TECHNISCHE HOGESCHOOL EINDHOVEN
Afdeling Algemene Wetenschappen
Onderafdeling der Wiskunde

DISCRETE WISKUNDE 2

Prof. Dr. J.H. van Lint

Herfst 1987

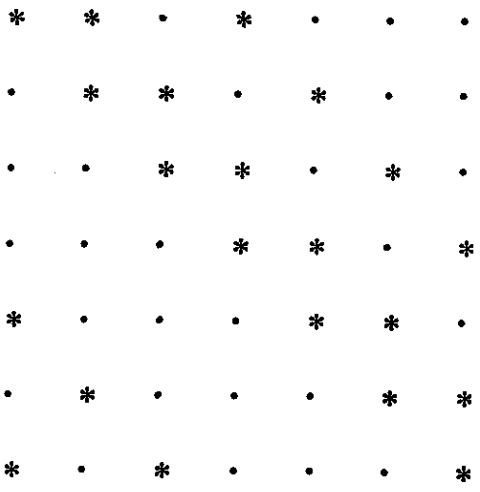
Technische Universiteit
Eindhoven

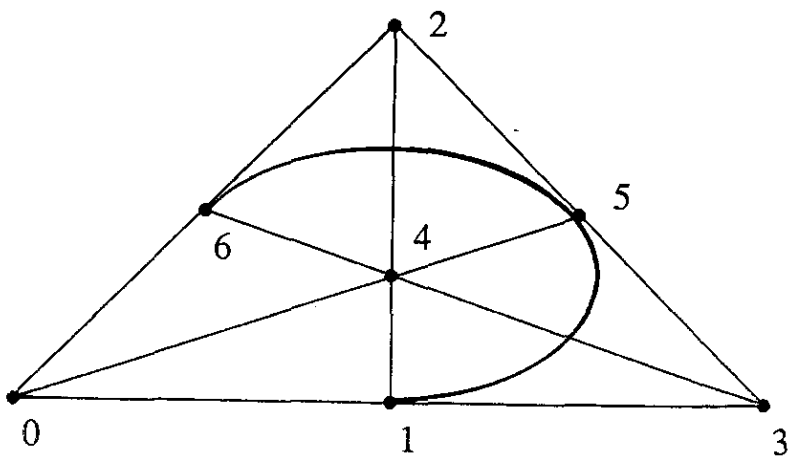
Faculteit der Wiskunde en Informatica

Discrete wiskunde 2

(2F550)

J.H. van Lint





4 002421 000009
Prijs f.4,50

TECHNISCHE UNIVERSITEIT EINDHOVEN

Faculteit Wiskunde en Informatica

DISCRETE WISKUNDE 2

(2F550)

J.H. van Lint

Herfst 1987

Inhoudsopgave

Hoofdstuk 6 De theorie van eindige lichamen

6.0 Definities en notaties voor ringen

WE beginnen met een precieze definitie van ring en lichaam en een aantal notatieafspraken. De meeste lezers zullen met de definities misschien al enigszins vertrouwd zijn. In elk geval veronderstellen we dat de lezer op de hoogte is van het begrip groep en dat hij of zij vertrouwd is met de elementaire lineaire algebra.

6.0.1 Definitie. Laat R een niet-lege verzameling zijn met daarop twee bewerkingen gegeven, optelling (+) en vermenigvuldiging ($\times$). We noemen R een *ring* met deze bewerkingen, als voldaan is aan de volgende axioma's.

1 R is met de optelling een commutatieve groep.
2 De vermenigvuldiging op R is associatief.
3 De distributieve wetten gelden, dat wil zeggen, voor alle a, b en $c \in R$ geldt

$$a \times (b + c) = (a \times b) + (a \times c)$$

$$(b + c) \times a = (b \times a) + (c \times a) \quad .$$

6.0.2 Betreffende notatie. Notatieconventies voor ringen sluiten aan bij wat we bij gewone getallen gewend zijn. We vermelden ze toch maar expliciet voor de zekerheid. We geven het neutrale element voor de optelling aan met 0 (nul) en het tegengestelde van een $a \in R$ met $-a$. Voor $a + (-b)$ schrijven we $a - b$. Voor $a + a$ schrijven we $2 \cdot a$, voor $(2 \cdot a) + a$ schrijven we $3 \cdot a$, enzovoorts. Let op! Deze notatieafspraak wil niet zeggen dat de gehele getallen bevat zijn in R. De notatie $17 \cdot a$ is gewoon een handige afkorting van

$$a + \underbrace{a + \cdots + a}_{} \quad ,$$

waar de accolade 16 summanden samenvat.
We definiëren $1 \cdot a := a$ en $0 \cdot a := 0$. In de laatste formule wordt 0 in twee betekenissen gebruikt, namelijk het gehele getal nul, en het ringelement 0. Algemeen definiëren we voor elke $n, m \in \mathbf{Z}$

$$(-n) \cdot a := n \cdot (-a) \quad ,$$

hetgeen tevens gelijk is aan $-(n \cdot a)$. Er geldt voor $n, m \in \mathbf{Z}$ en $a, b \in R$

$$(n + m) \cdot a = (n \cdot a) + (m \cdot a)$$

$$n \cdot (m \cdot a) = (nm) \cdot a$$

$$(n \cdot a) \times (m \cdot b) = (nm) \cdot (a \times b)$$

$$n \cdot (a + b) = (n \cdot a) + (n \cdot b) \quad .$$

Later zullen we de dikke punt overigens geheel weglaten.
Vermenigvuldigen gaat voor optellen, dat wil zeggen, met

$$a + b \times c$$

bedoelen we

$$a + (b \times c) \quad .$$

Meestal laten we het symbool voor de vermenigvuldiging helemaal weg. De dikke punt zal gelijke rang hebben met de ringvermenigvuldiging, zodat we zonder bezwaar haakjes kunnen weglaten in bovenstaande formules met dikke punt.

Voor aa schrijven we a^2, voor a^2a schrijven we a^3, enzovoorts. We spreken af dat $a^1 := a$.

6.1 Eenvoudige gevolgen van de ringaxioma's

Het is niet moeilijk om bovenstaande rekenregels voor de operatie $\cdot$ af te leiden. De volgende rekenregels geven evenmin problemen.

$$0a = a0 = 0$$

$$(-a)(-b) = ab$$

$$a(-b) = -(ab)$$

voor alle $a, b \in R$. Verder geldt voor alle positieve natuurlijke getallen n en m en alle $a \in R$

$$a^n a^m = a^{n+m}$$

$$(a^n)^m = a^{nm} \quad .$$

Als de vermenigvuldiging commutatief is, spreken we van een commutatieve ring.

6.1.1 Definitie. Laat R een commutatieve ring zijn en $a \in R \setminus \{0\}$. We noemen a een *nuldeler* in R als er een $b \in R \setminus \{0\}$ bestaat met $ab = 0$.

6.1.2 Gevolg. Als $a \in R$ niet nul is en ook geen nuldeler in R, dan geldt voor elke $b, c \in R$

$$ab = ac \text{ impliceert } b = c \quad .$$

We noemen dit ook wel de *schrapwet*.

Bewijs. Veronderstel $ab = ac$. Dan ook $a(b - c) = 0$. Dan $b - c = 0$. □

6.1.3 Definitie. Als R een element $x \neq 0$ bevat zodanig dat voor alle $a \in R$ geldt

$$ax = xa = a \quad ,$$

dan noemen we dat element een *eenheidselement* in R. Zo'n eenheidselement is noodzakelijk uniek, en we noteren het meestal met 1, behalve als het al een bekende naam heeft (bijvoorbeeld e of I). Als de notatie 1 in conflict komt met andere notaties, kiezen we ook een ander symbool voor het eenheidselement.

6.1.4 Voorbeelden van ringen. Er zijn heel veel voorbeelden van ringen. We noemen er enkele. **R**, **Q**, **Z**, de verzameling van 3×3 matrices met gehele coëfficiënten, reële functies gedefinieerd op [0,1], de verzameling van alle voortbrengende functies, de verzameling van alle polynomen met gehele coëfficiënten.
Welke van deze ringen zijn niet commutatief? Welke van de commutatieve bevatten nuldelers?

6.2 Lichaamsdefinitie

6.2.1 Definitie. Laat L een commutatieve ring zijn. We noemen L een *lichaam* als $L \setminus \{0\}$ een groep is voor de vermenigvuldiging.
Deze groep wordt vaak genoteerd als L^*.

6.2.2 Notatie en eenvoudige gevolgen. De inverse van $a \in L \setminus \{0\}$ noteren we als a^{-1} en voor ab^{-1} schrijven we ook wel a/b of $\frac{a}{b}$. We spreken af dat $a^{-3} := (a^{-1})^3$ en evenzo voor andere exponenten. Per definitie stellen we

$$a^0 := 1 \quad ,$$

voor *alle* $a \in L$, dus ook voor nul.
Met deze definities geldt voor alle $a \neq 0$ en alle $n, m \in \mathbf{Z}$

$$a^n a^m = a^{n+m}$$

$$(a^n)^m = a^{nm} \quad .$$

Het is duidelijk dat een lichaam L geen nuldelers bevat omdat $L \setminus \{0\}$ gesloten is voor vermenigvuldiging. Daaruit volgt weer dat voor alle $a, b \in L$ geldt

$$ab = 0 \text{ impliceert } (a = 0 \text{ of } b = 0) \quad .$$

6.2.3 Voorbeelden van lichamen. De verzamelingen **R**, **Q** en **C** zijn lichamen. De gehele getallen vormen geen lichaam, want behalve 1 en –1 heeft geen enkel geheel getal een gehele inverse. Ook een lichaam is de verzameling van alle breuken

$$\frac{p(x)}{q(x)} \quad ,$$

waar $p(x)$ en $q(x)$ polynomen met reële coëfficiënten zijn en bovendien $q(x)$ niet het nulpolynoom. We moeten dan wel afspreken wanneer we twee breuken als gelijk beschouwen: als $p(x)s(x) = q(x)r(x)$, dan vatten we $p(x)/q(x)$ en $r(x)/s(x)$ als gelijk op.

6.2.4 Definitie. Een deelverzameling R' van een ring R die met de optelling en vermenigvuldiging van R weer een ring is (in het bijzonder, als R' gesloten is onder optellen, aftrekken en vermenigvuldigen), noemen we een *deelring* van R. Een deelring L' van een lichaam L noemen we een *deellichaam* als L' ook nog gesloten is onder het nemen van inversen. Een deellichaam is dus een deelverzameling die met dezelfde bewerkingen een lichaam is.

