Cossos finits

Llorenç Huguet Rotger
Josep Rifà Coma
Juan Gabriel Tena Ayuso

PID_00185088

UOC
Universitat Oberta de Catalunya

Índex

Introducció

Els cossos finits han estat estudiats des de fa segles per diversos matemàtics, en particular Evariste Galois (de fet, són també coneguts com a cossos de Galois), però és en els últims 50 anys quan l'interès per aquestes estructures ha conegut un creixement espectacular, a causa de les seves aplicacions en diversos camps d'indubtable interès per al món industrial i financer com són la criptografia o els codis correctors d'errors.

La teoria dels codis correctors d'errors tracta de preservar la qualitat de la informació quan és transmesa a través de canals susceptibles de sofrir pertorbacions, que introdueixen errors en el missatge transmès. Un codi corrector permet, dintre de certs límits, detectar i corregir tals errors. Aquesta teoria comparteix amb la criptografia finalitats (si els codis correctors tracten de defensar la informació de la degradació natural la criptografia tracta de defensarla dels atacs humans) i tècnics; en particular, diversos sistemes criptogràfics com els de McEliece i de Niederreiter, estan basats en codis correctors.

Anomenarem $\mathbb{F}_q$ un cos finit amb q elements (alguns autors utilitzen la notació $GF(q)$, de *Galois field* amb q elements). El present mòdul estudia aquesta estructura matemàtica, amb especial èmfasi en els aspectes computacionals de la seva aritmètica.

Objectius

En els materials didàctics d'aquest mòdul l'estudiant trobarà els continguts necessaris per a assolir els objectius següents:

1. Conèixer l'estructura additiva i multiplicativa d'un cos finit $\mathbb{F}_q$, de $q = p^m$ elements, on p és un nombre primer.
2. Saber calcular la taula d'equivalències polinomial-exponencial i saber calcular en un cos finit F_q donant els resultats en qualsevol de les dues representacions.
3. Saber reconeixer la complexitat computacional d'un càlcul en cossos finits.
4. Coneixer i saber aplicar els principals algorismes aritmètics en cossos finits.

1. Existència i propietats dels cossos finits

En aquest apartat es mostra per a quins valors de q existeix un cos finit $\mathbb{F}_q$ i com construir-lo explícitament, al mateix temps que s'estudien les seves propietats i estructura.

1.1. Existència i construcció de cossos finits

En primer lloc assenyalem el resultat del teorema 1.1.

Teorema 1.1 (Teorema de Wedderburn). Tot cos finit és commutatiu (és a dir, la seva multiplicació és commutativa).

Lectura recomanada

Sobre el teorema de Wedderburn podeu consultar l'obra de Lidl i Niederreiter (1997).

Definició 1.2 (Característica d'un cos). La característica d'un cos K és defineix com el mínim p dels enters positius n tals que $n \cdot 1 = 1+1+\cdots+1 = 0$ (suma de n còpies de 1), en què 0 és l'element neutre de la suma i 1 l'element neutre del producte en el cos K. Si tal p no existeix, com succeeix amb el cos dels nombres reals, diem que K té característica 0. En cas contrari p ha de ser un nombre primer (si $p = r \cdot s$, $1 < r,s < p$ es tindria que $0 = p \cdot 1 = (r \cdot 1)(s \cdot 1)$ i un dels dos factors hauria de ser zero, en contradicció amb la minimalitat de p) i el cos es diu de característica prima p.

Observació

Hi ha cossos infinits que no són commutatius, com és el cas del cos dels quaternions.

Un primer exemple de cos finit està determinat pel resultat següent.

Proposició 1.3. Per a tot nombre primer p el conjunt $\mathbb{Z}_p$ dels enters mòdul p, amb la suma i producte induïdes per les de $\mathbb{Z}$, constitueix un cos commutatiu.

Demostració: Recordem que el conjunt $\mathbb{Z}_p$ dels enters mòdul p és el conjunt de classes d'equivalència de nombre enters, en què dos enters x,y són equivalents si i només si són congruents mòdul p: $x \equiv i \pmod{p}$ (és a dir, $x - y$ és divisible per p). El conjunt $\mathbb{Z}_p$ té cardinal p i un conjunt de representants està determinat per $\mathbb{F}_p = \{0,1,\ldots,p-1\}$.

Les operacions $a+b \pmod p$ i $a \cdot b \pmod p$ (fer la suma o producte de a i b, en $\mathbb{Z}$, dividir el resultat per p i agafar el residu) dota a aquest conjunt d'estructura de cos: és obvi que $(\mathbb{F}_p,+)$ és un grup additiu, amb 0 com a element neutre i com a oposat de $a \in \mathbb{F}_p$ l'element $-a = p - a$. Pel que fa $(\mathbb{F}_p^* = \mathbb{F}_p - \{0\},\cdot)$ la multiplicació és commutativa, l'element 1 actua com a unitat i donat un element $a \in \mathbb{F}_p^*$ l'existència d'invers (i un mètode efectiu de calcular-lo) és dedueix de l'algorisme d'Euclides (el qual és descriurà a continuació): donat que a i p són coprimers entre si, existeixen elements $x,y \in \mathbb{Z}$ tals que $mcd(a,p) = 1 = ax+py$, i per tant en $\mathbb{F}_p$ (noteu que $p \equiv 0 \pmod p$) $ax \equiv 1 \pmod p$, aleshores l'element $x \pmod p$ és l'invers de a. ∎

Cos binari

Si $p = 2$, es té el cos amb dos elements $\mathbb{F}_2 = \{0,1\}$ base de la computació binària (les operacions de cos coincideixen amb les operacions lògiques *OR*-exclusiva (*XOR*) i *AND*).

L'algorisme d'Euclides (Euclides, llibre VII), que permet obtenir el màxim comú divisor d de dos nombres $a,b \in \mathbb{N}$, és un dels algorismes bàsics en matemàtica computacional. Una modificació –algorisme d'Euclides estès– permet obtenir d com a combinació lineal de a i b amb coeficients enters (identitat de Bezout):

$$d = ax + by \tag{1}$$

Exposem a continuació l'algorisme d'Euclides estès.

Algorisme 1.4.

1. Agafar, com a valors inicials,

   $a_0 := a$, $a_1 := b$, $x_0 := 1$, $x_1 := 0$, $y_0 := 0$, $y_1 := 1$.

2. Per a $i = 0,1,\cdots$, iterar les assignacions

   $a_i := q_{i+1}a_{i+1} + a_{i+2}$ (calculem el quocient q_{i+1} i el residu a_{i+2} de la divisió entre a_i i a_{i+1})

   $x_i := q_{i+1}x_{i+1} + x_{i+2}$ (a partir de x_i,x_{i+1} i q_{i+1}, calculem x_{i+2})

   $y_i := q_{i+1}y_{i+1} + y_{i+2}$ (a partir de y_i,y_{i+1} i q_{i+1}, calculem y_{i+2})

   fins a obtenir un residu $a_i = 0$.

3. Si a_{n+1} és el primer residu nul, aleshores $d = a_n, x = x_n, y = y_n$.

Exemple 1.1. Siguin $a = 256, b = 96$. Aplicant l'algorisme 1.4 s'obté: $a_2 = 64, a_3 = 32, a_4 = 0$, $x_2 = 1, x_3 = -1$, $y_2 = -2, y_3 = 3$. Aleshores $d = a_3 = 32 = 256(-1) + 96 \cdot 3$.

Exemple 1.2. Sigui $p = 7$, i el cos $\mathbb{F}_7 = \{0,1,2,3,4,5,6\}$. Per a $a = 3, b = 6$ és té $3 + 6 \equiv 2 \pmod 7$, $3 \cdot 6 \equiv 4 \pmod 7$ i $3^{-1} \equiv 5 \pmod 7$ (noteu que $1 = 3 \cdot 5 - 7 \cdot 2$).

Observació

L'algorisme 1.4 es pot aplicar també a dos polinomis $a(X),b(X)$ amb coeficients en un cos K. Vegeu l'exemple 1.3.

Exemple 1.3. Calculeu el màxim comú divisor $mcd(P(X),Q(X))$ i expresseu el resultat com a combinació dels polinomis inicials $P(X)$ i $Q(X)$, en què $P(X)$ i $Q(X)$ són polinomis amb coeficients en $\mathbb{F}_3$: $P(X) = X^7 + 2X^2 + X + 1$; $Q(X) = X^3 + 2X^2$.

L'aplicació de l'algorisme d'Euclides estès ens dóna:

$a_0 = X^7 + 2X^2 + X + 1$; $a_1 = X^3 + 2X^2$; $a_2 = X + 1$; $a_3 = 1$; $a_4 = 0$
$q_1 = X^4 + X^3 + X^2 + X + 1$; $q_2 = X^2 + X + 2$
$x_0 = 1$; $x_1 = 0$; $x_2 = 2$; $x_3 = X^2 + X + 2$
$y_0 = 0$; $y_1 = 1$; $y_2 = 2X^4 + 2X^3 + 2X^2 + 2X + 2$; $y_3 = X^6 + 2X^5 + X^4 + X^3 + X^2$

O sigui que, $1 = mcd(P(X),Q(X))$ i, a més:

$(X^2 + X + 2)P(X) + (X^6 + 2X^5 + X^4 + X^3 + X^2)Q(x) = 1$

Determinem ara per a quins altres valors de q diferents dels primers, existeix un cos finit amb q elements.

Proposició 1.5. Sigui $K = \mathbb{F}_q$ un cos finit amb q elements, amb element neutre per a l'addició 0_K i element unitat per a la multiplicació 1_K. Existeix un primer p tal que K conté al cos $\mathbb{F}_p$ dels enters mòdul p.

Demostració: El cos K no pot tenir característica 0 (en cas contrari contindria el conjunt infinit $\{1_K, 2 \cdot 1_K, \cdots, n \cdot 1_K, \cdots\}$). K és, doncs de *característica* prima p i conté el subcos $\{0_K, 1_K, 2 \cdot 1_K, \cdots (p-1) \cdot 1_K\}$ isomorf al cos $\mathbb{F}_p$ dels enters mòdul p.∎

Corol·lari 1.6. Sigui $\mathbb{F}_q$ un cos de característica p. Existeix un enter positiu m tal que $q = p^m$.

Demostració: $\mathbb{F}_q$ admet una estructura d'espai vectorial sobre el seu subcos $\mathbb{F}_p$, Sigui m la seva dimensió (òbviament finita). Fixada una base qualsevulla d'aquest espai vectorial, $\mathbb{F}_q$ s'identifica amb el conjunt de vectors $\mathbb{F}_p^m$, conjunt amb cardinal p^m. ∎

El resultat anterior mostra que el cardinal d'un cos finit és sempre potència d'un nombre primer. El teorema següent mostra que per a qualsevulla potència d'un primer existeix un cos finit amb aquest cardinal i que tal cos és essencialment únic.

Cos $\mathbb{C}$

El cos $\mathbb{C}$ dels nombres complexos conté les arrels de tot polinomi amb coeficients en el cos $\mathbb{Q}$ dels nombres racionals. No obstant això, $\mathbb{C}$ no és una clausura algebraica de $\mathbb{Q}$ ja que no és compleix la condició de minimalitat. La clausura és un subcos de $\mathbb{C}$ denominat *cos dels nombres algebraics*.

Definició 1.7 (Clausura algebraica). Sigui K un cos. *La clausura algebraica* de K és un cos que conté K, tal que tot polinomi amb coeficients en K té totes les seves arrels en ell i és minimal amb aquesta propietat. Tal clausura existeix i és única, tret d'isomorfismes.

Teorema 1.8. Per a tot primer p i tot nombre natural m existeix un cos finit amb $q = p^m$ elements. Tal cos és únic tret d' isomorfismes.

Demostració: Sigui $\mathbb{F}_p$ el cos amb p elements i el polinomi definit sobre aquest cos: $F(X) = X^q - X$. Sigui R el conjunt de les q arrels de $F(X)$ en una certa clausura algebraica de $\mathbb{F}_p$ (no ho confongueu amb les arrels complexes de tal polinomi, noteu que $\mathbb{F}_p$ no està contingut en els complexos). Tals arrels són distintes (el polinomi $F(X)$ no té arrels múltiples, ja que la seva derivada no és nul·la: $F'(X) = qX^{q-1} - 1 \equiv -1 \pmod{p}$) i per tant R té cardinal q.

