام الرقم مقابل الحرف المبين في الجدول الوارد في الفصل الثامن عشر.