6.2.5 Stelling. Laat $p \in \mathbf{N}$ een priemgetal zijn. Dan is de verzameling van alle congruentieklassen modulo p, met de gebruikelijke optelling en vermenigvuldiging, een lichaam.
Bewijs. Ongeacht of p een priemgetal is of niet, de verzameling congruentieklassen modulo p is een commutatieve ring met eenheidselement (de klasse van 1). Dat is niet moeilijk in te zien. De vraag is of elke klasse ongelijk de nulklasse een inverse heeft. Laat c zo'n klasse zijn en laat $d \in c$. Dat wil zeggen $d \not\equiv 0 \pmod{p}$, dus $\mathrm{GGD}(d, p) = 1$, dus

$$dx + py = 1$$

voor zekere gehele x en y. Met andere woorden,

$$dx \equiv 1 \pmod{p} \quad ,$$

dus de klasse van zo'n x is de inverse van c. □

6.2.6 Voorbeeld. Van elk der klassen modulo 11 geven we zo mogelijk de inverse.

klasse van:	0	1	2	3	4	5	6	7	8	9	10
inverse is klasse van:	–	1	6	4	3	9	2	8	7	5	10

6.2.7 Definitie. Het lichaam bestaande uit de verzameling congruentieklassen modulo een priemgetal p noteren we met $\mathbf{F}_p$ (Engels 'field' betekent lichaam), of ook wel $\mathrm{GF}(p)$ (voor de verklaring van deze notatie zie 6.8.5).
Voor een getal $m > 1$ dat niet priem is, vormen de klassen modulo m een ring.
Die ring wordt wel genoteerd met $\mathbf{Z}_m$ of met $\mathbf{Z}/m\mathbf{Z}$. De ring $\mathbf{Z}_m$ heeft nuldelers als m niet priem is en hij is dan dus geen lichaam. In feite zijn de klassen van de getallen a met

$1 < \mathrm{GGD}(a,m) < m$ juist de nuldelers modulo m.
In het algemeen is het niet zo dat een commutatieve ring zonder nuldelers automatisch ook een lichaam is, denk maar aan $\mathbf{Z}$. We hebben echter de volgende stelling:

6.2.8 Stelling. Laat R een *eindige* commutatieve ring zijn zonder nuldelers en met eenheidselement. Dan is R een lichaam.
Bewijs. Laat $a \in R \setminus \{0\}$. We denken ons even de elementen van R genummerd:

$$r_1, r_2 \cdots, r_n \quad . \tag{1}$$

Beschouw de rij

$$ar_1, ar_2 \cdots, ar_n \quad . \tag{2}$$

De leden van deze rij zijn alle element van R en verder, als $ar_i = ar_j$ dan volgt met de schrapwet dat $r_i = r_j$, dus $i = j$. Hieruit volgt dat in de rij (2) ook n verschillende elementen van R staan. Dat wil zeggen dat alle elementen van R in die rij staan, dus ook 1. Met andere woorden, $ar_k = 1$ voor zekere $r_k \in R$. Dat is de inverse van a. □

6.2.9 Gevolg. Laat L een eindig lichaam zijn en laat $\{0,1\} \subset K \subset L$; veronderstel dat K gesloten is onder optelling en vermenigvuldiging. Dan is K een deellichaam van L.
Bewijs. We hoeven alleen maar aan te tonen dat K een deelring is, want een deelverzameling van een lichaam bevat natuurlijk geen nuldelers. Om aan te tonen dat K een deelring is hoeven we alleen maar te laten zien dat voor alle $a \in K$ er een $b \in K$ is met $a + b = 0$. Maar als t de additieve orde is van a in L, dat wil zeggen $t \cdot a = 0$, dan is $(t-1)\cdot a$ de gezochte b. □

Bovenstaand feit zal later handig blijken.

6.3 De karakteristiek en het priemlichaam

Beschouw in een willekeurig lichaam L de verzameling L', bestaande uit

$$0, 1, 1+1, 1+1+1, \cdots \quad ,$$

enzovoorts, dat wil zeggen

$$L' := \{n\cdot 1 \mid n \in \mathbf{N}\} \quad .$$

Dit is zo'n deelverzameling die gesloten is onder optelling en vermenigvuldiging. De verzameling L' bevat precies evenveel elementen als de additieve orde van 1 bedraagt in L. Als L eindig is dan is L' een deellichaam van L. Als L' niet eindig is, dan is

$$L'' := \{(n\cdot 1)(m\cdot 1)^{-1} \mid n \in \mathbf{Z}, m \in \mathbf{P}\}$$

een lichaam. ($\mathbf{P}$ is de verzameling van de positieve gehele getallen.) In dit geval zeggen we dat L karakteristiek nul heeft.
Voorbeelden van lichamen met karakteristiek nul zijn gegeven in 6.2.3
We veronderstellen nu verder dat L' eindig is. Laat $p > 0$ de additieve orde van 1 zijn in L. Stel dat $p = nm$, dus

$$0 = p\cdot 1 = (mn)\cdot 1 = (m\cdot 1)(n\cdot 1) \quad ,$$

dus $m\cdot 1 = 0$ of $n\cdot 1 = 0$. Daaruit volgt dat $p \mid m$ of $p \mid n$, dus p is een priemgetal. Dit priemgetal noemen we de *karakteristiek* van L, en het lichaam L' noemen we het *priemlichaam* van L. Dit priemlichaam is isomorf met $\mathbf{F}_p$, en we zullen in het vervolg geen onderscheid meer maken tussen $\mathbf{F}_p$ en het priemlichaam van een lichaam met karakteristiek p.

6.4 Lichaam als vectorruimte

6.4.1 Vectorruimten over $\mathbf{F}_p$. In een lichaam L met karakteristiek p geldt voor elke $l \in L$ dat $p \cdot l = (p \cdot 1)l = 0$. Verder is elk lichaam L met karakteristiek p een vectorruimte over $\mathbf{F}_p$. Dit vereist enige toelichting.
L is een commutatieve groep voor de optelling. Voor de definitie van het produkt tussen een scalair $\alpha \in \mathbf{F}_p$ en een $x \in L$ vatten we $\mathbf{F}_p$ op als een deellichaam van L, en dan heeft αx een bekende interpretatie. Voor de vermenigvuldiging met scalairen moet aan de volgende axioma's voldaan zijn.

$$\alpha(x + y) = \alpha x + \alpha y$$
$$(\alpha\beta)x = \alpha(\beta x)$$
$$(\alpha + \beta)x = \alpha x + \beta x$$
$$1x = x \quad .$$

Dit is allemaal in orde wanneer de scalairen een deellichaam vormen. De hele theorie van vectorruimten berust op axioma's voor vectorruimten, en ook op het feit dat de scalairen een lichaam vormen. Als L eindig is, dan is L eindigdimensionaal, opgevat als vectorruimte over $\mathbf{F}_p$. In dat geval is er een positief natuurlijk getal d, de dimensie van L over $\mathbf{F}_p$, en een basis van L, zeg $x_1, \ldots, x_d$, zodanig dat elk element van L op precies één manier te schrijven is als

$$\alpha_1 x_1 + \cdots + \alpha_d x_d$$

met $\alpha_1, \ldots, \alpha_d \in \mathbf{F}_p$. Het is duidelijk dat er p^d mogelijkheden zijn voor het rijtje $\alpha_1, \ldots, \alpha_d \in \mathbf{F}_p$, en dus bevat L precies p^d elementen; we schrijven vaak $L = \mathrm{GF}(p^d)$.

6.4.2 Voorbeeld. Het lichaam van vier elementen is als volgt voor te stellen.

$$\mathrm{GF}(4) := \{0, 1, a, b\}$$

met de volgende opteltabel

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

en als vermenigvuldigingstabel:

×	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

We kunnen elk tweetal uit $\{1, a, b\}$ als basis nemen. Als we 1 en a als basis nemen, dan kunnen we b als $a + 1$ schrijven. Merk op dat door de regel $a^2 = a + 1$ de vermenigvuldiging is vastgelegd.

6.5 Polynoomringen over een lichaam

6.5.1 Inleiding. Laat L een lichaam zijn. We noteren met $L[x]$ de verzameling van alle polynomen in een variabele x en coëfficiënten in L. Elementen van $L[x]$ geven we aan met $p(x)$, $l(x)$, $f(x)$, enzovoorts, net als bij voortbrengende functies.
Opgelet! Polynomen zijn geen functies in de gebruikelijke zin. Bijvoorbeeld, x^2 en x nemen op $\mathbf{F}_2$ dezelfde waarden aan, maar we beschouwen ze als verschillende polynomen over $\mathbf{F}_2$.
Elk polynoom $l(x) \in L[x]$ kan worden geschreven als

$$l(x) = l_0 + l_1 x + \cdots + l_n x^n \quad ,$$

waar $l_0, \ldots, l_n \in L$ de coëfficiënten van $l(x)$ zijn. Wij schrijven hier de machten van x van laag naar hoog, zoals bij voortbrengende functies, maar dat is niet verplicht. In feite zullen we vaak met de hoogste macht van x beginnen. Een coëfficiënt 1 voor een positieve macht van x schrijven we meestal niet, en termen met coëfficiënt 0 laten we meestal geheel weg. Als $l_n \neq 0$, dan noemen we n de *graad* van $l(x)$, en we schrijven ook wel $n = \text{graad}(l(x))$. De coëfficiënt l_n noemen we de *hoogste* coëfficiënt, van $l(x)$ in dit geval. De term *kop*coëfficiënt is hiervoor ook heel gebruikelijk. Een polynoom van de graad 0 noemen we ook wel een *constante* of *constant polynoom*. Als de hoogste coëfficiënt van een polynoom 1 is, noemen we het polynoom (met een niet zo mooi woord) *monisch*. De graad van het nulpolynoom definiëren we als -1. Ook 0 zullen we een constante noemen. De verzameling $L[x]$ vormt met de gebruikelijke optelling en vermenigvuldiging van polynomen een ring. De verzameling van constante polynomen in $L[x]$ is een deelring van $L[x]$, isomorf met L. We zullen in het vervolg geen onderscheid meer maken tussen constante polynomen in $L[x]$ en elementen van L.

6.5.2 Stelling. (Deling met rest) Laat L een lichaam zijn. Voor elk polynoom $a(x) \in L[x]$ en elk polynoom $b(x) \in L[x]$ ongelijk het nulpolynoom zijn er polynomen $q(x)$ en $r(x)$ met

$$a(x) = q(x)b(x) + r(x)$$

en $\text{graad}(r(x)) < \text{graad}(b(x))$.
Bewijs. (Schets) Met inductie naar de graad van $a(x)$. Als $\text{graad}(a(x)) < \text{graad}(b(x))$ dan is het al heel eenvoudig. Als a_n en b_m de hoogste coëfficiënt voorstellen van respectievelijk $a(x)$ en $b(x)$, dan geldt

$$a(x) = \frac{a_n}{b_m} x^{n-m} b(x) + c(x) \quad ,$$

waar $\text{graad}(c(x)) < \text{graad}(a(x))$. □
Bovenstaande stelling is precies wat we nodig hebben om de theorie van GGD en ontbinding in priemfactoren uit de elementaire getaltheorie na te spelen in $L[x]$. We brengen in herinnering dat niet-constante polynomen die niet ontbonden kunnen worden in factoren van lagere graad *irreducibel* worden genoemd. De stelling over ontbinding in irreducibele factoren luidt:

6.5.3 Stelling. (Ontbindingsstelling) Elk polynoom $l(x) \in L[x]$ ongelijk het nulpolynoom is te ontbinden als een produkt

$$c_0 P_1(x) \cdots P_k(x) \quad ,$$

waarin c_0 een constante is en waarin $P_1(x), \ldots, P_k(x)$ irreducibele monische polynomen zijn van positieve graad. Deze ontbinding is uniek op de volgorde van de factoren $P_1(x), \ldots, P_k(x)$ na. □
Alle polynomen van de vorm

$$-\alpha + x$$

met $\alpha \in L$ zijn irreducibel, en andere monische polynomen van de eerste graad zijn er niet. Laat $a(x) \in L[x]$ een willekeurig polynoom zijn, en $\alpha \in L$. Op grond van de reststelling geldt dan

$$a(x) = q(x)(x - \alpha) + r_0$$

voor een constante r_0. We hoeven de deling niet uit te voeren om r_0 te bepalen. We substitueren voor de formele variabele x het lichaamselement α en dan vinden we $r_0 = a(\alpha)$. Het feit dat de rest na deling door $x - \alpha$ juist $a(\alpha)$ is wordt ook wel de *reststelling* genoemd. Het resultaat is dus

6.5.4 Stelling. Laat $a(x) \in L[x]$ en $\alpha \in L$. Het polynoom $x - \alpha$ is een factor van $a(x)$ als en alleen als $a(\alpha) = 0$. []

Bijvoorbeeld, als we rekenen in $\mathbf{Q}[x]$, dan is $x - 1$ een factor van $x^n - 1$ voor elke $n > 0$, en $x + 1$ is een factor van $x^n + 1$ als n oneven is.

We noemen een element $\alpha \in L$ een *nulpunt* van $a(x) \in L[x]$ wanneer $a(\alpha) = 0$. We zeggen ook wel dat α een *wortel* is van de *vergelijking* $a(x) = 0$. We hebben zojuist gezien dat α nulpunt is van $a(x)$ als en alleen als $x - \alpha$ een deler is van $a(x)$. Het aantal factoren $x - \alpha$ in $a(x)$ noemen we dan de *multipliciteit* van het nulpunt α.

Een belangrijk gevolg is

6.5.5 Stelling. Een polynoom $a(x) \in L[x]$ van niet-negatieve graad n heeft ten hoogste n nulpunten.

Bewijs. Het polynoom $a(x)$ heeft ten hoogste zoveel nulpunten als irreducibele factoren van de eerste graad. []

6.5.6 Gevolg. Als van een n-de graads monisch polynoom n nulpunten $\alpha_1, \ldots, \alpha_n$ gegeven zijn, dan ligt dat polynoom ook vast, het is

$$\prod_{i=1}^{n}(x - \alpha_i) \quad .$$

Bovenstaande stelling hebben we al gebruikt, namelijk bij het bewijs dat de multiplicatieve groep van een eindig lichaam cyclisch is (zie 4.3.3.1).