Ara bé R és un cos: siguin $\alpha,\beta \in R$, és a dir $\alpha^q = \alpha$, $\beta^q = \beta$. Òbviament aleshores $(\alpha \cdot \beta)^q = \alpha \cdot \beta$ i (suposant $\beta \neq 0$) $(\alpha/\beta)^q = \alpha/\beta$. Però tenint en compte que a $\mathbb{F}_p$, $q \equiv 0$, també $(\alpha \pm \beta)^q = \alpha \pm \beta$ (ja que tots els altres membres del desenvolupament de $(a+b)^q$ són múltiples de p), aleshores la suma, diferència, producte i quocient d'elements de R són a R.

Sigui K un altre cos amb q elements. El grup multiplicatiu $K^* = K - \{0\}$ té cardinal $q-1$ i per tant tot element $a \in K^*$ verifica $a^{q-1} = 1_K$, aleshores $a^q = a$, equació que òbviament també verifica O_K. És a dir, els q elements de K són arrels de $X^q - X$ i per tant K es pot identificar amb R. ∎

Habitualment en criptografia s'utilitzen els dos tipus de cos següents:

1) cossos binaris $\mathbb{F}_{2^m}$, amb 2^m elements.

2) cossos $\mathbb{F}_{p^m}$, amb p^m elements i p primer (habitualment molt gran).

El teorema 1.8 demostra l'existència d'un cos finit amb q elements, però no en dóna una construcció explícita. El mètode següent proporciona tal construcció, que és formalment anàloga a la de del cos $\mathbb{F}_p$ com a classes d'equivalència dels enters mòdul p.

Sigui $f(X) = X^m + f_{m-1}X^{m-1} + \cdots + f_1X + f_0 \in \mathbb{F}_p[X]$ un polinomi mònic (coeficient del terme de major grau igual a 1) i irreductible, amb coeficients en $\mathbb{F}_p$. En l'anell de polinomis $\mathbb{F}_p[X]$ considerem el conjunt de les seves classes d'equivalència mòdul $f(X)$. Un conjunt de representants d'aquestes classes està determinat pel conjunt K dels $q = p^m$ polinomis $a_0 + a_1X + \cdots + a_{m-1}X^{m-1} \in \mathbb{F}_p[X]$ de grau més petit que m (ja que tot $g(X) \in \mathbb{F}_p[X]$ és equivalent al polinomi residu de la seva divisió per $f(X)$).

Si denotem $\alpha \in K$ en la classe d'equivalència de X, és a dir, $\alpha \equiv X \pmod{f(X)}$, podem identificar l'element $a_0 + a_1X + \cdots + a_{m-1}X^{m-1}$ amb $a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$ i a K amb el conjunt d'aquestes expressions.

Noteu que $\alpha^m + f_{m-1}\alpha^{m-1} + \cdots + f_1\alpha + f_0 \equiv 0_K$ i per tant α es pot considerar com una arrel del polinomi $f(X)$ a K. Aleshores tenim:

Teorema 1.9. El conjunt K amb les operacions suma i producte en $\mathbb{F}_p[\alpha]$ induïdes per la suma i el producte de polinomis en $\mathbb{F}_p[X]$ és un cos amb q elements.

Demostració: El raonament és totalment anàleg al de la proposició 1.3 i els detalls és deixen com a exercici. En particular, l'invers d'un element no nul s'obté utilitzant l'algorisme d'Euclides estès per a polinomis. ∎

Nota

S'ha comentat que α es pot considerar com a arrel de $f(X)$. Atès que aquest polinomi de grau m té m arrels és pot plantejar quina d'aquestes és α. No obstant això, a diferència del que succeeix amb les arrels d'un polinomi amb coeficients racionals, les quals es poden individualitzar i tenen un valor concret (real o complex), això no passa en cossos finits. L'element α es pot considerar com un símbol, que s'agafa com a arrel de $f(X)$; una vegada fixada aquesta arrel, les restants es poden expressar en funció de α (vegeu l'exemple següent).

Exemple 1.4. Considerem el polinomi irreductible $X^3 + X + 1 \in \mathbb{F}_2[X]$, i sigui α una arrel. Les altres dues arrels són: α^2 i $\alpha^2 + \alpha$. Un cos amb 8 elements estaria format pels elements:

$$\mathbb{F}_8 = \{0,1,\alpha,1+\alpha,\alpha^2,1+\alpha^2,\alpha+\alpha^2,1+\alpha+\alpha^2\} \quad (2)$$

amb les taules d'addició i multiplicació següents:

+	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
1	1	0	$1+\alpha$	α	$1+\alpha^2$	α^2	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$
α	α	$1+\alpha$	0	1	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	α^2	$1+\alpha^2$
$1+\alpha$	$1+\alpha$	α	1	0	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α^2
α^2	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	0	1	α	$1+\alpha$
$1+\alpha^2$	$1+\alpha^2$	α^2	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	1	0	$1+\alpha$	α
$\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	α^2	$1+\alpha^2$	α	$1+\alpha$	0	1
$1+\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α^2	$1+\alpha$	α	1	0

·	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
1	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
α	α	α^2	$\alpha+\alpha^2$	$1+\alpha$	1	$1+\alpha+\alpha^2$	$1+\alpha^2$
$1+\alpha$	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$	α^2	1	α
α^2	α^2	$1+\alpha$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	α	$1+\alpha^2$	1
$1+\alpha^2$	$1+\alpha^2$	1	α^2	α	$1+\alpha+\alpha^2$	$1+\alpha$	$\alpha+\alpha^2$
$\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	1	$1+\alpha^2$	$1+\alpha$	α	α^2
$1+\alpha+\alpha^2$	$1+\alpha+\alpha^2$	α	1	$\alpha+\alpha^2$	α^2	α^2	$1+\alpha$

Nota

En l'exemple anterior s'ha construït un cos amb 8 elements utilitzant el polinomi irreductible $X^3+X+1 \in \mathbb{F}_2[X]$. Però una construcció anàloga es podria obtenir a partir d'una

arrel β del polinomi $X^3+X^2+1 \in \mathbb{F}_2[X]$, el qual és també irreductible (en realitat, tret del cas per a $p=m=2$ en què l'únic polinomi irreductible és X^2+X+1, sempre existeix més d'un polinomi irreductible de grau m). En aquesta altra construcció s'obtindrien taules additiva i multiplicativa aparentment diferents.

No obstant això, el teorema 1.8 garanteix que només existeix un cos amb 8 elements. Quina és l'explicació d'aquesta aparent contradicció? En realitat és un simple problema d'*etiquetatge* dels elements: en concret és pot comprovar que l'assignació $\alpha \to \beta' = 1+\beta$ s'estén a un isomorfisme entre tots dos cossos (les taules per a α i β' són iguals).

1.2. Estructura additiva i multiplicativa d'un cos finit

El cos finitamb $\mathbb{F}_q$ té dos grups abelians, $(\mathbb{F}_q,+)$ y $(\mathbb{F}_q^*,\cdot)$. L'estructura d'aquests grups és particularment simple.

Teorema 1.10 (Estructura additiva). Si $q = p^m$, el grup additiu $(\mathbb{F}_q,+)$ és un producte directe de m grups cíclics d'ordre p:

$$(\mathbb{F}_q,+) \simeq \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}. \qquad (3)$$

Demostració: Com s'ha indicat $(\mathbb{F}_q,+)$ és un espai vectorial sobre el seu subcos primer $\mathbb{F}_p$. Qualsevulla base d'aquest espai (per exemple, una base del tipus $\{1,\alpha \cdots ,\alpha^{m-1}\}$ utilitzada en el teorema 1.9 indueix l'isomorfisme indicat. ∎

1.2.1. Representació additiva

En virtut del teorema 1.10 els elements de $\mathbb{F}_q$ es poden representar com a vectors m-dimensionals amb coeficients en $\mathbb{F}_p$, És a dir, expressions de la forma $(a_1,a_2,\ldots,a_m)$ amb $a_i \in \{0,1,\ldots,p-1\}$. Així, per exemple, els elements de $\mathbb{F}_8$ es poden identificar amb el conjunt de triples binàries $\{(i,j,k)\}|i,j,k \in \{0,1\}$, la qual cosa proporciona una manera adequada de transmetre els elements d'aquest cos a través d'un canal binari.

En aquesta forma additiva els elements es poden sumar (sumant coordenada per coordenada mòdul p) o multiplicar-se escalarment per un element de $\mathbb{F}_p$.

Per a estudiar l'estructura multiplicativa, recordem que donat un grup abelià finit $(G,\cdot)$, anomenarem ordre de $x \in G$ l'ordre del subgrup generat per x, és a dir, $ord(x) = \min\{n \mid x^n = 1\}$ i exponent de G $exp(G) = mcm\{ord(x) \mid x \in G\}$.

Lema 1.11. Si $(G,\cdot)$ és un grup abelià finit d'exponent n, aleshores existeix un element $x \in G$ d'ordre n.

Demostració: Sigui $n = p_1^{e_1} \cdots p_m^{e_m}$ la descomposició de n en factors primers. Com $p_i^{e_i}$ apareix en la factorització, existeix $x_i \in G$ d'ordre $k_i p_i^{e_i}$ per a un cert enter natural k_i. Aleshores l'element $x_i^{k_i}$ tindrà ordre $p_i^{e_i}$ i per tant $x = \prod_{i=1}^{m} x_i^{k_i}$ tindrà ordre exactament n. ∎

Teorema 1.12 (Estructura multiplicativa). El grup multiplicatiu $(\mathbb{F}_q^*, \cdot)$ és cíclic d'ordre $q-1$.

Demostració: Sigui n l'exponent de $\mathbb{F}_q^*$. En virtut del lemma anterior ha d'existir un element d'ordre n. Per tant $n \leq q-1 = \#\mathbb{F}_q^*$. Per altra banda, per ser n múltiple de l'ordre de tot element, els $q-1$ elements de $\mathbb{F}_q^*$ satisfan l'equació $x^n - 1 = 0$, amb la qual cosa $q-1 \leq n$ i finalment $n = q-1$.

Atès que hi ha un element d'ordre $q-1$, el grup és cíclic. ∎

Definició 1.13 (Element primitiu). Anomenarem *element primitiu* de $\mathbb{F}_q$ un generador del grup cíclic $(\mathbb{F}_q^*, \cdot)$.

Nota

La noció d'element primitiu en el context d'un grup cíclic finit d'ordre n i la notació $\varphi(n)$ per al nombre de tals elements primitius es pot trobar en el mòdul 5 del curs *Criptografia* de la UOC. Aquest nombre és important en matemàtiques i serà utilitzat en altres parts d'aquest curs; per això donem a continuació la definició i algunes de les propietats.

Definició 1.14 (Funció d'Euler). Per a tot nombre natural n es denota $\varphi(n)$ el nombre d'elements a; $0 < a < n$ tals que $mcd(a,n) = 1$. Aquesta funció és denominada *funció d'Euler*.

Proposició 1.15. La funció d'Euler verifica les propietats següents:

1) Si p és un nombre primer, $\varphi(p) = p-1$.

2) Si p és un nombre primer i r un nombre natural, $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

3) Si m,n són nombres naturals primers entre si (és a dir, $mcd(m,n) = 1$), $\varphi(mn) = \varphi(m)\varphi(n)$.

La demostració és senzilla i es deixa com a exercici.

Corol·lari 1.16. Sigui $n = p_1^{r_1} \dots p_s^{r_s}$ la factorització en primers del nombre natural n. Aleshores:

$$\varphi(n) = n \cdot \prod_i (1 - 1/p_i) \tag{4}$$

El corol·lari 1.16 mostra que el càlcul de $\varphi(n)$ és fàcil si es coneix la factorització de n. Per contra, sense conèixer tal factorització, aquest càlcul és un problema computacionalment ineficient.

1.2.2. Representació multiplicativa

En virtut del teorema 1.12, si α és un element primitiu de $\mathbb{F}_q$, aleshores $\mathbb{F}_q^* = \{\alpha^i \mid i = 1, \dots, q-1\}$. Aquesta representació serà fonamental en els sistemes criptogràfics basats en el problema del logaritme discret.

Exemple 1.5. Per a $q = 11$, $\alpha = 2$ és un element primitiu de $\mathbb{F}_{11}^*$.

Exemple 1.6. Igual que en l'exemple 1.4, considerem el polinomi irreductible $X^3 + X + 1 \in \mathbb{F}_2[X]$, i sigui α una arrel.

Per a saber si α és un element primitiu en $\mathbb{F}_8$ n'hauríem de calcular l'ordre i veure si és màxim. O sigui, si el menor enter positiu r tal que $\alpha^r = 1$ és $r = q - 1 = 7$.

Sabem que $\alpha^3+\alpha+1 = 0$, o sigui, $\alpha^3 = \alpha+1$. Aleshores, $\alpha^4 = \alpha^2+\alpha$; $\alpha^5 = \alpha^3+\alpha^2 = \alpha^2+\alpha+1$; $\alpha^6 = (\alpha^3)^2 = \alpha^2 + 1$ i $\alpha^7 = \alpha^3 + \alpha = 1$.

En aquest cas, α és un element primitiu i la taula d'equivalències entre la representació vectorial (o polinòmica) i exponencial és:

Exponencial	Vectorial	Polinomial
0	(0,0,0)	0
α^0	(1,0,0)	1
α^1	(0,1,0)	α
α^2	(0,0,1)	α^2
α^3	(1,1,0)	$1 + \alpha$
α^4	(0,1,1)	$\alpha + \alpha^2$
α^5	(1,1,1)	$1 + \alpha + \alpha^2$
α^6	(1,0,1)	$1 + \alpha^2$

Observació

No es coneix cap algorisme computacionalment eficient per al càlcul d'un element primitiu, ni tan sols per al cas dels cossos $\mathbb{F}_p$, p primer.

Observació

Noteu que quan hem escrit un polinomi com a vector, utilitzant els coeficients de la seva expressió additiva, hem començat pel terme de grau zero com a primera coordenada.

2. Bases de cossos finits

Com s'ha indicat, els elements de $\mathbb{F}_q$, $q = p^m$ es poden expressar com a combinació lineal, amb coeficients en $\mathbb{F}_p$ dels elements d'una base. Des d'un punt de vista computacional, hi ha dos tipus de bases que són especialment importants.

Definició 2.1 (Base polinòmica). Es denomina base polinòmica del cos $\mathbb{F}_q$ una base del tipus $\{1,\alpha \cdots ,\alpha^{m-1}\}$, amb α arrel d'un polinomi mònic i irreductible amb coeficients en $\mathbb{F}_p$.

El nombre de bases polinòmiques de $\mathbb{F}_q$ serà, doncs, igual al nombre de polinomis mònics i irreductibles de grau m amb coeficients en $\mathbb{F}_p$. Tal nombre es pot determinar explícitament.

Proposició 2.2. $X^q - X$ és el producte de tots els polinomis irreductibles sobre $\mathbb{F}_p$ tals que el seu grau divideix m.

Demostració: Sigui $g(X) \in \mathbb{F}_p[X]$ un polinomi mònic i irreductible de grau $d|m$. És a dir, $m = dd'$. En virtut del teorema 1.9 les arrels de $g(X)$ determinen un cos amb $\mathbb{F}_{p^d}$ elements i, per tant, pel teorema 1.8, són arrels de $X^{p^d} - X$; aleshores $g(X)$ divideix $X^{p^d} - X$. Així es té $p^m - 1 = (p^d - 1)(p^{d(d'-1)} + p^{d(d'-2)} + \cdots p^d + 1)$ és a dir, $p^d - 1$ divideix $p^m - 1$. Un raonament anàleg amb X en lloc de p, mostra que $X^{p^d-1} - 1$ divideix $X^{p^m-1} - 1$ i aleshores $X^{p^d} - X$ i per tant $g(X)$ divideix $X^q - X$.

Recíprocament, un raonament similar prova que si $g(X)$ és un polinomi mònic i irreductible que divideix $X^q - X$, el seu grau és un divisor de m. ∎

Corol·lari 2.3. Si designem per $N_p(d)$ el nombre de polinomis irreductibles de grau d sobre $\mathbb{F}_p$, aleshores,

$$q = \sum_{d|m} dN_p(d). \tag{5}$$

El nombre cercat $N_p(m)$ figura com a sumand en l'expressió anterior. Vegem com obtenir-lo.

Definició 2.4 (Funció de Moebius). Anomenarem *funció de Moebius* la funció de variable natural, $\mu : \mathbb{N} \longrightarrow \{-1,0,1\}$ definida de la forma següent:

Si $n \in \mathbb{N}$ i $n = \prod_{i=1}^{s} p_i^{e_i}$ és la seva descomposició en factors primers, aleshores

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1; \\ 0 & \text{si } e_i \geq 2 \text{ per a algún valor de } i; \\ (-1)^s & \text{si } e_i = 1 \text{ per a tot valor de } i. \end{cases} \tag{6}$$

Lema 2.5. Si $n \in \mathbb{N}$, es verifica que

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1; \\ 0 & \text{si } n > 1. \end{cases} \tag{7}$$

Demostració: El cas $n = 1$ és trivial. Suposem ara que $n > 1$ i siguin $p_1, p_2, \ldots, p_s$ els diferents divisors primers de n. Tenint en compte la definició de la funció de Moebius,

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{s} \mu(p_i) + \sum_{1 \leq i < j \leq s} \mu(p_i p_j) + \cdots + \mu(p_1 p_2 \ldots p_s) \\ &= 1 + \binom{s}{1}(-1) + \binom{s}{2}(-1)^2 + \cdots + \binom{s}{s}(-1)^s \\ &= (1-1)^s = 0. \end{aligned}$$

∎

Lema 2.6 (Fórmula d'inversió de Moebius). Sigui f una funció de variable natural amb valors en un grup abelià. Per a $n \in \mathbb{N}$ definim $g(n)$ mitjançant

$$g(n) = \sum_{d|n} f(d). \tag{8}$$

Es verifica que

$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) g(d). \tag{9}$$

Demostració:

$$\begin{aligned} \sum_{d|n} \mu(d) g(\frac{n}{d}) &= \sum_{d|n} \mu(d) \sum_{e|(n/d)} f(e) \\ &= \sum_{e|n} \sum_{d|(n/e)} \mu(d) f(e) \\ &= \sum_{e|n} f(e) \sum_{d|(n/e)} \mu(d) \\ &= f(n). \end{aligned}$$

en què en l'última igualtat hem tingut en compte el lema 2.5. ∎

Teorema 2.7. El nombre de polinomis irreductibles de grau m sobre $\mathbb{F}_p$ és:

$$N_p(m) = \frac{1}{m} \sum_{d|m} \mu(d) p^{m/d} = \frac{1}{m} \sum_{d|m} \mu(\frac{m}{d}) q^d. \tag{10}$$

Demostració: N'hi ha prou aplicant la fórmula d'inversió de Moebius a la funció $f(m) = mN_p(m)$. ∎

Exemple 2.1. Per a $p = 2$ el nombre de polinomis de grau m és:

1) 1 si $m = 2$. El polinomi: $X^2 + X + 1$.

2) 2 si $m = 3$. Els polinomis: $X^3 + X + 1$ i $X^3 + X^2 + 1$.

3) 3 si $m = 4$. Els polinomis: $X^4 + X + 1$, $X^4 + X^3 + 1$ i $X^4 + X^3 + X^2 + X + 1$.

4) etc.

Observació

Un polinomi irreductible de grau m es pot obtenir agafant polinomis arbitraris i aplicant-los un *test d'irreductibilitat* (Lidl i Niederreiter, 1997). El valor $N_p(m)$ donat pel teorema 2.7 proporciona una estimació de la probabilitat d'èxit d'aquesta cerca aleatòria.

Definició 2.8 (Base normal). S'anomena base normal de $\mathbb{F}_q$ una base del tipus $\{\alpha,\alpha^p,\cdots,\alpha^{p^{m-1}}\}$ amb $\alpha \in \mathbb{F}_q$.

Com es veurà en l'apartat següent, les bases normals són molt eficients per al càlcul de l'exponenciació en $\mathbb{F}_q$, operació bàsica en els algorismes criptogràfics basats en el problema del logaritme discret. Per a tenir una base normal és necessari un element α tal que les seves potències p-èsimes successives siguin linealment independents.

Exemple 2.2. Sigui $q = 8 = 2^3$, α arrel del polinomi irreductible,

- $X^3 + X + 1$. En aquest cas $\{\alpha,\alpha^2,\alpha^4\}$ no és base normal (ja que ni tan sols és base, ja que els tres elements són linealment dependents).
- $X^3 + X^2 + 1$. En aquest cas $\{\alpha,\alpha^2,\alpha^4\}$ és base normal.

En general, no és òbvia l'existència d'un element α que generi una base normal. No obstant això, tenim el teorema 2.9.

Lectura recomanada

Sobre el teorema de la base normal podeu veure l'obra de Lidl i Niederreiter (1997) o la de Menezes (1993).

Teorema 2.9 (Teorema de la base normal). Existeix una base normal per a tot cos finit.

Avaluem el nombre de bases normals. Suposem fixada una tal base normal $\mathcal{B} = \{\alpha,\alpha^p,\ldots,\alpha^{p^{m-1}}\}$ (la seva existència la garanteix el teorema 2.9). Un canvi de base de $\mathcal{B}$ a una nova base $\mathcal{B}' = \{\beta_0,\beta_1,\ldots,\beta_{m-1}\}$ està determinat per una matriu $m \times m$ invertible $C = (c_{ij})$, $c_{ij} \in \mathbb{F}_p$.

Observació

Començar amb 0 els subíndexs dels elements de la base $\mathcal{B}'$ i dels components de la matriu circulant és per coherència amb els exponents de la base normal $\mathcal{B}$: $p^0,p^1,\ldots,p^{m-1}$.

Vegem quina condició ha de complir C perquè la nova base $\mathcal{B}'$ sigui també normal.

Definició 2.10 (matriu circulant). S'anomena *matriu circulant* (amb coeficients en un cos o en un anell) una matriu del tipus:

$$[a_0,a_1,\ldots,a_{m-1}] = \begin{pmatrix} a_0 & a_1 & \ldots & a_{m-1} \\ a_{m-1} & a_0 & \ldots & a_{m-2} \\ . & . & . & . \\ . & . & . & . \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}. \qquad (11)$$

És a dir, la matriu queda determinada per la seva primera fila, ja que les següents es dedueixen cadascuna de l'anterior mitjançant una permutació cíclica dels seus elements que desplaça cada coordenada una posició a la dreta.

Teorema 2.11. La base $\mathcal{B}'$ és normal si i només si la matriu C de canvi de base és circulant.

Demostració: Suposem que la matriu és circulant, és a dir, $C = [a_0, a_1, \ldots, a_{m-1}]$ la qual cosa implica que $c_{ij} = a_{j-i}$; aleshores,

$$\beta_i = \sum_j a_{j-i}\alpha^{p^j} = \left(\sum_j a_{j-i}\alpha^{p^{j-i}}\right)^{p^i} = \left(\sum_j a_j\alpha^{p^j}\right)^{p^i} = \beta_0^{p^i}$$

mostra que la base $\mathcal{B}'$ és normal.

Si recíprocament suposem $\mathcal{B}'$ normal, sigui $\beta_0 = \sum_j c_{0j}\alpha^{p^j}$. Aleshores:

$$\beta_i = \beta_0^{p^i} = \sum_j c_{0j}\alpha^{p^{i+j}} = \sum_j c_{0,j-i}\alpha^{p^j} \qquad (12)$$

però també (per definició) $\beta_i = \sum_j c_{ij}\beta^{p^j}$, la qual cosa mostra que la matriu C és circulant. ∎

El nombre de bases normals del cos $\mathbb{F}_q$ serà, doncs, igual al nombre de matrius $m \times m$ circulants i invertibles amb coeficients en $\mathbb{F}_p$.