6.6 Constructie

6.6.1 Modulorekenen in $L[x]$. Als $m \geq 2$ een geheel getal is, kunnen we rekenen modulo m. We rekenen dan met klassen modulo m, al laten we dat in de notatie niet altijd merken. Twee getallen zitten in dezelfde klassen modulo m, als ze een veelvoud van m verschillen. Zo ontstaat een ring, zoals we al opmerkten. We zagen ook al dat als m niet priem is, die ring nuldelers heeft, en anders is die ring een lichaam.

Precies zo gaat het in de ring $L[x]$, als L een lichaam is. Laat $l(x)$ een irreducibel polynoom zijn uit $L[x]$. Voor elk polynoom $h(x) \in L[x]$ noteren we de klasse van $h(x)$ met $\langle h(x) \rangle$. Die klasse bestaat uit alle polynomen uit $L[x]$ die met $h(x)$ een veelvoud van $l(x)$ verschillen. Elementen van een klasse heten ook wel representanten van die klasse.

Bijvoorbeeld, als L het lichaam $\mathbf{F}_2$ is, en $l(x) = x^2 + x + 1$ dan zitten x^2 en $x + 1$ in dezelfde klasse. De polynomen $x^3 + x$ en $x + 1$ zijn representanten van dezelfde klasse.

De verzameling van alle klassen noteren we met $L[x]/(l(x))$. Elke klasse bevat precies één polynoom van laagste graad. Deze graad is kleiner dan de graad van $l(x)$. Dit polynoom van laagste graad noemen we de standaardrepresentant van de klasse. Elk polynoom van graad kleiner dan de graad van $l(x)$ is een standaardrepresentant van precies één klasse modulo $l(x)$.

Tussen klassen definiëren we optelling en vermenigvuldiging als volgt.

$$\langle h(x)\rangle + \langle g(x)\rangle := \langle h(x) + g(x)\rangle$$

$$\langle h(x)\rangle \times \langle g(x)\rangle := \langle h(x) \times g(x)\rangle \quad .$$

We gebruiken hetzelfde symbool voor de optelling van polynomen als voor de optelling van klassen. Dit zal meestal geen verwarring geven. Omdat $l(x)$ irreducibel is, heeft $L[x]/(l(x))$ geen nuldelers. In geval L een eindig lichaam is, volgt dan al meteen dat $L[x]/(l(x))$ een lichaam is. Immers, er zijn dan maar een eindig aantal standaardrepresentanten.
Hiermee hebben we nog geen efficiënte manier om de inverse van een klasse ongelijk de nulklasse te bepalen. Ook als L niet eindig is, is $L[x]/(l(x))$ een lichaam, en we geven hier een constructief bewijs voor.
Laat $\langle h(x)\rangle$ niet de nulklasse zijn. Dan is $l(x)$ geen factor van $h(x)$, en dus zijn $l(x)$ en $h(x)$ relatief priem. Dit betekent dat voor geschikte polynomen $p(x)$ en $q(x)$ geldt

$$h(x)p(x) + l(x)q(x) = 1 \quad .$$

Het polynoom $p(x)$ kan geconstrueerd worden met behulp van het algoritme van Euclides. Bovenstaande gelijkheid betekent dat

$$\langle h(x)\rangle \langle p(x)\rangle = \langle 1\rangle \quad ,$$

waarmee we de inverse van de klasse van $h(x)$ geconstrueerd hebben.

6.6.2 Notatieafspraken. Net als bij de gehele getallen zullen we nu verder in de notatie het onderscheid laten vervallen tussen klassen en hun representanten. In plaats van over de standaardrepresentant zullen we verder spreken van de standaardvoorstelling van een element van $L[x]/(l(x))$. Het berekenen van die standaardvoorstelling noemen we *reduceren*.

6.6.3 Voorbeelden

1 We nemen voor L het lichaam $\mathbf{F}_2$ en voor $l(x)$ nemen we $x^2 + x + 1$. De standaardvoorstellingen van de elementen van $\mathbf{F}_2[x]/(x^2 + x + 1)$ zijn

$$0,\ 1,\ x,\ x + 1 \quad .$$

Het polynoom x^2 reduceert tot $x + 1$.

2 We nemen voor L het lichaam $\mathbf{F}_3$ en voor $l(x)$ nemen we $x^2 + 1$. Dit polynoom is irreducibel over $\mathbf{F}_3$, omdat het geen nulpunten heeft in $\mathbf{F}_3$, zoals men door substitutie eenvoudig kan nagaan.
In $\mathbf{F}_3[x]/(x^2 + 1)$ geldt bijvoorbeeld

$$(x + 1) + (x + 2) = 2x$$

$$(x + 1)(x + 2) = x^2 + 2 = 1 \quad .$$

Dit lichaam heeft 9 elementen.

3 We nemen voor L het lichaam $\mathbf{R}$ en voor $l(x)$ nemen we weer $x^2 + 1$. Het is bekend dat de vergelijking

$$x^2 + 1 = 0$$

geen wortels heeft in $\mathbf{R}$. De elementen van $\mathbf{R}[x]/(x^2 + 1)$ hebben de volgende voorstelling:

$$a + bx \quad ,$$

met a en b reëel. Er geldt

$$(a + bx) + (c + dx) = a+c + (b+d)x \quad ;$$
$$(a + bx)(c + dx) = ac + (bc+ad) + bdx^2$$
$$= (ac - bd) + (bc + ad)x + bd(x^2 + 1)$$
$$= (ac - bd) + (bc + ad)x \quad .$$

We zien dat we op deze manier met de elementen van dit lichaam rekenen als met de complexe getallen: schrijf overal i in plaats van x in de standaardvoorstelling.
Het idee de complexe getallen zo op te vatten is door A.L. Cauchy gepubliceerd in 1847.

6.7 Eindige lichamen

6.7.1 Eigenschappen. We gaan nu de eindige lichamen nauwkeuriger onderzoeken. We vatten samen wat we al wisten over eindige lichamen.
Laat L een eindig lichaam zijn.

1 De karakteristiek van L is een priemgetal; als we dit met p aanduiden, dan heeft L een deellichaam L_p isomorf met $\mathbf{F}_p$ (het lichaam van congruentieklassen modulo p). Dit deellichaam heet ook wel het priemlichaam.
2 L is een vectorruimte over $\mathbf{F}_p$ en daarom heeft L precies p^r elementen voor zekere $r > 0$.
3 $L \setminus \{0\}$ is een cyclische groep voor de vermenigvuldiging in L.

Van dit laatste feit brengen we het bewijs in herinnering: als $|L^*| = n$, dan zijn er precies d elementen $l \in L$ met $l^d = 1$, als $d \mid n$, en als elementen bestaan van orde d in L^*. Onder die elementen zijn er dan $\phi(d)$ met orde d in $L \setminus \{0\}$. Netjes tellen levert dan dat elke deler van n ook moet voorkomen als orde van een element van L. Dus er zijn elementen van orde n in $L \setminus \{0\}$. In de groepentheorie noemen we zulke elementen voortbrengers van de groep, in de theorie van eindige lichamen heten zulke elementen *primitief*. Een lichaam van p^r elementen heeft dus $\phi(p^r - 1)$ primitieve elementen.

6.7.2 Voorbeelden

1. In $\mathbf{F}_3[x]/(x^2 + 1)$ is x niet primitief, want $x^4 = 1$ in dit lichaam; de vier elementen $\pm x \pm 1$ zijn wel primitief.

2. In $\mathbf{F}_{11}$ is 2 primitief, maar bijvoorbeeld 4 en 10 zijn niet primitief.

3. Laat een lichaam L met q elementen gegeven zijn en een element α van L^*. Dan is α primitief als en alleen als de orde van α precies $q - 1$ is. Echter, we weten al dat

$$\alpha^{q-1} = 1 \quad .$$

Dus de orde van α is een deler van $q - 1$. Om vast te stellen of α geen lagere orde heeft, hoeven we alleen maar α^k te berekenen voor echte delers k van $q - 1$.
Bijvoorbeeld, $x^6 + x + 1$ is irreducibel over $\mathbf{F}_2$ en x is primitief in $\mathbf{F}_2[x]/(x^6 + x + 1)$. Dat $x^6 + x + 1$ irreducibel is, kunnen we inzien door op te merken dat dit polynoom geen irreducibele factoren heeft van graad 1, 2 en 3.
We berekenen aan aantal machten van x:

$$x^7 = (x^6)x = x^2 + x$$
$$x^9 = x^4 + x^3$$
$$x^{18} = (x + 1)^3 = x^3 + x^2 + x + 1$$
$$x^{21} = x^6 + x^5 + x^4 + x^3$$

$$= x^5 + x^4 + x^3 + x + 1$$

Natuurlijk heeft x geen orde 3 of 1, dus de orde van x is 63, dat wil zeggen x is primitief.
3. Het is beslist niet zo dat in een lichaam

$$\mathrm{GF}(2)[x]/(q(x))$$

x of $x + 1$ primitief is. Rekenen in kleine lichamen kan wel die indruk wekken, maar we laten aan een voorbeeld zien dat die indruk niet correct is.
We nemen

$$\begin{aligned} q(x) &:= x^8 + x^6 + x^5 + x^4 + x^3 + x + 1 \\ &= (x^2 + x)^4 + (x^2 + x)^3 + (x^2 + x)^2 + (x^2 + x) + 1 \\ &= \frac{(x^2 + x)^5 + 1}{x^2 + x + 1} \end{aligned}$$

Dit polynoom is irreducibel en het is een factor van

$$x^{16} + x + 1 \quad .$$

Dus

$$x^{16} \equiv x + 1$$

en bijgevolg

$$x^{85} \equiv x^{80}x^5 \equiv (x + 1)^5 x^5 \equiv (x^2 + x)^5 \equiv 1 \quad ,$$

alles modulo $q(x)$. De orde van x is dus een deler van 85, maar omdat $x^{17} \equiv x^2 + x$ volgt dat die orde niet 1 of 17 is, en 5 is zij ook al niet, dus de orde van x is 85.
Nu is $x^2 + x$ invariant onder de substitutie van $x + 1$ voor x. Daarom is de orde van $x + 1$ ook 85.
Het is niet moeilijk om na te rekenen dat de tweedegraadspolynomen x^2, $x^2 + 1$, $x^2 + x$ en $x^2 + x + 1$ ordes hebben gelijk aan respectievelijk 85, 85, 5 en 15. Het polynoom $x^3 + x + 1$ heeft orde 255.

6.7.3 Definitie. Als L een eindig lichaam is en $l(x) \in L[x]$ is een irreducibel polynoom dan noemen we het polynoom $l(x)$ *primitief* als (de klasse van) x een primitief element is van het lichaam $L[x]/(l(x))$.
We zullen in 6.11 zien dat primitieve polynomen handig zijn voor de constructie van een vereenvoudigde vermenigvuldigingstabel van het lichaam, de zogeheten logaritmentabel.

6.7.4. Voorbeelden.
1. Het polynoom $x^2 + 1$ is niet primitief over $\mathbf{F}_3$; het is overigens het enige niet-primitieve irreducibele polynoom van de tweede graad over $\mathbf{F}_3$.

2. Alle zes irreducibele polynomen van graad 5 over $\mathbf{F}_2$ zijn primitief, omdat voor een dergelijk polynoom $l(x)$ de multiplicatieve groep van het lichaam $\mathbf{F}_2[x]/(l(x))$ 31 elementen heeft, en dus zijn in zo'n lichaam alle elementen behalve 0 en 1 primitief.
Een feit dat meteen volgt uit het bovenstaande is het volgende.

6.7.5 Stelling. Laat L een eindig lichaam zijn met q_1 elementen en laat K een deellichaam zijn van L met q_2 elementen. Dan is q_1 een macht van q_2.
Bewijs 1. L is een vectorruimte over K.
Bewijs 2. Noem de karakteristiek van L even p, dan geldt voor zekere positieve gehele r en k dat $q_1 = p^r$ en $q_2 = p^k$. Omdat $K \setminus \{0\}$ voor de vermenigvuldiging een ondergroep is van $L \setminus \{0\}$ geldt $(p^k - 1) \mid (p^r - 1)$ waaruit volgt $k \mid r$, zeg $r = tk$. Maar dan $q_2^t = q_1$. □

6.7.6 Voorbeeld. Het lichaam $\mathbf{F}_2[x]/(x^6 + x + 1)$ heeft 64 elementen en het heeft een deellichaam van 2 elementen (het priemlichaam), maar ook van 4 en 8 elementen.
Bijvoorbeeld,

$$x^{21} = x^5 + x^4 + x^3 + x + 1 \quad ,$$

en dus (gebruik freshman's dream)

$$\begin{aligned} x^{42} &= x^{10} + x^8 + x^6 + x^2 + 1 \\ &= x^4(x + 1) + x^2(x + 1) + x + 1 + x^2 + 1 \\ &= x^5 + x^4 + x^3 + x = x^{21} + 1 \quad . \end{aligned}$$

Als we even definiëren $\alpha := x^{21}$, dan geldt duidelijk

$$\alpha^2 = \alpha + 1 \quad ,$$

dus

$$\{0, 1, \alpha, \alpha + 1\}$$

is een deellichaam. De optel- en vermenigvuldigingstabel zien er precies zo uit als die van het lichaam van 4 elementen in Voorbeeld 6.4.2.

6.7.7 Voorbeeld. Een lichaam van 8 elementen heeft alleen maar het priemlichaam als deellichaam.

6.8 Bestaan van lichamen en deellichamen

6.8.1 De basisformule. We vragen ons af of er wel voor alle toegestane aantallen lichamen en deellichamen bestaan. Preciezer: laat $q = p^r$ een positieve macht van een priemgetal p zijn. Bestaat er een lichaam van q elementen, en zo ja heeft dit voor elke deler k van r een deellichaam van p^k elementen?
Het antwoord op de eerste vraag is al gegeven. We gaven het aantal irreducibele polynomen over $\mathbf{F}_2$ van graad $k > 0$ aan met d_k, en we hebben afgeleid dat

$$2^r = \sum_{k \mid r} k d_k \quad ,$$

waar over k wordt gesommeerd. Een analoge formule geldt voor het aantal $D_{p,r}$ van irreducibele veeltermen van graad r over $\mathbf{F}_p$ met p priem

$$p^r = \sum_{k \mid r} k D_{p,k} \quad .$$

Daaruit concluderen we als tevoren dat er irreducibele polynomen van graad r bestaan voor elke $r > 0$:
Omdat $D_{p,1} = p$ geldt $kD_{p,n} < p^n$ voor elke $n > 1$, en dan volgt dat de r-de summand van bovenstaande formule niet nul kan zijn.
Deze formule vertelt ons echter veel meer! Als we goed kijken vertelt deze formule ons dat voor elke positieve r het lichaam van p^r elementen in wezen uniek is. We noteren dit lichaam voortaan met $\mathrm{GF}(p^r)$, zoals we al hadden vermeld in 6.4.1, en we identificeren $\mathbf{F}_p$ met $\mathrm{GF}(p)$.
De formule vertelt ons verder dat voor elke k die r deelt, $\mathrm{GF}(p^k) \subset \mathrm{GF}(p^r)$. Voor we dit alles kunnen inzien, moeten we nog wat theorie bedrijven.

6.8.2 Deellichamen voortgebracht door een element. Laat L een eindig lichaam zijn met karakteristiek p en met p^r elementen. Laat α een willekeurig element zijn van L. In de rij

$$1, \alpha, \alpha^2, \ldots, \alpha^r$$

komt een element voor dat een lineaire combinatie is van zijn voorgangers in de rij, met coëfficiënten in $\mathbf{F}_p$. Immers, L is een r-dimensionale vectorruimte over $\mathbf{F}_p$. Laat α^k het eerste element in de rij zijn dat een lineaire combinatie is van $1, \alpha, \ldots, \alpha^{k-1}$. Dan geldt

$$l_0 + l_1\alpha + \cdots + l_{k-1}\alpha^{k-1} + \alpha^k = 0$$

voor zekere $l_0, \ldots, l_{k-1} \in \mathbf{F}_p$.
We schrijven

$$l_\alpha(X) = l_0 + l_1X + \cdots + l_{k-1}X^{k-1} + X^k \quad ,$$

waar we X als formele variabele gebruiken (om verwarring te voorkomen met een x die misschien al gebruikt is voor de constructie van L). Er geldt natuurlijk $l_\alpha(\alpha) = 0$. Het polynoom $l_\alpha(X)$ is irreducibel over $\mathbf{F}_p$, want uit een echte ontbinding $l_\alpha(X) = m(X)n(X)$ volgt $m(\alpha) = 0$ of $n(\alpha) = 0$, in tegenspraak met de minimaliteit van k. Het polynoom $l_\alpha(X)$ heet het *minimaalpolynoom* van α.
De deelring van L die bestaat uit alle lineaire combinaties van $1, \alpha, \ldots, \alpha^{k-1}$ is nuldelervrij en is dus een deellichaam, L is immers eindig. Dit deellichaam heeft p^k elementen, en daaruit volgt dat $k \mid r$. Met de lineaire combinaties van $1, \alpha, \ldots, \alpha^{k-1}$ rekenen we op precies dezelfde manier als met de standaardvoorstellingen van elementen van $\mathbf{F}_p[X]/(l_\alpha(X))$. We hebben dus

6.8.3 Stelling. Laat L een eindig lichaam zijn met karakteristiek p en $q = p^r$ elementen. Elke $\alpha \in L$ is nulpunt van een uniek irreducibel monisch polynoom l_α met coëfficiënten in $\mathbf{F}_p$ van positieve graad k, waar k een deler is van r. Dan is α bevat in een deellichaam L' van p^k elementen. Het deellichaam L' is isomorf met $\mathbf{F}_p[X]/(l_\alpha(X))$. []
Opmerking. Als $k > 0$, dan is k een deler van r, zoals we al zagen in 6.7.5.

6.8.4 Definitie. Het polynoom $l_\alpha(X)$ als in bovenstaande stelling noemen we het *minimaalpolynoom* van α.

6.8.5 Gevolg. Voor p priem en $r > 0$ is elk lichaam van orde p^r isomorf met elk der lichamen

$$\mathbf{F}_p[X]/(l(X))$$

waar $l(x)$ een irreducibel polynoom voorstelt van graad r met coëfficiënten in $\mathbf{F}_p$. []
We vinden dus dat er in wezen maar één eindig lichaam van gegeven orde is, maar dat de voorstelling van zo'n lichaam door middel van polynomen op heel veel manieren kan gebeuren.
Daarom stellen we ons meestal voor dat met $\mathbf{F}_q$ of GF (q) één enkele verzameling wordt bedoeld.
De notatie GF is afgeleid van Galois Field.
De Fransman Evariste Galois (1811-1832) was een van de grondleggers van de moderne algebra. Hij overleed op 20-jarige leeftijd aan de verwondingen die hij bij een duel opliep.

6.8.6 Het polynoom dat overal nul is. Beschouw nu het produkt $k(X)$ van *alle* irreducibele monische polynomen die voorkomen als $l_\alpha(X)$ voor de een of andere $\alpha \in L$. Voor alle α geldt $k(\alpha) = 0$, dus $k(X)$ heeft q nulpunten, en dus is de graad van $k(X)$ ten minste gelijk aan q. Aan de andere kant, de graad van $k(X)$ is ten hoogste gelijk aan

$$\sum_{k \mid r} kD_{p,k} = p^r = q \quad ,$$

dus de graad van $k(X)$ is precies q.

Er is echter maar één monisch q-degraadspolynoom dat de hele L als nulpuntenverzameling heeft, en dat is

$$\prod_{\alpha \in L}(X - \alpha) \quad .$$

Omdat voor alle $\alpha \in L$ geldt $\alpha^q = \alpha$, geldt tevens dat $X^q - X$ de hele L als nulpuntenverzameling heeft, en dus

$$k(X) = \prod_{\alpha \in L}(X - \alpha) = X^q - X \quad .$$

Als we nu nog eens naar onze formule kijken, zien we dat elk irreducibel polynoom met graad een deler van r ook voorkomt als $l_\alpha(X)$, anders zou de graad van $k(X)$ geen q kunnen zijn. Als we de nulpunten van het produkt $k(X)$ tellen, zien we dat elke factor $l_\alpha(X)$ niet alleen ten hoogste graad$(l_\alpha(X))$ nulpunten heeft, maar dat zo'n factor er ook precies zoveel heeft, anders zou $k(X)$ er niet genoeg hebben.
Het gevolg hiervan is dat er voor elke deler k van r ook een irreducibele factor $l(X)$ van $X^q - X$ is van graad k. Bij deze irreducibele factor zijn er k elementen $\alpha \in L$ met $l(\alpha) = 0$. Het kleinste deellichaam van L dat zo'n α bevat heeft p^k elementen.

6.8.7 Voorbeeld. Laat L een lichaam met 16 elementen zijn. De karakteristiek van L is dan 2. Elk element van L is nulpunt van

$$X^{16} - X \quad ,$$

hetgeen gelijk is aan $X^{16} + X$, omdat de karakteristiek 2 is. We kunnen dit gemakkelijk in factoren ontbinden, als volgt. We merken op dat $X^{16} + X = X\,(X^{15} + 1)$, en dat dus $X^{16} + X$ zowel een factor $X^5 + 1$ als een factor $X^3 + 1$ heeft. Zo vinden we de ontbinding

$$X\,(X+1)\,(X^2+X+1)\,(X^4+X^3+X^2+X+1)\,(X^4+X^3+1)\,(X^4+X+1)$$

van $X^{16} + 1$.
Het lichaam L bevat dus bijvoorbeeld 4 elementen α met de eigenschap

$$\alpha^4 + \alpha + 1 = 0 \quad ,$$

maar ook 2 elementen $\beta_{1,2}$ die allebei voldoen aan

$$\beta^2 + \beta + 1 = 0$$

en die beide liggen in het deellichaam met 4 elementen. Dit deellichaam bestaat in feite uit

$$\{0, 1, \beta_1, \beta_2\} \quad .$$

6.8.8 Voorbeeld. Rekenende over $\mathbf{F}_2$ vinden we dat $X^{128} + X$ het produkt is van alle irreducibele polynomen met graad een deler van 7, dat wil zeggen

$$X^{128} + X = X\,(X + 1)\sum_{i=0}^{126} X^i \quad ,$$

en de laatste factor is het produkt van alle 18 irreducibele zevendegraadspolynomen.
We keren terug naar het vorige voorbeeld. Als we een α kiezen die voldoet aan $\alpha^4 + \alpha + 1 = 0$, dan kunnen we elk element van L voorstellen als

$$\varepsilon_0 + \varepsilon_1\alpha + \varepsilon_2\alpha^2 + \varepsilon_3\alpha^3 \quad ,$$

waar $\varepsilon_i \in \{0, 1\}$ voor $i = 0,1,2,3$. Met deze voorstellingen van elementen kunnen we gemakkelijk rekenen, omdat $\alpha^4 = \alpha + 1$. Dat betetekent dat L isomorf is met

$$L' := \mathbf{F}_2[X]/(X^4 + X + 1) \quad .$$

6.8.9 Voorbeeld. Er geldt

$$\mathbf{F}_2[x]/(x^3 + x + 1) \cong \mathbf{F}_2[y]/(y^3 + y^2 + 1) \quad .$$

We maken een tabel van de lichaamselementen van beide lichamen. Zie het einde van deze paragraaf. We laten 0 weg uit die tabel.
In beide voorstellingen (met de x en de y) vormt het bovenste drietal de verzameling nulpunten van het polynoom

$$X^3 + X + 1$$

en analoog hoort het onderste drietal bij

$$X^3 + X^2 + 1 \quad .$$

Als we de elementen op eenzelfde rij met elkaar laten corresponderen krijgen we een isomorfisme van het ene lichaam met het andere. Dit is eenvoudig in te zien door hetzij de substitutie van $y + 1$ voor x, hetzij de substutie van $x + 1$ voor y uit te voeren.
Hier is de tabel:

$x^0 =$	1	1	$= y^0$
$x^1 =$	x	$y + 1$	$= y^5$
$x^2 =$	x^2	$y^2 + 1$	$= y^3$
$x^4 =$	$x^2 + x$	$y^2 + y$	$= y^6$
$x^3 =$	$x + 1$	y	$= y^1$
$x^6 =$	$x^2 + 1$	y^2	$= y^2$
$x^5 =$	$x^2 + x + 1$	$y^2 + y + 1$	$= y^4$