Lectura recomanada

Per a la determinació del nombre de bases normals del cos $\mathbb{F}_q$ vegeu l'obra de Lidl i Niederreiter (1997).

3. Computació en cossos finits

El propòsit d'aquest apartat és mostrar com es poden fer, amb els elements d'un cos finit $\mathbb{F}_q$, les operacions aritmètiques habituals i quin és el seu cost computacional.

3.1. Aritmètica en cossos finits

Tal com s'ha indicat en el teorema 1.10, fixada una base de $\mathbb{F}_q$ sobre $\mathbb{F}_p$, tot element $a \in \mathbb{F}_q$ es pot representar com un vector de la forma $a = (a_1, a_2, \ldots, a_m)$, amb $a_i \in \{0, 1, \ldots, p-1\}$. L'addició o substracció de dos elements a, b es fa sumant o restant coordenada per coordenada i reduint el resultat mòdul p.

3.1.1. Multiplicació

Fixada una base qualsevulla $\mathcal{B} = \{v_1, v_2, \ldots, v_m\}$ i dos elements de $\mathbb{F}_q$: $a = a_1v_1 + a_2v_2 + \cdots + a_mv_m$, $b = b_1v_1 + b_2v_2 + \cdots + b_mv_m$ (que podem identificar amb els vectors $a = (a_1, a_2, \cdots, a_m)$, $b = (b_1, b_2, \cdots, b_m)$), tenim:

$$c = a \cdot b = (\sum_i a_i v_i)(\sum_j b_j v_j) = \sum_{ij} a_i b_j (v_i v_j) = \sum_{ij} a_i b_j (\sum_k t_{ij}^k v_k) \qquad (13)$$

Aleshores, denotant $T_k = (t_{ij}^k)$, $k = 1, 2, \ldots, m$, es tenen m matrius $m \times m$ anomenades *taules de multiplicació*. Si $c = c_1v_1 + c_2v_2 + \cdots + c_mv_m$, les coordenades c_i estan determinades per l'equació matricial:

$$c_k = aT_kb^t. \qquad (14)$$

Observació

En l'equació 14 la b^t denota el vector transposat del b (en aquest cas un vector escrit verticalment).

Les taules de multiplicació determinen, doncs, el producte. Aquest es pot implementar tant en programari, emmagatzemant les m taules, com en maquinari específic, que consta de m circuits, cadascun dels quals dóna com a sortida a les entrades $a, b \in \mathbb{F}_q$ un component c_k del producte.

Usualment s'usen bases particulars, com les polinòmiques o les normals, ja descrites. Vegem-ne ara algunes característiques:

- **Base polinòmica**: sigui $\{1, \alpha, \cdots, \alpha^{m-1}\}$, amb α arrel del polinomi (mònic i irreductible) $f(X)$. En aquest cas, donats $a = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$ i $b = b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1}$, el càlcul de $a \cdot b$ implica dues operacions:

1) Multiplicació de a i b com si fossin polinomis en X.

2) Reducció del polinomi obtingut, de grau com a màxim $2m-2$, mòdul $f(X)$ (és a dir, fer la divisió euclídiana per $f(X)$ i agafar el residu de la divisió).

Exemple 3.1. Sigui el cos $\mathbb{F}_8$ i α arrel de $f(X) = X^3 + X + 1$ i els elements $a = 1 + \alpha^2$, $b = 1 + \alpha$.

1) El producte dels polinomis $a(X) = X^2 + 1$ i $b(X) = X + 1$ dóna com a resultat el polinomi $c(X) = X^3 + X^2 + X + 1$.

2) La divisió de $c(X)$ per $f(X)$ dóna de residu X^2.

Aleshores, $a \cdot b = \alpha^2$.

- **Base normal**: si s'utilitza una base normal $\mathcal{B} = \{\alpha_0 = \alpha, \alpha_1 = \alpha^p, \ldots, \alpha_{m-1} = \alpha^{p^{m-1}}\}$, les m taules de multiplicació $T_k = (t_{ij}^k)$ verifiquen la relació següent:

Lema 3.1. Per a $0 < l \leq m-1$ tenim que $t_{ij}^l = t_{i-l,j-l}^0$. És a dir, la taula T_l es dedueix de la T_0 per desplaçament de l posicions en files i columnes.

Demostració: Per definició de les taules $\alpha_i\alpha_j = \sum_k t_{ij}^k \alpha_k$. Elevant tots dos membres a p^{-l} tenim que $\alpha_i^{p^{-l}}\alpha_j^{p^{-l}} = \alpha_{i-l}\alpha_{j-l} = \sum_k t_{ij}^k \alpha_{k-l}$. Però, per definició, $\alpha_{i-l}\alpha_{j-l} = \sum_k t_{i-l,j-l}^k \alpha_k$. Igualant els coeficients de α_0 en totes dues expressions s'obté el resultat. ∎

En conseqüència, si es té un algorisme (o en maquinari, un circuit electrònic) per a calcular la primera coordenada c_0 del producte dels elements $a,b \in \mathbb{F}_q$ l'algorisme o circuit mateix calcula la coordenada c_l amb les coordenades de a i b desplaçades l posicions.

3.1.2. Divisió

La divisió de dos elements $a,b \in \mathbb{F}_q$, $b \neq 0$ implica la multiplicació de a per l'invers de l'element$b$. Si s'usa una base polinòmica, aquest invers es pot computar utilitzant l'algorisme d'Euclides 1.4 per a polinomis.

Exemple 3.2. Sigui $f(X) = X^3 + X + 1$, $b = 1 + \alpha^2$. L'algorisme d'Euclides proporciona $a_2 = 1, a_3 = 0$, $x_2 = 1$, $y_2 = X$, i per tant $1 = f(X) \cdot 1 + (X^2 + 1)X$, i aleshores $b^{-1} = \alpha$.

3.1.3. Exponenciació

Càlculs del tipus $a^n \pmod m$, amb $a,n,m \in \mathbb{Z}$ (o bé del tipus a^n, $a \in \mathbb{F}_q$, $n \in \mathbb{N}$), són una eina fonamental en els sistemes criptogràfics basats en el problema del

logaritme discret i en altres camps com els tests de primalitat*. En principi, es podria fer aquest càlcul multiplicant a per si mateix n vegades i posteriorment reduir mòdul m el resultat obtingut. Ara bé, per a n gran, un càlcul del tipus anterior seria impracticable per dues raons:

* També necessaris en el sistema criptogràfic RSA; vegeu l'obra de Koblitz (1994).

1) El nombre excessiu de multiplicacions.

2) Els càlculs intermedis d'aquestes multiplicacions proporcionen nombres de mida creixent, que superen la capacitat d'emmagatzematge de l'ordinador.

Hi ha un algorisme (*multiplicació i elevació al quadrat*) que permet evitar aquests dos inconvenients:

Sigui $n = s_0 + s_1 2 + \cdots s_{k-1} 2^{k-1}$ l'expressió binària de n i sigui $b := 1$,

Algorisme 3.2 (**Multiplicar i elevar al quadrat**).

Des de $j = k - 1$ fins a 0

Si $s_j = 1$ aleshores $b := b \cdot a \pmod{m}$.

Si $j > 0$ aleshores $b := b^2 \pmod{m}$.

Final des de

El resultat és $a^n = b \pmod{m}$.

Exemple 3.3. Siguin $a = 3, m = 5, n = 67$. Tenint en compte que en base 2, $67 = 1000011$, executant les etapes de l'algorisme anterior s'obté $3^{67} \equiv 2 \pmod{5}$.

Notes

1) L'algorisme es pot adaptar a l'expressió de l'exponent n en una altra base diferent de 2 (per exemple, per a la base 3 es tindria un algorisme en què en lloc d'elevar al quadrat s'elevaria al cub).

2) La reducció mòdul m es pot substituir per *operació en un cos finit* $\mathbb{F}_q$. En particular per a $m = p$ primer, la reducció mòdul p és l'operació en el cos finit $\mathbb{F}_p$.

L'exponenciació es pot simplificar, especialment en el cas de cossos binaris, utilitzant bases normals. En efecte, es té:

Lema 3.3. Siguin $\{a_0, a_1, \ldots, a_{m-1}\}$ les coordenades d'un element $a \in \mathbb{F}_q$ en la base normal $\{\alpha, \alpha^p, \ldots, \alpha^{p^{m-1}}\}$. L'element a^p té per coordenades $(a_{m-1}, a_0, a_1, \ldots, a_{m-2})$.

Demostració: Tenint en compte que tots els altres membres del desenvolupament de $(a+b)^q$ són potència de p i, per tant, nuls en característica p, tenim que $a_i^p = a_i$ i que $\alpha^{p^n} = \alpha^q = \alpha$). Per tant:

$$(a_0\alpha+a_1\alpha^p+\cdots+a_{m-1}\alpha^{p^{m-1}})^p = a_0\alpha^p+a_1\alpha^{p^2}+\cdots+a_{m-1}\alpha^{p^m} = a_{m-1}\alpha+a_0\alpha^p+\cdots+a_{m-2}\alpha^{p^{m-1}}$$

∎

El lema anterior mostra que l'elevació a la potència p implica simplement una permutació circular dels coeficients, i per tant el seu cost computacional és menyspreable. Si $p = 2$ és l'elevació al quadrat, peça fonamental en l'algorisme 3.2, la qual té cost zero.

3.2. Complexitat de l'aritmètica en cossos finits

Vegem ara com podem obtenir una estimació del cost dels algorismes aritmètics descrits en un cos finit $\mathbb{F}_q$. La disciplina que estudia el cost dels algorismes i problemes matemàtics es denomina *teoria de la complexitat computacional*. Si volem mesurar la *quantitat* de computació necessària per a *executar* un algorisme, és necessària una unitat de mesura. Com que un ordinador redueix qualsevol càlcul a sumes binàries elementals, es pot agafar aquesta suma com a unitat.

Definició 3.4 (Operació bit). S'anomena *operació bit* l'addició de dos elements en el cos $\mathbb{F}_2$, és a dir, la suma binària (mod 2) de dos nombres iguals a 0 o 1 (bits).

Per a mesurar en operacions bit el *temps* o *quantitat* de computació d'un algorisme, la teoria de la complexitat computacional introdueix dues precisions:

1) El temps ha de ser funció de la *longitud* de les dades (*inputs*). Tals dades són sempre nombres naturals (o reduïbles a aquests: per exemple, un element d'un cos finit amb cardinal $q = p^m$ queda determinat per m nombres naturals menors que p).

2) El temps d'execució d'un algorisme, per a una longitud donada de les dades, varia en cada cas concret. S'adoptarà el criteri del *cas pitjor* agafant un fita vàlida per a tota instància particular d'aquesta mateixa longitud.

Definició 3.5 (Longitud binària d'un nombre). S'anomena longitud (binària) k d'un nombre natural n el nombre de dígits de la seva expressió en base 2. Aquesta longitud és el nombre natural k tal que $2^{k-1} \leq n < 2^k$, i per tant $k = \lfloor \log_2(n) \rfloor + 1$. Noteu que la longitud d'un nombre és també el nombre de bits de memòria necessaris per a emmagatzemar en un ordinador.

Definició 3.6 (Notació *O*). Donades f,g funcions en les variables naturals $k_1,k_2,\ldots,k_s$ i amb valors reals positius, es diu que f és de l'ordre de g ($f = O(g)$) si existeixen constants reals t,C tals que si $k_i > t$ per a tot i, $f(k_1,k_2,\ldots,k_s) < Cg(k_1,k_2,\ldots,k_s)$.

Definició 3.7 (Complexitat polinòmica). Un algorisme amb dades inicials els enters $n_1,n_2,\ldots,n_s$, de longituds $k_1,k_2,\ldots,k_s$, es diu de *complexitat polinòmica* si existeix un polinomi P en s variables tal que el *temps* d'execució de l'algorisme, mesurat en operacions bit, és $O(P(k_1,k_2,\ldots,k_s))$.