6.9 Karakterisering van deellichamen

We hebben al opgemerkt dat voor p priem en positieve gehele k en r met $k \mid r$ geldt

$$\mathrm{GF}(p^k) \subset \mathrm{GF}(p^r) \quad .$$

We gaan het deellichaam $\mathrm{GF}(p^k)$ van $\mathrm{GF}(p^r)$ nog eens op een andere manier kenschetsen.
Voor elke $\alpha \in \mathrm{GF}(p^k)$ geldt

$$\alpha^{p^k} = \alpha \quad ,$$

dus de p^k elementen van $\mathrm{GF}(p^k)$ vormen juist alle nulpunten van het polynoom

$$X^{p^k} - X \in \mathbf{F}_p[X] \quad .$$

Dat betekent dat $\mathrm{GF}(p^k)$ juist de hele nulpuntenverzameling is van dit polynoom, want meer dan p^k nulpunten heeft dit polynoom niet. Met andere woorden

$$\mathrm{GF}(p^k) = \{\alpha \in \mathrm{GF}(p^r) \mid \alpha^{p^k} = \alpha\}$$

en in het bijzonder

$$\mathrm{GF}(p) = \{\alpha \in \mathrm{GF}(p^r) \mid \alpha^p = \alpha\} \quad .$$

6.10 Nulpunten van polynomen over het priemlichaam

6.10.1 De p-de machten van nulpunten. We beginnen met op te merken dat voor een eindig lichaam L met karakteristiek p geldt

$$(\alpha\beta)^p = \alpha^p \beta^p \quad \text{voor alle } \alpha, \beta \in L \quad ,$$

en, wegens de freshman's dream,

$$(\alpha + \beta)^p = \alpha^p + \beta^p \quad .$$

Daarom is de afbeelding

$$A_p : \alpha \to \alpha^p$$

een automorfisme van L op L. Dit automorfisme noemt men vaak het *Frobeniusautomorfisme*. We kunnen A_p voortzetten tot een afbeelding

$$A_p : L[X] \to L[X] \quad ,$$

door $A_p(X) := X$ te definiëren, en in het algemeen

$$A_p(l_0 + l_1X + \cdots + l_tX^t) := l_0^p + l_1^pX + \cdots + l_t^pX^t \quad .$$

De uitgebreide A_p is weer een isomorfisme van de polynoomring $L[X]$ op zichzelf. Het isomorfisme A_p heeft de eigenschap dat A_p de elementen van $\mathbf{F}_p$ elk op zichzelf afbeeldt, en de elementen van $\mathbf{F}_p[X]$ worden ook door A_p op zichzelf afgebeeld.
Laat $l(X) \in \mathbf{F}_p[X]$ en veronderstel dat $\alpha \in L$ een nulpunt is van $l(X)$. Dan volgt uit $l(\alpha) = 0$ dat

$$(l(\alpha))^p = 0$$

en dus ook dat

$$l(\alpha^p) = 0 \quad .$$

Met andere woorden, mèt α is ook α^p een nulpunt van $l(X)$. Het isomorfisme A_p permuteert dus de nulpunten van elk polynoom onderling. In het hierboven besproken voorbeeld van GF(8) zien we dat kwadrateren in elk verticaal lijstje van 3 elementen een cyclische permutatie teweegbrengt.
We bewijzen nu een omkering van wat we zojuist gevonden hebben.

6.10.2 Stelling. Laat L een eindig lichaam zijn met karakteristiek p en laat $l(X)$ een monisch polynoom zijn in $L[X]$, dat in eerstegraadsfactoren ontbonden kan worden over L. Als geldt dat voor elk nulpunt α van $l(X)$ ook α^p nulpunt is van $l(X)$ met dezelfde multipliciteit, dan geldt $l(X) \in \mathbf{F}_p[X]$, met andere woorden, de coëfficiënten van $l(X)$ liggen in $\mathbf{F}_p$.
Bewijs. We veronderstellen dat de graad van $l(X)$ gelijk is aan m, en dat

$$l(X) = \prod_{i=1}^{m} (X - \alpha_i)$$

de ontbinding van $l(X)$ voorstelt in eerstegraadsfactoren; de α_i zijn allemaal elementen van L. Er geldt dat

$$A_p(l(X)) = \prod_{i=1}^{m} A_p(X - \alpha_i) = \prod_{i=1}^{m} (X - \alpha_i^p) \quad .$$

Omdat de rij $\alpha_1^p, \ldots, \alpha_m^p$ op volgorde na dezelfde rij is als $\alpha_1, \ldots, \alpha_m$, geldt

$$A_p(l(X)) = l(X) \quad ,$$

met andere woorden, de coëfficiënten van $l(X)$ zijn onveranderlijk onder de werking van A_p, dus $l(X) \in \mathbf{F}_p[X]$. □

6.10.3 Toepassing. Voor elke n die een macht van 3 is, geldt

$$X^{2n} + X^n + 1$$

is irreducibel over $\mathbf{F}_2$.

Bewijs. In het lichaam $GF(2^{2n})$ is er een element α van orde $3n$, omdat

$$3n \mid 4^n - 1 \text{ en } 9n \nmid 4^n - 1$$

voor elke n van de vorm 3^t. Immers, die deelbaarheidseigenschap geldt voor $t = 0$, en uit

$$4^{3n} - 1 = (4^n - 1)^3 + 3 \cdot 4^n \cdot (4^n - 1)$$

volgt dat voor elke oneven n, $4^{3n} - 1$ precies één factor 3 meer heeft dan $4^n - 1$.
Bekijk het polynoom

$$k(X) := (X - \alpha)(X - \alpha^2)(X - \alpha^4) \cdots (X - \alpha^{2^{2n-1}}) \quad .$$

Dit polynoom is van de graad $2n$. Bovendien is met elke nulpunt α^{2^k} ook het kwadraat $\alpha^{2^{k+1}}$ ervan nulpunt van $k(X)$. Immers,

$$\alpha^{2^{2n}-1} = 1 \quad ,$$

dus

$$\alpha^{2^{2n}} = \alpha \quad ,$$

waaruit volgt dat de zojuist gedane uitspraak waar is voor $k = 2n - 1$. Het is niet moeilijk om in te zien dat al deze nulpunten multipliciteit 1 hebben, omdat $2^k - 1$ pas bij $k = 2n$ een veelvoud is van de orde van α.
Het spreekt vanzelf dat $k(X)$ een factor is van elk polynoom over $\mathbf{F}_2$ dat α als nulpunt heeft. Daaruit volgt zowel dat $k(X)$ irreducibel is, als dat $k(X)$ een factor is van

$$X^{3n} + 1 = (X^n + 1)(X^{2n} + X^n + 1) \quad .$$

Dus $k(X)$ is een factor van $X^{2n} + X^n + 1$, waaruit volgt dat $k(X)$ is $X^{2n} + X^n + 1$. □

6.11 De logaritmentafel van een eindig lichaam

We beschouwen de constructie van $GF(2^4)$ met behulp van het primitieve polynoom $x^4 + x + 1$. Het lichaam bestaat uit de 16 polynomen $a_0 + a_1x + a_2x^2 + a_3x^3$ met $a_i = 0$ of $a_i = 1$ $(0 \leq i \leq 3)$. De optelstructuur is die van de vectorruimte $(\mathbf{F}_2)^4$ met elementen (a_0, a_1, a_2, a_3). In dit lichaam is het element x een van de primitieve elementen. We maken nu een lijst van de machten van x door voor iedere i het element x^i te schrijven in de vorm $a_0 + a_1x + a_2x^2 + a_3x^3$. Zie Figuur 1.
Het rekenen in GF (16) gaat met deze tabel heel eenvoudig. Optelling is gewoon vectoroptelling in $(\mathbf{F}_2)^4$. Om het *produkt* van $1 + x^2 + x^3$ en $1 + x + x^2$ uit te rekenen, merken we op dat deze polynomen respectievelijk x^{13} en x^{10} voorstellen. Het produkt is dus $x^{23} = x^8 = 1 + x^2$.

Voorbeeld. Zie de tabel van Figuur 1. We zoeken een polynoom $f(X) \in \mathbf{F}_2[X]$ waarvan het lichaamselement x^3 een nulpunt is. Uit 6.10.1 weten we dat dan ook x^6, x^{12} en $x^{24} = x^9$ nulpunten van $f(z)$ zijn. Volgens Stelling 6.10.2 is echter

	1	x	x^2	x^3
$x^0 = 1 =$	1	0	0	0
$x^1 = x =$	0	1	0	0
$x^2 = x^2 =$	0	0	1	0
$x^3 = x^3 =$	0	0	0	1
$x^4 = 1+x =$	1	1	0	0
$x^5 = x+x^2 =$	0	1	1	0
$x^6 = +x^2+x^3 =$	0	0	1	1
$x^7 = 1+x +x^3 =$	1	1	0	1
$x^8 = 1 +x^2 =$	1	0	1	0
$x^9 = x +x^3 =$	0	1	0	1
$x^{10} = 1+x+x^2 =$	1	1	1	0
$x^{11} = x+x^2+x^3 =$	0	1	1	1
$x^{12} = 1+x+x^2+x^3 =$	1	1	1	1
$x^{13} = 1 +x^2+x^3 =$	1	0	1	1
$x^{14} = 1 +x^3 =$	1	0	0	1

Figuur 1

$$(X - x^3)(X - x^6)(X - x^9)(X - x^{12}) \in \mathbf{F}_2[X] \quad ,$$

en dus hebben we het gewenste polynoom gevonden. Door met de tabel te rekenen vinden we dat dit polynoom gelijk is aan $X^4 + X^3 + X^2 + X + 1$.
Dit kan ook vlugger: immers x^3, x^6, x^9 en x^{12} zijn nulpunten van de vergelijking $X^5 = 1$; alleen het nulpunt 1 ontbreekt. Dus er geldt

$$(X - x^3)(X - x^6)(X - x^9)(X - x^{12}) = \frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1 \quad .$$

6.12 Kwadraatresten

In Hoofdstuk 5 hebben we bestudeerd welke elementen van $\mathbf{F}_p$ kwadraten zijn, en welke niet. Met behulp van de rekenregels voor het Legendresymbool kunnen we meestal snel bepalen of een concreet gegeven element van $\mathbf{F}_p$ een kwadraat is of niet. In het bijzonder geldt dat -1 een kwadraat is als $p \equiv 1 \pmod 4$, en ook voor $p = 2$, maar dat in de andere gevallen -1 geen kwadraat is.
In alle gevallen kunnen we zeggen dat alle elementen ongelijk 0 machten zijn van een primitief element, en dus dat de kwadraten juist de even machten zijn van een primitief element.
Hoe staat het met meer gecompliceerde eindige lichamen? Ook in dit geval geldt dat de kwadraten juist de even machten zijn van een primitief element.
Bekijk eerst $q = p^r$, met oneven priemgetal p. Als α een primitief element is, dan zijn blijkbaar de elementen α^{2i} $(0 \leq i < \frac{1}{2}(q-1))$ de kwadraten ongelijk 0 van $GF(q)$ en de andere elementen ongelijk 0 zijn de niet-kwadraten. De multiplicatieve groep van het lichaam heeft even orde, namelijk $q - 1$. Als $q - 1$ een viervoud is, dan is er een element van orde 4 in die groep, en het kwadraat daarvan is -1. Is daarentegen $q - 1$ geen viervoud, dan is -1 ook geen kwadraat. Bijvoorbeeld, in GF (125) en GF (49) is -1 een kwadraat, maar in GF (27) is -1 geen kwadraat.
Anders gaat het voor $p = 2$. Dan is $q - 1$ oneven en bijgevolg is ieder element van $GF(q)$ in dat geval een kwadraat.

Het verschil tussen $p = 2$ en oneven p kunnen we ook begrijpen door op te merken dat voor oneven p geldt

$$(-x)^2 = x^2 \quad ,$$

dat wil zeggen behalve 0 zijn er niet meer dan $\frac{1}{2}(q-1)$ kwadraten. Daar echter ook $x^2 = y^2$ impliceert $y = x$ of $y = -x$, zijn er ook precies $\frac{1}{2}(q-1)$ kwadraten. Als $p = 2$ dan zijn x en $-x$ echter gelijk.