Com veurem, les operacions aritmètiques usuals en cossos finits, en particular les implicades en els algorismes criptogràfics, tenen una complexitat polinòmica. Atès que les operacions en cossos finits es remeten a operacions amb nombres enters, vegem prèviament la complexitat d'alguns algorismes bàsics amb enters.

Algorismes eficients

Els algorismes de complexitat polinòmica s'anomenen computacionalment *eficients* o *bons*, ja que l'ordinador els pot executar en un temps raonable, per oposició als algorismes d'una complexitat exponencial en la longitud de les dades.

Proposició 3.8.

- El temps necessari per a sumar dos nombres naturals de longitud binària k és $O(k)$. L'addició de nombres naturals té, doncs, complexitat lineal en la longitud de les dades.
- El temps necessari per a multiplicar dos enters naturals de longituds k, l, $l \leq k$ és $O(k^2)$. La multiplicació té, doncs, una complexitat quadràtica en la longitud de les dades.

Observació

S'ha d'assenyalar que l'algorisme habitual de multiplicació no és el millor algorisme conegut per a fer aquesta operació. N'hi ha un altre, degut a Schönhage i Strassen, amb complexitat $O(k\log(k)\log\log(k))$.

Demostració:

1) Sempre es pot suposar la mateixa longitud per a tots dos sumands, afegint, si ve al cas, zeros a l'esquerra de la representació binària del de menys longitud. La suma s'obté aleshores fent k sumes binàries. És a dir, per definició, k operacions bit.

2) Sigui $l \leq k$. Amb la regla habitual de multiplicació: col·locar el nombre menor sota del major i multiplicar cada dígit d'aquell pel d'aquest, col·locar els resultats en files desplaçades cada una una posició a l'esquerra respecte de l'anterior i sumant, com a màxim, les l files, de longitud $k + l$, (tenint en compte els $k - l$ desplaçaments), tenim un nombre d'operacions bit

$$O(l(k + l)) = O(2kl) = O(2k^2) = O(k^2)$$

∎

Nota

L'operació de substracció o resta té, òbviament, el mateix temps d'execució que la suma. La divisió, amb la regla habitual, es redueix a multiplicacions i diferències i té igual tipus de complexitat que la multiplicació, és a dir, quadràtica. No obstant això, s'ha de recordar que l'estimació de la complexitat, donada per la notació O, implica una constant, per la qual cosa dos algorismes amb igual complexitat poden tenir, de fet, costos molt diferents. És el cas de la divisió, bastant més costosa que la multiplicació. Aquest fet justifica tractar d'evitar o limitar al màxim el nombre de divisions; en el cas de la criptografia amb corbes el·líptiques això es pot aconseguir mitjançant l'ús de coordenades projectives.

Vegem la complexitat de l'algorisme 1.4 (d'Euclides estès) necessari, com hem vist, per al càlcul d'inversos en $\mathbb{F}_p$.

Observeu que en l'algorisme 1.4 els residus a_i, obtinguts en iterar el pas 2, formen una successió decreixent. Per tant, l'algorisme finalitza necessàriament en un nombre finit d'etapes. Més concretament:

Lema 3.9. Si $a \geq b$, el nombre d'etapes necessàries en l'execució de l'algorisme d'Euclides estès és $O(\log(a))$.

Demostració: N'hi ha prou de provar que els residus a_i verifiquen la relació $a_{i+2} < \frac{1}{2}a_i$, la qual cosa implica que el nombre d'etapes és, com a màxim, $2\lfloor \log(a) \rfloor$. Ara bé, si $a_{i+1} \leq \frac{1}{2}a_i$, aleshores $a_{i+2} < a_{i+1} \leq \frac{1}{2}a_i$. Si $a_{i+1} > \frac{1}{2}a_i$, la divisió euclidiana proporciona $a_i = a_{i+1} + a_{i+2}$, amb la qual cosa, també en aquest cas, $a_{i+2} = a_i - a_{i+1} < \frac{1}{2}a_i$. ∎

Proposició 3.10. El cost computacional de l'algorisme d'Euclides estès és $O(\log^3 a)$ (és a dir, cúbic en la longitud de les dades).

Demostració: Cada etapa de l'algorisme comporta una divisió (de a_i entre a_{i+1}), dues multiplicacions (de q_{i+1} per x_{i+1} i per y_{i+1}) i dues diferències (per a obtenir x_{i+2} i y_{i+2}). El cost total d'aquestes operacions elementals és $O(\log^2 a)$. La proposició es dedueix tenint en compte el lema anterior. ∎

Vegem finalment la complexitat de l'algorisme 3.2, de multiplicar i elevar al quadrat:

Proposició 3.11. L'algorisme de multiplicar i elevar al quadrat per a calcular $a^n \pmod m$ té una complexitat de $O(\log^2 m \log(n))$.

Demostració: En efecte, l'algorisme comporta, com a màxim, $O(\log(n))$ quadrats, $O(\log(n))$ multiplicacions i $O(\log(n))$ divisions (per a fer les reduccions mòdul m), de nombres, tots, de longitud $O(\log(m))$. Aleshores, la complexitat seria de l'ordre de $3\cdot\log(n)\cdot\log^2(m)$, o sigui, $O(\log^2(m)\cdot\log(n))$. ∎

Cost computacional de les operacions en cossos finits

Un cop establert el cost computacional, mesurat en operacions bit, de les operacions aritmètiques elementals amb nombres naturals, i també de l'algorisme d'Euclides i l'algorisme de multiplicar i elevar al quadrat, podem deduir el cost de l'aritmètica en el cos finit $\mathbb{F}_q$, en què $q = p^m$,

Proposició 3.12. El cost computacional d'una addició (o d'una substracció) d'elements de $\mathbb{F}_q$ és $O(\log(q))$ operacions bit.

Demostració: L'addició de dos elements a,b, feta com a addició (o substracció) de vectors amb coeficients en $\mathbb{F}_p$ implica la realització de m addicions (o substraccions) de nombres naturals més petits que p i la reducció de cada resultat mòdul p. Observeu que per a aquesta reducció no és necessària una divisió: com que els nombres obtinguts són més petits o iguals que $2(p-1)$, per a obtenir el resultat mòdul p n'hi ha prou de deixar el resultat sense alterar si el nombre és més petit que p i restar-li p en cas contrari. Així la complexitat serà,

$$O(m)O(\log(p)) = O(m\log(p)) = O(\log(q)). \qquad (15)$$

∎

Proposició 3.13. El cost computacional (utilitzant la representació polinòmica) d'una multiplicació (o d'una divisió) d'elements de $\mathbb{F}_q$ és $O(\log^3 q)$ operacions bit.

Observació

A l'efecte computacional el cost de les sumes o diferències en un algorisme en cossos finits se sol considerar irrellevant, ja que la seva complexitat és més petita que la de la multiplicació. A vegades, tal complexitat s'expressa no en operacions bit sinó en nombre d'operacions elementals; en aquest cas s'entenen per tals les multiplicacions.

Demostració: Els elements $a \in \mathbb{F}_q$ es manejaran com a expressions $a = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$, $a_i \in \{0,1,\ldots,p-1\}$. Per la multiplicació de a per b implica fer el producte dels polinomis que els representen i la reducció del resultat mòdul $f(X)$.

La multiplicació de dos polinomis de grau $m-1$ sobre $\mathbb{F}_p$ implica la realització de $O(m^2)$ multiplicacions d'enters mòdul p, cada una de les quals requereix $O(\log^2 p)$ operacions bit, més una sèrie d'addicions que, per a tenir un cost computacional inferior, podem no prendre en consideració. Així doncs, aquesta primera etapa requereix $O(m^2 \log^2 p)$ operacions bit. La divisió del resultat pel polinomi $f(X)$ requereix fer $O(m)$ divisions d'enters mòdul p (que fetes amb l'algorisme d'Euclides requereixen $O(\log^3 p)$ operacions bit) i $O(m^2)$ multiplicacions d'enters mòdul p; per tant, aquesta reducció representa un cost de $O(m\log^3 p + m^2 \log^2 p)$.

Observació

Observeu que la complexitat de la multiplicació (o divisió) en un cos finit és cúbica, mentre que la multiplicació (o divisió) en nombres naturals és quadràtica. Aquest fet obeeix al sobrecost de la reducció mòdul p i del càlcul de l'invers mòdul p.

En total, la multiplicació de a per b implica, doncs

$$O(m^2 \log^2 p + m\log^3 p + m^2 \log^2 p) = O((m\log(p))^3) = O(\log^3(q)) \qquad (16)$$

operacions bit.

Pel que fa a la divisió x/y, només manca provar que l'invers de $y \in \mathbb{F}_q^*$ es pot computar en $O(\log^3 q)$ operacions bit. N'hi ha prou d'aplicar l'algorisme d'Euclides a $f(X)$ i al polinomi que representa b, la qual cosa requereix $O(m)$ divisions de polinomis de grau com a màxim m, cadascuna de les quals comporta $O(m\log^3 p + m^2 \log^2 p)$ operacions bit. En definitiva, el cost total és $O(m^3 \log^3 p) = O(\log^3 q)$ operacions bit. ∎

3.3. Algorismes aritmètics en cossos finits

El subapartat 3.1. descriu els aspectes matemàtics de les operacions aritmètiques en cossos finits. Des d'un punt de vista computacional, especialment per a cossos de cardinal q molt gran, és crucial poder implementar, tant en programari com en maquinari, aquestes operacions el més eficientment possible. Hi ha nombrosos algorismes amb aquest propòsit, adaptats tant al tipus de cos finit com a la plataforma particular en la qual es vol implementar tal aritmètica (per exemple, hi ha algorismes específics per a plataformes amb capacitat de computació i de memòria reduïdes, com les targetes intel·ligents o les etiquetes electròniques). És aquest un camp d'investigació molt actiu actualment, però que sobrepassa els objectius del curs, per la qual cosa ens limitarem a mostrar tan sols un exemple bàsic per a l'addició i la multiplicació en els dos tipus de cossos més usuals en criptografia: els cossos primers $\mathbb{F}_p$ i els cossos binaris $\mathbb{F}_{2^m}$.

1) Cossos primers $\mathbb{F}_p$

Si el cardinal p del cos és gran els seus elements tindran longitud $k = \lceil \log_2 p \rceil$ més gran que la longitud P de paraula de l'ordinador (usualment $P = 16,32$ o 64 bits). Si $t = \lceil k/P \rceil$ els elements $a \in \mathbb{F}_p$ es poden representar en la forma $A := A[t-1] \dots A[1]A[0]$, concatenació de t blocs $A[i]$ de P bits.

Per a dos d'aquests blocs x,y, escriurem $[z,\varepsilon]$ si $x + y = \varepsilon 2^P + z$, $\varepsilon = 0,1$, $0 \leq z \leq 2^P - 1$.

Algorisme d'addició: siguin $a,b \in \{0,1,\dots,p-1\}$. L'algorisme següent calcula $c \equiv a + b \pmod{p}$.

Algorisme 3.14.

1. Sigui $(C[0],\varepsilon) := A[0] + B[0]$.
2. Per a $i = 1,\dots,t-1$ sigui $(C[i],\varepsilon) := A[i] + B[i] + \varepsilon$.
3. Sigui $c = C[t-1] \cdots C[0]$.

   Si $\varepsilon = 1$ agafar $c := c - p$.

   Si $c \geq p$ agafar $c := c - p$.
4. $c \equiv a + b \pmod{p}$.

Exemple 3.4. Per simplicitat suposarem $P = 2$ (tal com s'ha indicat, els valors habituals de P solen ser 16,32,64, etc). Sigui el primer $p = 101$, la qual cosa implica $k = 7$, $t = 4$.