6.13 Toepassingen op primaliteitstesten†

6.13.1 Inleiding

We zijn al een manier tegengekomen om te bewijzen dat een getal n geen priemgetal is. Natuurlijk is de meest voor de hand liggende manier een deler $d > 1$ van n te zoeken. In interessante gevallen is dat veel werk, zelfs als je weet dat je niet verder hoeft te zoeken dan $\sqrt{n}$. Algemener, we kunnen een a zoeken met

$$GGD(n,a) \neq 1 \quad , \quad 0 < a < n \tag{1}$$

Een verfijndere methode is om voor een a die niet aan (1) voldoet, na te gaan of geldt

$$a^{n-1} \not\equiv 1 \pmod{n} \tag{2}$$

Is dit het geval, dan is wegens de stelling van Fermat n zeker niet priem. Als $a^{n-1} \equiv 1 \pmod{n}$ geldt voor een niet-priemgetal n, dan noemen we n een pseudopriemgetal op basis a; deze test heet ook wel de pseudopriemtest.
In 5.8.2 hebben we deze test nog iets verfijnd. Als namelijk voor zekere k en priemgetal n geldt

$$a^{2k} \equiv 1 \pmod{n}$$

dan zal ook gelden

$$a^k \equiv \pm 1 \pmod{n} \quad .$$

Als $k = (n-1)/2$ dan is het rechterlid gelijk aan het Legendresymbool (a/n).
We kunnen hiervan gebruik maken, door voor een gegeven getal n te schrijven $n - 1 = b\,2^c$ met oneven b; voor priemgetallen n moet dan in de rij

$$a^b, a^{2b}, a^{4b}, \ldots, a^{n-1}$$

ten minste één 1 (modulo n) voorkomen, en als die niet vooraan staat, moet er een -1 aan voorafgaan. De test die dit nagaat wordt de sterke pseudopriemtest genoemd. Deze sterke pseudopriemtest vangt bijna alle niet-priemgetallen. Proefondervindelijk is gevonden dat er onder de 25 miljard maar circa 5000 niet-priemen zijn die deze test op basis 2 overleven. Dat is erg weinig, vergeleken met het circa miljard priemgetallen in datzelfde interval.
Helaas, als een niet-priemgetal één of meerdere sterke pseudopriemtests overleeft, dan neemt zijn kans om de volgende te overleven sterk toe. In 5.8.2 is overigens bewezen, dat die kans niet boven de 50% komt.
We gaan nu een derde primaliteitstest bespreken, de zogeheten Lucastest. We kunnen deze Lucastest gemakkelijk uitleggen met de lichaamstheorie die we tot nu toe hebben ontwikkeld.
De Lucastest is ongeveer even sterk als de pseudopriemtest, maar lijkt daarvan onafhankelijk. Tot op heden (1987) is er geen niet-priemgetal gevonden dat zowel de sterke pseudopriemtest

† De inhoud van paragraaf 6.13 wordt verder niet toegepast, en er zijn geen vraagstukken over.

op basis 2, als een bepaalde versie van de Lucastest overleeft.
De Lucastest heet naar Edouard Lucas, die hem gebruikte voor het testen van Mersennegetallen. In het geval van Mersennegetallen werkt de test ook andersom: een Mersennegetal dat de test passeert is ook zeker priem.

6.13.2 Gegeneraliseerde Fibonacci- en Lucasgetallen

Laat A en B gehele getallen zijn, met $A^2 + 4B \neq 0$ en laat $(u_n)_{n\in\mathbf{N}}$ de oplossing voorstellen van

$$u_{n+2} = Au_{n+1} + Bu_n \quad (n \geq 0)$$
$$u_0 = 0 \ , \ u_1 = 1 \quad .$$

Laat bovendien $(v_n)_{n\in\mathbf{N}}$ de oplossing voorstellen van

$$v_{n+2} = Av_{n+1} + Bv_n \quad (n \geq 0)$$
$$v_0 = 2 \ , \ v_1 = A \quad .$$

Dan geldt voor alle $n \in \mathbf{N}$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

en

$$v_n = \alpha^n + \beta^n \quad ,$$

waar α en β de oplossingen zijn van de vergelijking

$$t^2 = At + B \quad ,$$

zoals we in hoofdstuk 3 al besproken hebben.
Als $A = B = 1$, dan zijn de u_n juist de Fibonaccigetallen, en de getallen v_n vormen dan de rij van Lucas. Laten we afspreken dat we de u_n en de v_n *gegeneraliseerde* Fibonacci- respectievelijk Lucasgetallen noemen.
We geven een paar feiten over deze gegeneraliseerde Fibonacci- en Lucasgetallen. We noteren

$$Q := \begin{bmatrix} A & B \\ 1 & 0 \end{bmatrix} \quad ..EQ.IP\ 1) Voor\ \text{alle}$$
$$Q^n = \begin{bmatrix} u_{n+1} & Bu_n \\ u_n & Bu_{n-1} \end{bmatrix} \quad .$$

De eenvoudigste manier om dit te bewijzen is volledige inductie naar n.
2) Hieruit volgt, door uitschrijven van de identiteit $Q^n Q^n = Q^{2n}$:

$$u_{2n+1} = u_{n+1}^2 + Bu_n^2 = (-B)^n + Au_n u_{n+1} + 2Bu_n^2$$

en

$$u_{2n} = 2u_{n+1}u_n - Au_n^2 \quad .$$

(Merk op dat $\det Q^n = (-B)^n = Bu_n^2 + Bu_{n+1}u_{n-1} = Bu_n^2 + u_{n+1}(u_{n+1} - Au_n)$.)
Deze formules kunnen gebruikt worden om voor grote waarden van n toch snel u_n te berekenen. Door de formules voor u_n en v_n te gebruiken vinden we:

$$u_{2n} = u_n v_n$$

$$v_n = 2u_{n+1} - Au_n$$
$$v_{2n} = v_n^2 - 2(-B)^n \quad .$$

3) Stel dat $GGD(A,B) = 1$. Dan hebben opeenvolgende getallen u_n geen priemfactoren gemeenschappelijk, met andere woorden voor elke n geldt $GGD(u_n,u_{n+1}) = 1$. Voor elke n hebben dan u_n en v_n geen oneven priemfactoren gemeenschappelijk.
De eerste van deze twee beweringen is eenvoudig in te zien met inductie naar n. De tweede van deze beweringen volgt meteen uit de formule voor v_n hierboven.
4) Voor alle natuurlijke n en k volgt door uitschrijven van $Q^{nk}Q^n = Q^{n(k+1)}$

$$u_{n(k+1)} = u_{nk}u_{n+1} + Bu_{nk-1}u_n \quad ,$$

waaruit volgt $u_n \mid u_{kn}$ voor alle n en k.

6.13.3 Rekenen met Fibonaccigetallen in GF(p)

Vanaf deze paragraaf is p een oneven priemgetal. Veronderstel dat $A^2 + 4B$ een kwadraat is modulo p, maar niet nul modulo p, zeg $A^2 + 4B = C^2 \pmod p$. We mogen als we modulo p rekenen de getallen α en β wel opvatten als elementen van GF(p), namelijk

$$\alpha = \frac{A + C}{2} \quad , \quad \beta = \frac{A - C}{2}$$

en omdat $\alpha - \beta = C \neq 0$ geldt dan

$$u_n \equiv 0 \pmod p$$

als en alleen als

$$\alpha^n \equiv \beta^n \pmod p \quad . \tag{3}$$

Als bovendien $B \not\equiv 0 \pmod p$, dan zijn α en β niet nul modulo p en dan is (3) equivalent met

$$(\alpha\beta^{-1})^n \equiv 1 \pmod p \quad ,$$

oftewel

$$(\alpha^2 \cdot (-B^{-1}))^n \not\equiv 1 \pmod p \quad ,$$

omdat $\alpha\beta = -B$.
Evenzo is

$$v_n \equiv 0 \pmod p$$

onder dezelfde voorwaarden equivalent met

$$(\alpha^2 \cdot (-B^{-1}))^n \equiv -1 \pmod p \quad .$$

Als $-B$ geen kwadraat is modulo n, dan mogen we concluderen dat $u_n \equiv 0 \pmod p$ als $(p-1) \mid n$. Als $-B$ wel een kwadraat is modulo p dan volgt zelfs dat $u_n \equiv 0$ als $(p-1)/2 \mid n$. In elk geval, als $u_n \equiv 0$, en n is het kleinste positieve getal met die eigenschap, dan is n een deler van $p - 1$.
Voor priemgetallen p kunnen we over de v_n ook iets zeggen. Als de kleinste positieve n met $u_n \equiv 0 \pmod p$ even is, dan geldt eveneens $v_{n/2} \equiv 0 \pmod p$.

Voorbeeld. We beschouwen de echte Fibonaccigetallen, namelijk het geval $A = B = 1$. Laten we voor p het getal 11 nemen. In ons geval geldt $A^2 + 4B = 5$, en dat is een kwadraat modulo 11, namelijk $4^2 \equiv 5 \pmod{11}$. Modulo 11 zijn de oplossingen van $t^2 = t + 1$ gelijk aan

$$\frac{1+4}{2} = 8 \quad \text{en} \quad \frac{1-4}{2} = 4$$

er geldt dus

$$u_n \equiv 3(8^n - 4^n) \pmod{11} \quad ,$$

dus $u_n \equiv 0 \pmod{11}$ als n een veelvoud is van 10; merk op dat -1 geen kwadraat is modulo 11. Inderdaad, $u_{10} = 55$ hetgeen deelbaar is door 11. Bovendien geldt zelfs v_5 is een elfvoud (toevallig $v_5 = 11$).
Evenzo, als we modulo 61 rekenen vinden we zonder u_{30} uit te rekenen al dat dit een 61-voud is (-1 is een kwadraat modulo 61). In feite geldt

$$u_n \equiv -7\cdot(44^n - 18^n) = -7\cdot 18^n((-44^2)^n - 1) \quad .$$

Modulo 61 geldt $44^2 \equiv 44 + 1$, dus $-44^2 \equiv -45 \equiv 16$ en dus $u_n \equiv -7\cdot 18^n(2^{4n} - 1)$, waaraan we kunnen zien dat u_{15} ook al een 61-voud is, en inderdaad, $u_{15} = 610$.

6.13.4 Rekenen met Fibonaccigetallen in $GF(p^2)$

De toepassing van hoofdstuk 6 begint eigenlijk met de veronderstelling dat $A^2 + 4B$ géén kwadraat is modulo p, met andere woorden, we kunnen α en β opvatten als elementen van een lichaam $GF(p^2)$, preciezer, van

$$GF(p)[t]/(t^2 - At - B) \quad ,$$

immers, het polynoom $t^2 - At - B$ is wegens onze veronderstelling irreducibel over $GF(p)$. De formules

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad , \quad v_n = \alpha^n + \beta^n$$

zijn in dit lichaam evenzeer geldig. De u_n en v_n zijn invariant onder het Frobeniusautomorfisme van $GF(p^2)$, namelijk de afbeelding

$$\xi \longmapsto \xi^p \quad .$$

Dit automorfisme verwisselt α en β, dus u_n en v_n zitten in feite in het priemlichaam $GF(p)$. Dit wisten we al, omdat ze klassen modulo p van gehele getallen zijn.
Als tevoren vinden we dat voor alle natuurlijke getallen n

$$u_n \equiv 0 \pmod{p} \Leftrightarrow (\alpha\beta^{-1})^n = 1 \tag{4}$$

en

$$v_n \equiv 0 \pmod{p} \Leftrightarrow (\alpha\beta^{-1})^n = -1 \quad . \tag{5}$$

Omdat $\alpha = \beta^p$, kunnen we (4) en (5) ook schrijven als

$$u_n \equiv 0 \pmod{p} \Leftrightarrow (\beta^{p-1})^n = 1 \tag{4'}$$

en

$$v_n \equiv 0 \pmod{p} \Leftrightarrow (\beta^{p-1})^n = -1 \quad . \tag{5'}$$

We kunnen in dit geval concluderen dat $u_n \equiv 0$ als $(p-1)n$ een veelvoud is van $(p^2 - 1)$, dat wil zeggen, als n een veelvoud is van $p + 1$.
Ook nu kunnen we nog de gevallen onderscheiden dat $-B$ wel of geen kwadraat is modulo p. Stel eerst dat $-B \equiv C^2$ modulo p. We kunnen dan schrijven

$$A^2 + 4B \equiv (A + 2C)(A - 2C) \pmod{p} \quad ,$$

en omdat het linkerlid geen kwadraat is, zal precies één van beide factoren van het rechterlid wel een kwadraat zijn, zeg

$$A + 2C \equiv T^2 \pmod{p} \quad ,$$

en dan geldt

$$\left[\frac{\beta + C}{T}\right]^2 = \frac{\beta^2 + 2\beta C + C^2}{T^2} = \frac{A\beta + B + 2\beta C - B}{A + 2C} = \beta \quad ,$$

zoals men eenvoudig narekent (denk eraan dat $\beta^2 = A\beta + B$). Dus in dit geval is β een kwadraat.
Stel vervolgens dat β een kwadraat is, zeg

$$\beta = (a\beta + b)^2$$

voor zekere a en b uit het priemlichaam GF(p). Uitwerken geeft dan

$$a^2B + c^2 = 0 \quad ,$$

waaruit volgt dat $-B$ een kwadraat is, namelijk van ca^{-1}. Dus resumerend, β is een kwadraat in GF(p^2) als en alleen als $-B$ het is in GF(p).
Als $-B$ een kwadraat is modulo p, dan geldt zelfs dat $u_n \equiv 0 \pmod{p}$ als $p + 1$ een deler is van $2n$.