Siguin $a = 83 = 2^6 + 2^4 + 2 + 1$ (aleshores $A[0] = 11, A[1] = 00, A[2] = 01, A[3] = 01$) i $b = 71 = 2^6 + 2^2 + 2 + 1$ (és a dir, $B[0] = 11, B[1] = 01, B[2] = 00, B[3] = 01$). Apliquem l'algorisme anterior als elements a,b. Tindrem que $(C[0],\varepsilon) = (10,1)$ (ja que $A[0] + B[0] = 3 + 3 = 6 = 1 \cdot 2^P + 2$). Anàlogament s'obté:

$$(C[1],\varepsilon) = (10,0),\ (C[2],\varepsilon) = (01,0),\ (C[3],\varepsilon) = (10,0)$$

concatenant els blocs $C[i]$ tindrem: $c = 10011010 = 2^7 + 2^4 + 2^3 + 2 = 154$. Com que aquest nombre és més gran que p el resultat final és $c := c - p = 53$.

Algorisme de multiplicació: siguin $a,b \in \{0,1,\dots,p-1\}$. El producte en $\mathbb{F}_p$ implica el càlcul del producte enter $c = a \cdot b$ i la reducció posterior mòdul p. Per a l'etapa de reducció hi ha diversos algorismes (Barret, Montgomery, etc). L'algorisme següent calcula el producte enter $c = a \cdot b$.

Referències addicionals

Per a altres algorismes d'addició i multiplicació, i també d'exponenciació i divisió, ens remetem a la nombrosa bibliografia sobre el tema, com per exemple:

I. Blake; G. Seroussi; N. Smart (2000). "Elliptic Curves in Cryptography". *London Mathematical Society Lecture Note, Series 265*. Cambridge: Cambridge U. Press, i

D. Hankerson; A. Menezes; S. Vanstone (2004). *Guide to Elliptic Curve Cryptography*. Springer.

Algorisme 3.15.

1. Siguin $R_0 := 0, R_1 := 0, R_2 = 0$.
2. Per a $k = 0,1,\ldots 2t-2,$ calcular,

   2.1: Per a cada parella (i,j); $i+j=k, 0 \leq i,j \leq t-1$.

   $UV := A[i] \cdot B[j]$.

   $(R_0,\varepsilon) := R_0 + V$.

   $(R_1,\varepsilon) := R_1 + U + \varepsilon$.

   $R_2 := R_2 + \varepsilon$.

   2.2 $C[k] := R_0$, $R_0 := R_1$, $R_1 := R_2$, $R_2 := 0$.

3 $C[2t-1] := R_0$.

4 $c = C[2t-2] \ldots C[0]$.

Exemple 3.5. Suposem les mateixes dades que les de l'exercici 3.4. Apliquem l'algorisme anterior a a,b.

Per a $k = 0$ tindrem $UV = A[0]B[0] = 9 = 1001$ (aleshores $U = 10$, $V = 01$). Per tant

$$(R_0,\varepsilon) = (01,0), (R_1,\varepsilon) = (10,0), R_2 = 0$$

aleshores $c[0] = 01$. Anàlogament s'obtindria,

$$C[1] = 01,\ C[2] = 00,\ C[3] = 00,\ C[4] = 11,\ C[5] = 01,\ C[6] = 01$$

És a dir, $c = 011100000101 = 5893$.

2) Cossos binaris $\mathbb{F}_{2^m}$

En aquest cas la longitud binària del cardinal del cos és òbviament m. En la base polinòmica determinada per una arrel α del polinomi irreductible de grau m $f(X)$, els elements $a \in \mathbb{F}_{2^m}$ s'expressen en la forma: $a = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$, $a_i = 0,1$. Escrivim $f(X) = X^m + r(X)$.

L'addició de dos elements $a,b \in \mathbb{F}_{2^m}$ és trivial: expressats a,b en qualsevulla base n'hi ha prou de fer la suma binària dels dos bits corresponents a cadascuna de les m coordenades.

Algorisme de multiplicació: el producte dels elements a, b comporta la multiplicació de dos polinomis binaris $a(X),b(X)$, de grau com a màxim $m-1$

i la posterior reducció mòdul $f(X)$. El següent algorisme resol el primer problema. El resultat $c(X)$ polinomi de grau com a màxim $2m-2$ pot expressar-se com una paraula C formada per t blocs $C[j]$, de grandària P, els components de la qual són el bloc B, que representa a $b(X)$, o bé un bloc nul.

Algorisme 3.16.

1. $C :=$ concatenació de t blocs de grandària P amb entrades nul·les.
2. Per a $k = 0,1,\ldots P-1$,

   Per a $j = 0,1,\ldots,t-1$.

   Si el bit k de $A[j]$, és 1 col·locar B en la posició k, del bloc $A[j]$.

   Cas contrari col·locar un bloc nul en aquesta posició.
3. C és la representació de $c(X)$.

Exemple 3.6.

Siguin $a = 101101$ i $P = 2$, per tant $t = 3$, $A[0] = 01, A[1] = 11, A[2] = 10$.

C estarà format per 3 blocs de grandària 2, les entrades dels quals són nul·les o B: Per a cada $k = 0,1$ si el bit corresponent de $A[j]$; $j = 0,1,2$ és 1 posarem B en la casella corresponent de $C[j]$ i, cas contrari, un bloc 0. Queda, finalment, $C = [B,0][B,B][0,B]$.

Noteu que el resultat correspon a la forma polinòmica $c(X) = BX^5 + BX^3 + BX^2 + B$, que és el mateix resultat que s'hauria obtingut multiplicant $a(X) = X^5 + X^3 + X^2 + 1$ per B.

Exercicis d'autoavaluació

1. Justifiqueu la necessitat que n sigui primer perquè $\mathbb{Z}_n$, el conjunt dels enters mòdul n, tingui estructura de cos. Mostreu que $\mathbb{Z}_6$ no és un cos.

2. Construïu explícitament el cos finit $\mathbb{F}_9$ amb 9 elements i doneu-ne la taula d'equivalències vectorial-exponencial.

3. Quins elements de $\mathbb{F}_9$ es poden agafar com a generadors del seu grup multiplicatiu? Quins elements de $\mathbb{F}_9$ tenen arrel quadrada en aquest cos?

4. Per a quins valors de p (p = 3,5,7,11,13,19,23) es pot construir un cos d'ordre p^2 usant el polinomi $x^2 + 1$?

5. Trobeu els valors de m per als quals $X^2 + mX + 2$ és un polinomi irreductible i primitiu en $\mathbb{Z}_{11}[X]$.

6. Sigui $q = p^m$, p primer, $r \in \mathbb{N}$. Proveu que el cos $\mathbb{F}_{p^r}$ està contingut en el cos $\mathbb{F}_q$ si i només si r és un divisor de m.

7. Sigui el cos $\mathbb{F}_8$, definit pel polinomi binari $f(X) = X^3 + X + 1$, i sigui α una arrel de $f(X)$. Expresseu en la base polinòmica $\{1,\alpha,\alpha^2\}$ els elements α^5 i $\frac{\alpha}{1+\alpha^2}$.

8. Demostreu que en el cos $\mathbb{F}_q$ la suma de tots els elements és zero i si q és una potència d'un nombre primer senar, el producte de tots els elements no nuls és –1.

9. Demostreu que en un cos finit de característica p,
a) Si $p = 2$, cada element és un quadrat;
b) Si p és senar, exactament la meitat dels elements són quadrats.

10. Escriviu la taula d'equivalències vectorial-exponencial per al cos finit $\mathbb{F}_{2^4}$, amb generador α.
a) Determineu δ com a potència de α, en què $\delta = \alpha^{10} + \dfrac{\alpha^7 + \alpha^{23}}{1 + \alpha^{12}} + 1$
b) Trobeu totes les arrels de l'equació:

$$\alpha^7 x^2 + (\alpha^2 + \alpha^9)x + \frac{1+\alpha}{\alpha^4} = 0$$

11. Utilitzeu l'algorisme d'Euclides estès per a calcular:
a) L'invers de 43 en el cos $\mathbb{Z}_{101}$.
b) L'invers de (1,2) en el cos $\mathbb{F}_9$ (genereu $\mathbb{F}_9$ a partir del polinomi irreductible $f(X) = X^2 + 1$).

12. Trobeu totes les bases normals del cos $\mathbb{F}_8$ sobre el cos $\mathbb{F}_2$.

13. Sigui $q = p^m$, p primer, $\mathbb{F}_q$ el cos finit amb q elements i $\mathcal{B} : \{x_1, \ldots, x_m\}$ una base de $\mathbb{F}_q$ sobre $\mathbb{F}_p$. Donat $x \in \mathbb{F}_q$ sigui l'aplicació lineal $\varphi_x : \mathbb{F}_q \to \mathbb{F}_q$ donada per $\varphi_x(y) = xy$. Com tota aplicació lineal φ estarà determinada en la base $\mathcal{B}$ per una matriu $m \times m$ amb coeficients en $\mathbb{F}_p$, $A = (a_{ij})$.

S'anomena *traça* de x $Tr(x) = \sum_i a_{ii} \in \mathbb{F}_p$ (és a dir, el que s'anomena traça de la matriu A, la suma dels elements de la seva diagonal principal), i *norma* de x $N(x) = |A| \in \mathbb{F}_p$ (determinant de la matriu A). Encara que definit en termes d'una base concreta, es pot veure en qualsevol text d'àlgebra lineal que $Tr(x)$ i $N(x)$ tenen els mateixos valors en qualsevol base. En variar $x \in \mathbb{F}_q$ es tenen dues aplicacions $Tr : \mathbb{F}_q \to \mathbb{F}_p$ i $N : \mathbb{F}_q \to \mathbb{F}_p$. Proveu les propietats següents:

i) $Tr(x + y) = Tr(x) + Tr(y)$,

i') $N(x \cdot y) = N(x) \cdot N(y)$, $x,y \in \mathbb{F}_q$,

ii) $Tr(\lambda x) = \lambda Tr(x)$,

ii') $N(\lambda x) = \lambda^n N(x)$, $\lambda \in \mathbb{F}_p, x \in \mathbb{F}_q$,

iii) $Tr(\lambda) = m\lambda$,

iii') $N(\lambda) = \lambda^m, \lambda \in \mathbb{F}_p$.

14. Feu l'exercici següent:

a) Multipliqueu en binari els nombres $a = 103$, $b = 65$. Determineu el nombre d'operacions bits fetes.

b) Generalitzeu al cas a nombre de longitud binària k i $b = 2^{k-1} + 1$.

c) Compareu el nombre d'operacions bits d'aquesta última multiplicació amb la complexitat general per a la multiplicació obtinguda en la proposició 3.8.

15. Feu l'exercici següent:

a) Formuleu un algorisme per a l'exponenciació a^n en un cos finit anàleg a l'algorisme 3.2 per a l'exponenciació modular en $\mathbb{Z}$.

b) Determineu la complexitat de l'algorisme anterior.

c) Apliqueu al cas del cos $\mathbb{F}_8$, $a = 1 + \alpha$, α arrel del polinomi $X^3 + X + 1 \in \mathbb{F}_2[X]$ i $n = 5$.

Solucions

1) Si n no fos primer admetria una factorització $n = ab$, $1 < a,b < n$. Els elements a,b no admeten aleshores invers: si, per exemple, a admetés invers a^{-1}, $a^{-1} \in \{1,2,\ldots,n-1\}$ es tindria que $aa^{-1} = 1$ i multiplicant tots dos membres per b: $(ba)a^{-1} = na^{-1}$ i $1b = b$. Donat que $n \cdot a^{-1} = 0$ a $\mathbb{Z}_n$, aleshores $b = 0$, la qual cosa és una contradicció.

En el cas $n = 6$ del cas anterior es dedueix que els elements 2 i 3 no admeten invers, la qual cosa també es pot comprovar directament, i es veu que el producte de 2 o de 3 pels elements del conjunt $\{1,2,3,4,5\}$ mai no és 1.

2) D'acord amb la construcció donada pel teorema 1.9 és necessari agafar un polinomi irreductible de grau dos sobre el cos primer amb tres elements $\mathbb{F}_3$. Un polinomi tal és, per exemple, el $X^2 + 1$. Si α és una arrel d'aquest polinomi es tindria:

$$\mathbb{F}_9 = \{0,1,2,\alpha,2\alpha,1+\alpha,2+\alpha,1+2\alpha,2+2\alpha\}$$

les taules additives i multiplicatives per a aquest cos es podrien construir com en l'exemple 1.4. No obstant això, el polinomi emprat no és primitiu i una arrel d'aquest polinomi no ens serveix com a generador del grup multiplicatiu del cos (observeu que $\alpha^4 = 1$).