Voorbeeld. We nemen weer $A = B = 1$, maar nu laten we p gelijk aan 7 zijn. In dit geval is 5 geen kwadraat modulo 7, en inderdaad geldt

$$7 \mid u_{7+1} \quad ,$$

want $u_8 = 21$.
Nemen we $p = 13$, dan is 5 evenmin een kwadraat modulo p, maar $-B$ wel, dus er geldt zelfs

$$u_7 \equiv 0 \pmod{13} \quad ,$$

in feite geldt zelfs $u_7 = 13$.
Als we u_{14} bezien, dan geldt natuurlijk evenzeer dat 13 een deler is van u_{14}. Rekenen we modulo 29, dan is 5 weer wel een kwadraat, en -1 ook, dus zal u_{14} ook een 29-voud zijn. Men rekent gemakkelijk na dat $u_{14} = 377 = 13 \cdot 29$.

6.13.5 De Lucastest

Uit het voorgaande volgt een algemene primaliteitstest, die als volgt verloopt.
Laat N een oneven getal zijn groter dan 1, N geen kwadraat.
Stap 1. Kies gehele A en B zodanig dat $GGD(B, N) = 1$ en $GGD(A^2 + 4B, N) = 1$ en

$$\left[\frac{A^2 + 4B}{N}\right]_J = -1 \quad .$$

Dan is $A^2 + 4B$ in elk geval geen kwadraat modulo N.
In de praktijk kan dit bijvoorbeeld als volgt gebeuren: kies eerst de waarde van $A^2 + 4B$ uit de rij $-3, 5, -7, 9, -11, \ldots$ (allemaal congruent 1 modulo 4); daarna een oneven A, en dan ligt de waarde van B vast.
Stap 2. Schrijf $N + 1 = b\,2^c$ met oneven b, en bereken achtereenvolgens

$$u_b,\ u_{2b}\ (=u_b v_b),\ u_{4b}\ (=u_b v_b v_{2b}),\ \ldots,\ u_{N+1}\ (=u_b v_b \cdots v_{2^{c-1}b}) \quad ,$$

alles modulo N.

Stap 3. Als N een priemgetal is dan geldt ofwel

$$u_b \equiv 0 \pmod{N}$$

ofwel een der getallen

$$v_b,\ v_{2b},\ \ldots,\ v_{2^{c-1}b}$$

is congruent nul modulo N; als bovendien

$$\left[\frac{-B}{N}\right]_J = 1 \quad ,$$

dan is dit niet het laatste getal in die rij.

Voorbeeld. We passen deze test toe op een Mersennegetal $M_p = 2^p - 1$, met p een oneven priemgetal. We kiezen $A = 4$ en $B = -1$, dan geldt $A^2 + 4B = 12$ en

$$\left[\frac{12}{M_p}\right]_J = \left[\frac{3}{M_p}\right]_J = -\left[\frac{M_p}{3}\right]_J = -\left[\frac{(-1)^p - 1}{3}\right] = -1 \quad .$$

We gebruiken dus hier niet ons "recept" om A en B te zoeken. Merk op dat $-B$ een kwadraat is, dus ook een kwadraat modulo M_p, en dat $M_p + 1 = 2^p$. Ons criterium zegt dat in de rij

$$v_1,\ v_2,\ v_4,\ \ldots,\ v_{2^{p-2}}$$

een getal moet voorkomen dat congruent nul is modulo M_p. We hebben boven al gezien dat deze rij eenvoudig te berekenen is, omdat

$$v_{2n} = v_n^2 - 2$$

voor alle n, en dus kunnen we de getallen waar het om gaat gemakkelijk berekenen. Hier is het begin van de rij:

$$4,\ 14,\ 194,\ 37634,\ 1416317954,\ 2005956546822746114,\ \cdots \quad .$$

Modulo een gegeven M_p is de berekening heel eenvoudig. Bijvoorbeeld voor $p = 5$ komt er (alles modulo 31):

$$4,\ 14,\ 8,\ 0 \quad .$$

In feite is M_p een priemgetal als en alleen als

$$v_{2^{p-2}} \equiv 0 \pmod{M_p} \quad . \tag{6}$$

Een dergelijke test werd gebruikt door Lucas om aan te tonen dat M_{127} priem is; dat is tevens het grootste priemgetal dat gevonden is voor de komst van de computer. Nog steeds worden hele grote priemgetallen gevonden met deze Lucastest. Elke verbetering in computertechniek voegt weer een paar getallen toe aan de lijst van Mersennepriemgetallen. In de volgende paragraaf bewijzen we (6).

6.13.6 Primaliteit van Mersennegetallen

In deze paragraaf bewijzen we twee zaken. Ten eerste, als een Mersennegetal M_p priem is, dan geldt ook $v_{2^{p-2}} \equiv 0 \pmod{M_p}$. Vervolgens zullen we bewijzen dat deze voorwaarde ook voldoende is voor primaliteit van M_p.

We gaan eerst uit van de veronderstelling dat M_p priem is. De multiplicatieve groep van het lichaam $GF(M_p^2)$ is dan een cyclische groep met $(2^p - 1)^2 - 1 = 2^{2p} - 2^{p+1}$ elementen. De orde van een element bevat precies s factoren 2 als en alleen als dat element een 2^{p+1-s}-de macht is en geen 2^{p+2-s}-de macht. Dus $v_{2^{p-2}} \equiv 0 \pmod{M_p}$ als en alleen als $\alpha\beta^{-1}$ een vierde macht is en geen achtste macht.

We weten al dat

$$\alpha\beta^{-1} = \alpha^2 = (\sqrt{1/2}(\alpha - 1))^4 \quad ,$$

waar we gemakshalve $\sqrt{1/2}$ schrijven voor $2^{\frac{p-1}{2}}$, immers $(2^{\frac{p-1}{2}})^2 \cdot 2 \equiv 1 \pmod{M_p}$. Merk op dat de vergelijking $z^8 = 1$ in ons lichaam $GF(M_p^2)$ een oplossing heeft. Ons probleem is dus nu nog aan te tonen dat de vergelijking

$$y^2 = \sqrt{1/2}(\alpha - 1)$$

geen oplossing heeft in $GF(M_p^2)$. We moeten nu aantonen dat de vergelijking

$$(a\,\alpha + b)^2 = \sqrt{1/2}(\alpha - 1)$$

geen oplossingen heeft met a en b in $GF(M_p)$.

Uitwerking hiervan geeft twee vergelijkingen:

$$a^2\alpha^2 + 2\alpha ab + b^2 = \sqrt{1/2}\alpha - \sqrt{1/2}$$
$$a^2(4\alpha - 1) + 2\alpha ab + b^2 = \sqrt{1/2}\alpha - \sqrt{1/2}$$

dus

$$4a^2 + 2ab = \sqrt{1/2}$$
$$-a^2 + b^2 = -\sqrt{1/2}$$

Optellen van deze laatste twee vergelijkingen levert

$$(a + b)^2 + 2a^2 = 0 \quad .$$

Maar -1 is geen kwadraat in $GF(M_p)$, en 2 wel, daarom heeft

$$(a + b)^2 = -2a^2$$

geen oplossing met $(a, b) \neq (0, 0)$. Daarmee zijn we klaar met de eerste helft van deze paragraaf.

We gaan voor de tweede helft van deze paragraaf aannemen dat

$$v_{2^{p-2}} \equiv 0 \pmod{M_p} \quad .$$

Dan volgt in elk geval

$$u_{2^{p-1}} \equiv 0 \pmod{M_p} \quad .$$

Uit de deelbaarheidseigenschappen van de u_n en de v_n volgt dan meteen

$$GGD(u_{2^{p-2}}, M_p) = 1 \quad .$$

We weten ook dat

$$\left[\frac{3}{M_p}\right] = -1 \quad .$$

Dus onder de priemfactoren van M_p is er een q met

$$\left[\frac{3}{q}\right] = -1 \quad .$$

We willen bewijzen dat $q = M_p$, dus M_p is priem.
In elk geval geldt voor zekere deler S van $q + 1$:

$$\forall_{s \in \mathbf{N}} (u_s \equiv 0 \pmod q \Leftrightarrow S \mid s) \quad ,$$

waar S de orde is van $\alpha\beta^{-1}$, maar nu in GF(q^2).
Omdat

$$u_{2^{p-1}} \equiv 0 \pmod q \quad ,$$

volgt dat S zelf een macht van 2 is, $S \leq 2^{p-1}$.
Uit

$$GGD(u_{2^{p-2}}, M_p) = 1$$

volgt dat

$$u_{2^{p-2}} \not\equiv 0 \pmod q \quad ,$$

$$S \nmid 2^{p-2} \quad ,$$

met andere woorden

$$S = 2^{p-1} \quad .$$

Dus $q + 1$ is een veelvoud van 2^{p-1}, zeg $q + 1 = a\,2^{p-1}$, voor zekere positieve gehele a. Als $a = 1$, dan zou q een drievoud zijn. Omdat $q \leq M_p$, volgt $a = 2$, dus $q = M_p$, waarmee we het tweede deel van deze paragraaf besloten hebben.

Opgaven

1. Waarom zijn $\mathbf{Z}_{27}$ en $\mathbf{F}_{27}$ niet isomorf?

2. Wat is de multipliciteit van het nulpunt 1 van

$$x^8 + x^7 + x^6 + x^3 + x^2 + 1 \in \mathbf{F}_2[x] \quad ?$$

3. Hoeveel primitieve elementen heeft GF (25); hoeveel heeft GF (7^3) er?

4. a) Waarom is $x^2 + 3$ irreducibel over $\mathbf{F}_5$?
b) Van welke elementen in $\mathbf{F}_5[x]/(x^2 + 3)$ is het kwadraat gelijk aan -1?
c) Geef de inverse van $x + 1$ in $\mathbf{F}_5[x]/(x^2 + 3)$.

5. Geef de primitieve elementen van $\mathbf{F}_5[x]/(x^2 + 3)$.

6. (Zie Voorbeeld 6.7.6.) Geef de elementen van GF (8) in $\mathbf{F}_2[x]/(x^6 + x + 1)$. Geef ook hun standaardvoorstelling.

7. Ontbind $x^8 - 1$ in $\mathbf{F}_3[x]$ in irreducibele factoren. Welke factor van graad 2 is niet primitief?

8. Hoeveel irreducibele polynomen van de graad 5 zijn er in $\mathbf{F}_2[x]$? Welke zijn primitief?

9. (Zie 6.8.2.) Laat L een eindig lichaam zijn met karakteristiek p en p^r elementen. Laat α een willekeurig element zijn van L.
Waarom komt er in de rij

$$1, \alpha, \alpha^2, \ldots, \alpha^r$$

een element voor dat een lineaire combinatie is van zijn voorgangers, met coëfficiënten in $\mathbf{F}_p$?