Agafem ara el polinomi $X^2 + 2X + 2$ i sigui α una arrel i per tant $\alpha^2 = 1 + \alpha$. En resulta la correspondència.

Exponencial	Vectorial	Polinomial
0	(0,0)	0
α^0	(1,0)	1
α^1	(0,1)	α
α^2	(1,1)	$1+\alpha$
α^3	(1,2)	$1+2\alpha$
α^4	(2,0	2
α^5	(0,2)	2α
α^6	(2,2)	$2+2\alpha$
α^7	(2,1)	$2+\alpha$

3) Donat que $\mathbb{F}_9^*$ és un grup cíclic d'ordre 8, la teoria general de grups cíclics ens diu que hi ha $\phi(8) = \phi(2^3) = 2^2 \cdot 1 = 4$ generadors del grup multiplicatiu d'aquest cos. Si α és un generador tal (per exemple, com en l'exercici anterior, es pot agafar com a α una arrel del polinomi $X^2 + 2X + 2 \in \mathbb{F}_3[X]$), es té:

$$\mathbb{F}_9^* = \{\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8 = 1\}$$

Els generadors seran de la forma α^i, en què $mcd(i,8) = 1$ i, per tant, $i = 1,3,5$ i 7. Així doncs, els generadors seran $\{\alpha,\alpha^3,\alpha^5,\alpha^7\}$. En efecte, tots aquests elements tenen ordre 8, i per tant les seves potències recorren tot $\mathbb{F}_9^*$.

Els elements que tenen arrel quadrada són aquells en què l'exponent és parell, o sigui, $\{\alpha^2,\alpha^4,\alpha^6,\alpha^8\}$. En efecte, aquests elements tenen arrel quadrada, i de fet cadascun té dues arrels quadrades: per exemple, α^2 té per arrel α però també α^5 $((\alpha^5)^2 = \alpha^{10} = \alpha^2)$. En canvi, els elements amb exponent i senar no admeten arrel quadrada, la qual cosa es pot comprovar directament. Observeu que si $\beta \in \mathbb{F}_9$ fos una arrel quadrada de α^i, és a dir, $\beta^2 = \alpha^i$, com que α^i té ordre 8, β tindria ordre 16, la qual cosa és absurda, ja que el seu ordre ha de ser divisor de l'ordre del grup, que és 8.

4) Hem d'esbrinar per a quins valors de p es pot construir un cos amb p^2 elements a partir del polinomi *irreductible* $X^2 + 1$, és a dir, hem de poder construir un cos $\mathbb{F}_{p^2} = \mathbb{Z}_p[X]/(X^2+1)$. Si $f(X) = X^2+1$ no fos irreductible, podria ser descompost de la forma $(X-a)(X-b)$. Aleshores, si existeixen valors $X = a$ o $X = b$ tals que $f(X) = 0 \pmod p$, $f(X)$ no seria irreductible, i per tant, $\mathbb{Z}_p[X]/X^2+1$ no serà un cos. Suposem $f(X) = 0$, aleshores seria $X^2 + 1 = 0 \pmod p$ i $X^2 = -1 = p-1 \pmod p$. Així doncs, comprovarem si $p-1$ té arrel quadrada mòdul p i, en cas afirmatiu, $f(X)$ no serà irreductible.

a) Per a $p = 3$: $x^2 = 2$ no té solució, i per tant $f(X)$ és irreductible.

b) Per a $p = 5$: $x^2 = 4$ té solució $x = 2$, $x = -2$, i per tant $f(X)$ no és irreductible.

c) Per a $p = 7$: $x^2 = 6$ no té solució, i per tant $f(X)$ és irreductible.

d) Per a $p = 11$: $x^2 = 10$ no té solució, i per tant $f(X)$ és irreductible.

e) Per a $p = 13$: $x^2 = 12$ té solució $x = 5$ ($5^2 = 25 = 12 \pmod p$), i per tant $f(X)$ no és irreductible.

f) Per a $p = 19$: $x^2 = 18$ no té solució, i per tant $f(X)$ és irreductible.

g) Per a $p = 23$: $x^2 = 22$ no té solució, i per tant $f(X)$ és irreductible.

Els valors de p que compleixen que $\mathbb{F}_{p^2} = \mathbb{Z}_p[X]/X^2+1$ és un cos són: 3,7,11,19 i 23. Observeu que són tots els primers del conjunt donat congruents amb 3 mòdul 4.

5) Hem de trobar tots els valors de m tals que el polinomi $p(X) = X^2+mX+2$ sigui irreductible i primitiu en $\mathbb{Z}_{11}[X]$.

Primer trobarem els valors de m per als quals $p(X)$ és irreductible. Per això, suposarem que $p(X)$ es pot descompondre en factors, $X^2 + mX + 2 = (X - a)(X - b) = X^2 - bx - ax + ab = X^2 - (a + b)X + ab$. O sigui, $-(a + b) = m$ i $ab = 2$.

Les possibles solucions són: ($a = 1, b = 2, m = 8$); ($a = 2, b = 1, m = 8$), ($a = 3, b = 8, m = 0$), ($a = 4, b = 6, m = 1$), ($a = 5, b = 7, m = 10$), ($a = 6, b = 4, m = 1$), ($a = 7, b = 5, m = 10$), ($a = 8, b = 3, m = 0$), ($a = 9, b = 10, m = 3$), ($a = 10, b = 9, m = 3$). La conclusió és que els possibles valors de m perquè $p(x)$ sigui irreductible són 2,4,5,6,7 i 9.

Finalment, hem de substituir m per aquests valors i veure si $p(x)$ és primitiu. Per a veure que un polinomi és primitiu hem de comprovar que les seves arrels tinguin ordre $p^n - 1$, o sigui, ordre 120 en el nostre cas. Un element α té ordre i si $\alpha^i = \alpha^0 = 1$ en el cos en el qual estem treballant. Aleshores, podem agafar $\alpha = [X]$ com a arrel i anar calculant les potències d'aquest element fins a arribar a un exponent i tal que $\alpha^i = 1$. Si $i = 120$ (ordre màxim), podem dir que α és primitiu i el polinomi corresponent també (no cal calcular totes les potències de α fins a 120, n'hi ha prou de calcular α^i amb i divisor de 120). Finalment, després de les operacions pertinents, ens queden com a valors que fan que $p(x)$ sigui primitiu: $m = 4,5,6$ i 7.

6) Si $r|m$ s'ha provat en la proposició 2.2 que el polinomi $X^{p^r} - X$ divideix el polinomi $X^{p^m} - X$. Per tant, les arrels del primer (que constitueixen el cos $\mathbb{F}_{p^r}$) són també arrels del segon, és a dir, elements del cos $\mathbb{F}_q$.

Suposem recíprocament que $\mathbb{F}_{p^r} \subset \mathbb{F}_{p^m}$. Com que tots dos cossos contenen $\mathbb{F}_p$ es té la cadena $\mathbb{F}_p \subset \mathbb{F}_{p^r} \subset \mathbb{F}_{p^m}$. Aleshores es té que:

- $\mathbb{F}_{p^r}$ és un espai vectorial de dimensió r sobre $\mathbb{F}_p$
- $\mathbb{F}_{p^m}$ és un espai vectorial de dimensió m sobre $\mathbb{F}_p$
- $\mathbb{F}_{p^m}$ és un espai vectorial sobre $\mathbb{F}_{p^r}$. Anomenem s la seva dimensió.

És fàcil demostrar la relació següent entre les tres dimensions:

$$n = [\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^r}][\mathbb{F}_{p^r} : \mathbb{F}_p] = rs \Rightarrow r|m$$

[N'hi ha prou d'agafar bases $\{v_1, v_2, \ldots, v_s\}$ de $\mathbb{F}_{p^m}$ sobre $\mathbb{F}_{p^r}$ i $\{w_1, w_2, \ldots, w_r\}$ de $\mathbb{F}_{p^r}$ sobre $\mathbb{F}_p$ i comprovar que els productes $v_i w_j$ formen una base de $\mathbb{F}_{p^m}$ sobre $\mathbb{F}_p$.]

7) Per a ser arrel del polinomi $f(X) = X^3 + X + 1$, α verifica (en binari) $\alpha^3 = \alpha + 1$. Per tant

a) $\alpha^4 = \alpha^2 + \alpha$ i $\alpha^5 = \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^2$.

b) $\frac{\alpha}{1+\alpha^2} = \alpha(1 + \alpha^2)^{-1}$. Per a obtenir l'invers de $1 + \alpha^2$ s'aplica l'algorisme d'Euclides per a $a = a_0 = X^3 + X + 1$, $b = a_1 = X^2 + 1$ i $x_o = 1, x_1 = 0, y_0 = 0, y_1 = 1$. S'obté: $a_2 = 1, a_3 = 0, x_2 = 1, y_2 = X$. Aleshores

$$1 = mcd(a,b) = X^3 + X + 1 + X(X^2 + 1) \Rightarrow (1 + \alpha^2)^{-1} = \alpha$$

Finalment: $\frac{\alpha}{1+\alpha^2} = \alpha\alpha = \alpha^2$.

8) El cos $\mathbb{F}_{p^m}$ està format per tots els elements que compleixen $X^{p^m} - x = 0$. Siguin aquests elements $\{0, a_1, a_2, \cdots, a_{p^m-1}\}$. Aleshores $X^{p^m-1} - 1 = (X - a_1)(X - a_2)\cdots(X - a_{p^m-1})$. Fent operacions:

$$X^{p^m-1} - 1 = X^{p^m-1} - \underbrace{(a_1 + a_2 + \cdots + a_{p^m-1})}_{=0} Xp^m - 2 + \cdots + (-1)^{p^m-1} \prod a_i$$

En qualsevol cas la suma de tots els elements de $\mathbb{F}_{p^m}$ dóna zero i, si p és senar, $p^m - 1$ és parell i, aleshores, el producte és igual a –1.

9) Suposem que $p = 2$; llavors podem escriure el cos finit $\mathbb{F}_{2^m}$ com $\mathbb{F}_{2^m} = \{0,\alpha^1,\alpha^2,\cdots,\alpha^{2^m-1} = 1\}$, en què α és un element primitiu. Vegem si α té arrel quadrada:

$$1 = \alpha^0 = \alpha^{2^m-1} \Longrightarrow \alpha = \alpha^{2^m} \Longrightarrow \sqrt{\alpha} = \alpha^{2^{m-1}}$$

Com que α té arrel quadrada, tots els elements de $\mathbb{F}_{2^m}$ també en tindran.

En segon lloc, suposem que $p = 2k+1$. En aquest cas podem escriure $\mathbb{F}_{p^m} = \{0,\alpha^1,\alpha^2,\cdots,\alpha^{p^m-1}\}$, en què α és un element primitiu i $\alpha^{p^m-1} = \alpha^0$. Evidentment, α^{2k} té arrel quadrada, i també l'element zero. Per tant, els elements que podem assegurar que tenen arrel quadrada seran:

$$\{0,\alpha^0,\alpha^2,\cdots,\alpha^{p^m-1}\}$$

que són exactament la meitat dels elements no nuls de $\mathbb{F}_{p^m}$ i, a més, el zero.

Vegem que no hi ha més elements en $\mathbb{F}_{p^m}$ amb arrel quadrada i, per això, considerem $\phi : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$, definida com $\phi(x) = x^2$. En aquesta aplicació, excepte el zero, totes les imatges tenen exactament dues antiimatges. En efecte, suposem que dos elements $x,y \in \mathbb{F}_{p^m}, x \neq y$ tenen un mateix quadrat, és a dir, $x^2 = y^2$. Aleshores

$$x^2 = y^2 \Longrightarrow x^2 - y^2 = 0 \Longrightarrow (x+y)\cdot(x-y) = 0$$

Aquesta equació té dues solucions possibles: $x = y$ i $x = -y$. Com que p és senar, sempre existiran valors diferents $x,y \in \mathbb{F}_{p^m}$ tals que $x = -y$, excepte en el cas del zero.

10) Agafem el cos finit $\mathbb{F}_{2^4} = \mathbb{Z}_2[X]/f(x)$, en què $f(x)$ sigui un polinomi irreductible de grau 4 i coeficients en $\mathbb{Z}_2$. El nostre primer problema és, doncs, trobar un polinomi irreductible i primitiu de quart grau.

Comencem, primer, amb els polinomis irreductibles de grau 1 (n'hi ha dos: $X, X+1$). Els de grau 2 (n'hi ha un: X^2+X+1). Els de grau 3 (n'hi ha dos: X^3+X^2+1; X^3+X+1). Els de grau 4 (ni ha tres: $X^4+X^3+X^2+X+1$; X^4+X^3+1; X^4+X+1). Entre aquests últims polinomis de quart grau, en cerquem un que sigui primitiu, és a dir, que les seves arrels tinguin ordre $p^n - 1 = 15$.

Comprovem amb el polinomi $X^4+X^3+X^2+X+1$:

Sigui α una arrel, aleshores

$$\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1,$$
$$\alpha^5 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = 1,$$

O sigui, $\alpha^5 = 1$ i, per tant, α no és d'ordre 15 i el polinomi no és primitiu.

Comprovem ara amb el polinomi X^4+X^3+1.

Sigui α una arrel, aleshores

$$\alpha^4 = \alpha^3 + 1$$
$$\alpha^5 = \alpha^4 + \alpha = \alpha^3 + \alpha + 1$$
$$\alpha^6 = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$$
$$\alpha^7 = \alpha^4 + \alpha^3 + \alpha^3 + \alpha = \alpha^2 + \alpha + 1$$
$$\alpha^8 = \alpha^3 + \alpha^2 + \alpha$$
$$\alpha^9 = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^2 + 1$$
$$\alpha^{10} = \alpha^3 + \alpha$$
$$\alpha^{11} = \alpha^4 + \alpha^2 = \alpha^3 + \alpha^2 + 1$$

$$\alpha^{12} = \alpha^9 + \alpha^6 + \alpha^3 + 1 = \alpha + 1$$
$$\alpha^{13} = \alpha^2 + \alpha$$
$$\alpha^{14} = \alpha^3 + \alpha^2$$
$$\alpha^{15} = 1$$
$$\alpha^{16} = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + 1 + \alpha^2 = \alpha$$

Per tant, el polinomi $X^4 + X^3 + 1$ és primitiu.
Així doncs, utilitzarem el polinomi primitiu $X^4 + X^3 + 1$ i $\mathbb{F}_{2^4} = \mathbb{Z}_2[X]/X^4 + X^3 + 1$.
La taula d'equivalències vectorial-potencial és:

0	(0000)	α^0	(1000)	α^1	(0100)	α^2	(0010)	α^3	(0001)
α^4	(1001)	α^5	(1101)	α^6	(1111)	α^7	(1110)	α^8	(0111)
α^9	(1010)	α^{10}	(0101)	α^{11}	(1011)	α^{12}	(1100)	α^{13}	(0110)
α^{14}	(0011)								

- Per a calcular δ com a potència de α, calcularem:

$$\delta = \alpha^{10} + \frac{\alpha^7 + \alpha^{23}}{1 + \alpha^{12}} + 1 = \alpha^{10} + \frac{\alpha^7 + \alpha^8}{\alpha} + 1 = \alpha^{10} + \frac{\alpha^4}{\alpha} + 1 = \alpha^{10} + \alpha^3 + 1 = \alpha^{12}.$$

- Per a trobar les arrels de l'equació donada hem de resoldre:

$$\alpha^7 x^2 + (\alpha^2 + \alpha^9)x + \frac{1 + \alpha}{\alpha^4} = 0,$$

o sigui: $\alpha^7 x^2 + x + \alpha^8 = 0$.
Per cerca exhaustiva, trobarem les arrels α^3 i α^{13}.

11) En primer lloc, l'invers de 43 en $\mathbb{Z}_{101}$ serà un x tal que $43 \cdot x = 1 \pmod{101}$. Per tant, $43x = 1 + 101y$.

Apliquem l'algorisme d'Euclides estès amb $a_0 = a = 101, a_1 = b = 43$. Els valors trobats són:

$a_0 = a = 101, a_1 = b = 43, a_2 = 15, a_3 = 13, a_2 = 2, a_3 = 0$,

$q_1 = 2, q_2 = 2, q_3 = 1, q_4 = 6$,

$x_0 = 1, x_1 = 0, x_2 = 1, x_3 = -2, x_4 = 3, x_5 = -20$,

$y_0 = 0, y_1 = 1, y_2 = 2, y_3 = -5, y_4 = 7, y_5 = -47$.

Finalment, $1 = -101 \cdot 20 + 43 \cdot 47$ i $1 = 43 \cdot 47 \pmod{101}$.

Per tant, $43^{-1} = 47 \pmod{101}$.

En segon lloc calcularem l'invers de (1,2) en $\mathbb{F}_{3^2}$, en què $\mathbb{F}_{3^2}$ s'ha generat a partir de $f(X) = X^2 + 1$.

El vector (1,2), en forma polinòmica, està representat per $1+2\alpha$, en què $\alpha = [X] \in \mathbb{Z}_3[X]/X^2+1$.

Utilitzant l'algorisme d'Euclides estès entre $X^2 + 1$ i $2X + 1$ obtenim:

$a_0 = a = X^2 + 1, a_1 = b = 2X + 1, a_2 = 2$,

$q_1 = 2X - 1$,

$x_0 = 1, x_1 = 0, x_2 = 1$,

$y_0 = 0, y_1 = 1, y_2 = 2X - 1$.

Finalment, $2 = 1 \cdot (X^2 + 1) - (2X - 1) \cdot (2X + 1)$, o sigui:

$$(2X - 1) \cdot (2X + 1) = 1 \pmod{X^2 + 1}.$$

Per tant, $(1,2)^{-1} = (-1,2)$.

12) Sigui $\alpha \in \mathbb{F}_8$, arrel del polinomi irreductible X^3+X+1. El conjunt $B = \{\alpha,\alpha^2,\alpha^4 = 1+\alpha+\alpha^2\}$ forma una base normal. Pel teorema 2.11 qualsevol altra base B' és de la forma $B' = BC$, amb $C = [c_0,c_1,c_2]$ matriu circulant no singular, és a dir, amb determinant no nul (i per tant, en aquest cas determinant igual a 1).

El problema es redueix, doncs, a trobar tals matrius. Com que els coeficients $c_i \in \{0,1\}$ existeixen 8 matrius circulants. Vegem quines són no singulars:

a) Siguin $c_0 = c_1 = c_2 = 0$: la matriu és òbviament singular (tots els seus coeficients són nuls)

b) Siguin $c_0 = c_1 = c_2 = 1$: la matriu és singular (ja que té les seves tres files iguals).

c) Siguin $c_0 = 1$ i $c_1 = c_2 = 0$: la matriu obtinguda és la identitat, no singular, i tenim $B' = B$.

d) Siguin $c_0 = 0$, $c_1 = 1$, $c_2 = 0$: la matriu obtinguda és

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

matriu no singular que proporciona la base normal $B' = \{\alpha^4,\alpha,\alpha^2\}$ (Noteu que $(\alpha^4)^2 = \alpha^8 = \alpha$.

e) Siguin $c_0 = 0$, $c_1 = 0$, $c_2 = 1$: la matriu obtinguda és

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

matriu no singular que proporciona la base normal $B' = \{\alpha^2,\alpha^4,\alpha\}$

f) Siguin $c_0 = 1$, $c_1 = 1$, $c_2 = 0$: la matriu obtinguda és

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

matriu que és singular

g) Siguin $c_0 = 1$, $c_1 = 0$, $c_2 = 1$: s'obté també una matriu singular.

h) Siguin $c_0 = 0$, $c_1 = 1$, $c_2 = 1$: de nou la matriu obtinguda és singular.

Com a conclusió: existeixen tres bases normals, les $\{\alpha,\alpha^2,\alpha^4\}$, $\{\alpha^4,\alpha,\alpha^2\}$ i $\{\alpha^2,\alpha^4,\alpha\}$. Observeu, no obstant això, que les dues últimes són simplement permutacions de la primera.

13) Si A,B són les matrius associades amb les aplicacions φ_x, φ_y; $x,y \in \mathbb{F}_q$ es té que la matriu associada amb φ_{x+y} és $A+B$, d'on es dedueix i). La matriu associada amb $\varphi_{\lambda x}$ és (λa_{ij}), d'on es dedueix ii). La matriu associada amb $\varphi(\lambda)$ és la matriu diagonal amb λ en tots els elements de la diagonal principal, d'on es dedueix iii).

Les propietats i'), ii') i iii') es dedueixen de la mateixa forma, tenint en compte que la matriu associada a φ_{xy} és AB.

14)

a) L'expressió binària de tots dos nombres és $a = 1100111$, $b = 1000001$. Amb la regla habitual de multiplicació s'obté

$$\begin{array}{rcccccccccccccc} a & = & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ a' & = & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ a+a' = a\cdot b & = & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{array}$$

S'han fet un total de 13 operacions bits (suma de dos nombres binaris de longitud 13). El resultat obtingut és: $2^{12} + 2^{11} + 2^9 + 2^5 + 2^2 + 2 + 1 = 6695$.

b) Tots dos nombres tenen longitud binària k i expressió binària $a = 1a_{k-1} \cdots a_1 a_0$ i $b = 10 \cdots 01$. Com que b només té dos coeficients no nuls (el primer i l'últim), s'hauria de fer la suma de dos nombres binaris de longitud $2k - 1$, i obtenim un nombre amb longitud $2k - 1$ o $2k$, segons els casos, per la qual cosa el nombre d'operacions bits serà com a màxim $2k$.

c) La complexitat per al producte anterior és, doncs, $O(k)$, lineal en la longitud de les dades. La complexitat en el cas general, proposició 3.8, era, no obstant això, $O(k^2)$. Recordeu que el símbol O donava una expressió "en el cas pitjor".

15)

a) L'algorisme ha de calcular una expressió de la forma a^n, $a \in \mathbb{F}_q$, $n \in \mathbb{N}$. La reducció mòdul m en l'algorisme 3.2 s'ha de substituir ara per "operacions" (multiplicacions i quadrats) en el cos finit. Amb aquest canvi s'obté l'algorisme desitjat.

b) L'algorisme exigeix fer, com a màxim, $O(\log(n))$ multiplicacions i $O(\log(n))$ quadrats (a diferència de l'algorisme 3.2, no són necessàries divisions). Com la complexitat d'una multiplicació i un quadrat en $\mathbb{F}_q$ és $O(\log^2 q)$ el cost total serà:

$$O(\log(n))O(\log^2(q)) + O(\log(n))O(\log^2(q)) = O(\log(n)\log^2(q))$$

c) En aquest cas l'expressió binària de n és $5 = 101$. S'haurien, doncs, de fer tres etapes:

- Etapa 1: $s_2 = 1$, aleshores $b := 1 + \alpha$ i $b := (1 + \alpha)^2 = 1 + \alpha^2$.
- Etapa 2: $s_1 = 0$, aleshores $b := (1 + \alpha^2)^2 = 1 + \alpha + \alpha^2$.
- Etapa 3: $s_0 = 1$, aleshores $b := (1 + \alpha)(1 + \alpha + \alpha^2) = \alpha$.

Bibliografia

Koblitz, N. (1994). *A Course in Number Theory and Cryptography, Second Edition*. Nova York: Springer (Graduate Texts in Mathematics, 114).

Lidl, R.; Niederreiter, H. (1997). "Finite Fields". *Encyclopedia of Mathematics and its Applications* (vol. 20, pàg. 2). Cambridge: Cambridge U. Press.

Menezes, A. (ed.) (1993). *Applications of Finite Fields*. Massachusetts: Kluwer Academic Publishers.