10. Zie Voorbeeld 6.8.9. Stel $\mathbf{F}_9$ voor als $\mathbf{F}_3[x]/(x^2+1)$ en ook als $\mathbf{F}_3[y]/(y^2-y-1)$.
a) Laat zien dat er een isomorfisme ψ van het ene lichaam op het andere bestaat, waarbij $\psi(x) = y + 1$.
b) Wat is $\psi^{-1}(y)$?

11. We bestuderen GF (16). Met elementen bedoelen we in het volgende telkens elementen van GF (16).
a) Hoeveel primitieve elementen zijn er, en hoeveel van ordes 3 en 5?
b) Welk tweedegraadspolynoom $a(X)$ met coëfficiënten in $\mathbf{F}_2$ heeft precies de elementen van orde 3 als nulpunten?
c) Welk irreducibel polynoom $b(X)$ in $\mathbf{F}_2[X]$ heeft precies de elementen van orde 5 als nulpunten?
d) Laat

$$l(X) = \prod(X - \alpha) \quad ,$$

waar het produkt genomen wordt over alle niet-primitieve elementen van GF (16). Schrijf $l(X)$ als element van $\mathbf{F}_2[X]$.
e) Welk polynoom dat een deler is van $X^{15} - 1$ heeft precies alle primitieve elementen van GF (16) als nulpunten? Geef een eenvoudige formule voor dit polynoom, gebruik daarbij $a(X)$ en $b(X)$.

12. We bestuderen GF (64).
a) Welke deler van het polynoom

$$X^{63} - 1$$

heeft precies de elementen van orde 7 als nulpunt? Waarom is dit een polynoom in $\mathbf{F}_2[X]$?
b) Dezelfde vraag voor ordes 9, 21, 63.

13. Construeer $\mathbf{F}_{16}$ met behulp van $x^4 + x + 1$. Ga na dat de polynomen 0, 1, $x + x^2$ en $1 + x + x^2$ een deellichaam vormen.

14. Beschouw $GF(q)$, met $q = p^r$. Laat n een deler zijn van $p^r - 1$. Definieer $Q^{(n)}(x)$ als het polynoom in $\mathbf{F}_q[x]$ waarvan de nulpunten precies alle elementen van orde n uit $GF(q)$ zijn. Bewijs met de methode van hoofdstuk 4 dat geldt

$$Q^{(n)}(x) = \prod_{d \mid n} (x^{n/d} - 1)^{\mu(d)} \quad ,$$

waar μ de Möbiusfunctie voorstelt. Merk op dat $Q^{(n)}(x) \in \mathbf{F}_p[x]$. We noemen zo'n polynoom ook wel een *cyclotomisch polynoom* of *cirkeldelingspolynoom.*

15. Bepaal voor GF (16) het polynoom $Q^{(15)}(x)$ en ontbind dit polynoom in irreducibele factoren in $\mathbf{F}_2[x]$.

16. Maak een logaritmentafel van $\mathbf{F}_8$.

17. Maak een logaritmentafel van $\mathbf{F}_{27}$.

18. We stellen GF (16) voor als $\mathbf{F}_2[x]/(x^4 + x^3 + 1)$. GF (16) is een vectorruimte over $\mathbf{F}_2$ met als standaardbasis

$$1, x, x^2, x^3 \quad .$$

we definiëren de afbeelding Λ : GF (16) $\rightarrow$ GF (16) door

$$\Lambda(\alpha) := x\alpha \quad \text{voor alle } \alpha \in \text{GF (16)} \quad .$$

a) Bewijs dat Λ een lineaire afbeelding is.
b) Geef de matrix M van Λ ten opzichte van de standaardbasis.
c) Bewijs dat elke macht van Λ een lineaire combinatie is I, Λ, Λ^2, Λ^3, met coëfficiënten in $\mathbf{F}_2$.
d) Laat O de nulmatrix voorstellen en laat

$$L := \{O, I, M, M^2, \ldots, M^{15}\} \quad .$$

Bewijs dat L een lichaam is met de gebruikelijke optellling en vermenigvuldiging (alles modulo 2) van matrices. Geef ook een isomorfisme van L met $\mathbf{F}_2[x]/(x^4 + x^3 + 1)$.

19. Reken modulo 2. Laat

$$M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad .$$

Toon aan dat de nulmatrix O en de matrices M^i $(0 \leq i < 7)$ een lichaam vormen.

20. Bepaal het minimaalpolynoom van x^{14} in $\mathbf{F}_2[x]/(x^4 + x + 1)$.
a) Gebruik de methode van het voorbeeld in 6.11.
b) Gebruik dat $x^{14} = x^{-1}$.

21. Laat $\alpha \in \text{GF}(p^r) \setminus \{0\}$, met p en $r > 0$, en veronderstel dat

$$l_0 + l_1 X + \cdots + l_k X^k \in \mathbf{F}_p[X]$$

het minimaalpolynoom is van α. Wat zijn de coëfficiënten van het minimaalpolynoom van α^{-1}?
Voor een concreet voorbeeld zie het antwoord van het vorige vraagstuk.

22. De graad van het minimaalpolynoom van $\alpha \in \text{GF}(p^r)$ (p priem en $r > 0$) is een deler van r. Waarom?

23. Laat α primitief zijn in $\mathbf{F}_9$. Als $f(x) \in \mathbf{F}_3[x]$ irreducibel is en $f(\alpha^2) = 0$, bepaal dan $f(x)$.

24. In GF(2^6) is α primitief. Bepaal het minimaalpolynoom van α^7, zonder eerst een tabel van GF(2^6) te maken.

25. a) Gebruik de karakterisering van GF (4) $\subset$ GF (64) om aan te tonen dat voor elke $\alpha \in$ GF (64)

$$\alpha^{16} + \alpha^4 + \alpha + 1 \in \text{GF (4)} \quad .$$

b) We noteren de elementen van GF (4) met a_i, $i = 0,1,2,3$. Hoeveel oplossingen heeft elk der vergelijkingen

$$X^{16} + X^4 + X + 1 = a_i$$

ten hoogste?

c) Laat zien dat

$$X^{16} + X^4 + X + 1 = 0$$

precies 16 verschillende oplossingen heeft in GF (64). Waarom volgt hieruit dat $X^{16} + X^4 + X + 1$ alleen irreducibele factoren kan hebben van graad 1, 2, 3 of 6?
d) Laat zien dat voor elke wortel α van $X^{16} + X^4 + X + 1 = 0$ het element $\alpha + a_i$ wortel is van $X^{16} + X^4 + X + 1 = a_i$.
e) Laat zien dat $X^{16} + X^4 + X + 1$ deelbaar is door $X^4 + X^2 + X + 1$, en dat het quotiënt het produkt is van twee irreducibele factoren van graad 6. (Een van de factoren is $X^6 + X + 1$, maar het is de bedoeling dat het bovenstaande beredeneerd wordt zonder de irreducibele polynomen van graad 6 te kennen of te berekenen.)

26. Bewijs dat alle elementen van GF (2^{11}) derdemachten zijn.

27. Hoeveel paren (a, b) met $a \in$ GF (9) en $b \in$ GF (9) zijn er met $a^2 - b^2 = 1$?

28. Hoeveel paren (a, b) met $a \in$ GF (16) en $b \in$ GF (16) zijn er met $a^2 + b^3 = 1$?

29. Op $GF(p^r)$ met oneven p definiëren we een functie χ door $\chi(0) = 0$, $\chi(x) = 1$ als x een kwadraat is ongelijk nul, en $\chi(x) = -1$ als x een niet-kwadraat is. Bewijs dat voor alle x en y geldt $\chi(xy) = \chi(x)\chi(y)$.

Hoofdstuk 7 Latijnse vierkanten

7.1 Inleiding

EEN permutatiematrix van de orde n is een $n \times n$ matrix met elementen 0 en 1, zodanig dat in iedere rij en in iedere kolom precies één 1 voorkomt. Als afbeelding opgevat, doet een permutatiematrix niets anders dan van elke vector de coördinaten permuteren ten opzichte van een standaardbasis. Voorbeeld van een 4×4 permutatiematrix:

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} x_2 \\ x_4 \\ x_1 \\ x_3 \end{bmatrix}.$$

Het driedimensionale analogon is een $n \times n \times n$-kubus, met in iedere eenheidscel een 0 of een 1, zodanig dat in iedere rij eenheidscellen, zowel in x-, y- als in z-richting, precies één 1 voorkomt. Om dit toch tweedimensionaal voor te stellen, projecteren we de kubus op zijn grondvlak en noteren we in elk vakje van het grondvlak de hoogte k van de 1 in de kolom van de kubus erboven. Het resultaat is een $n \times n$ matrix $A = (a_{ij})$ met in iedere rij en in iedere kolom alle getallen 1 tot en met n precies één keer. Zo'n matrix heet een *Latijns vierkant.*
Opmerking. Het essentiële van een Latijns vierkant is dat er n verschillende symbolen zijn.

7.1.1 Voorbeeld. Laat G een groep zijn met n elementen; we noteren de bewerking in G met + (maar we veronderstellen niet dat G commutatief is). Laat zowel $(r_1, \ldots, r_n)$ als $(k_1, \ldots, k_n)$ (niet noodzakelijk verschillende) manieren voorstellen om de elementen van G te nummeren. Definieer $a_{ij} = r_i + k_j$. De matrix $A = (a_{ij})$ is een groepstabel voor G.
N.B. Het is gebruikelijk bij groepstabellen om het neutrale element vooraan te zetten, en verder voor kolommen en rijen dezelfde volgorde aan te houden, maar voor de zojuist gedefinieerde A zullen deze conventies in het algemeen niet gelden.
Het is triviaal dat A een Latijns vierkant is.

7.1.2 Voorbeeld. Het diagram van Figuur 2 ziet er uit als het begin van een Latijns vierkant.

a	b	c	d	e
b	a	e	c	d

Figuur 2

We kunnen dit inderdaad completeren tot een Latijns vierkant. Kunnen we dat zo doen dat we een groepstabel krijgen, zoals in Voorbeeld 7.1.1? Het antwoord luidt: neen.
Bewijs. Veronderstel dat Figuur 2 een gedeelte van een groepstabel voorstelt. Dan geldt met de notaties van Voorbeeld 7.1.1:

$$r_1 + k_1 = r_2 + k_2 \quad (= a) \quad , \tag{1}$$

$$r_1 + k_2 = r_2 + k_1 \quad (= b) \quad . \tag{2}$$

Uit (1) volgt eerst $r_1 = r_2 + k_2 - k_1$ en dan $r_1 + k_2 = r_2 + k_2 - k_1 + k_2$. Passen we vervolgens (2) toe, dan vinden we $r_2 + k_1 = r_2 + k_2 - k_1 + k_2$. Beide leden links met r_2 en rechts

met k_1 verminderen geeft

$$0 = k_2 - k_1 + k_2 - k_1 \quad , \tag{3}$$

dus is $k_2 - k_1$ een element van orde 2 in een groep van orde 5, maar in een groep zijn de ordes der elementen delers van de orde van de groep: tegenspraak. □

7.2 Intermezzo: partiële Latijnse vierkanten

Stel dat we in een $n \times n$-vierkant op sommige plaatsen al een van de symbolen 1 tot en met n hebben geschreven, en wel zo dat er geen twee dezelfde in één rij of kolom staan. Dan noemen we dat een *partieel* Latijns vierkant. Kunnen we een partieel Latijns vierkant completeren tot een Latijns vierkant?

Soms gaat dat wel, bijvoorbeeld als het partieel Latijns vierkant een Latijnse rechthoek is. Dit berust op een stelling die we hier niet zullen bewijzen. In de volgende twee voorbeelden is het eerste partiële Latijnse vierkant gecompleteerd, maar waar in het tweede voorbeeld zou de vierde 1 moeten komen?

1		3	
	4	2	
	3		

→

1	2	3	4
3	4	2	1
4	3	1	2
2	1	4	3

1			
	1		
		1	
			2

→

Het zogeheten *vermoeden van Evans* (1960) luidt als volgt. Indien in een $n \times n$-vierkant al $n-1$ elementen staan, zodanig dat er geen twee dezelfde in één rij of kolom staan, dan is dit een deel van een Latijns vierkant. Dit vermoeden is bewezen door B. Smetianuk (Ars Combinatoria **11** (1981), 155-172). Het bewijs van Smetianuk is, hoewel ingewikkeld, zonder voorkennis te lezen. De belangrijkste stap in het bewijs is een algoritme dat uit een $n \times n$-vierkant een vierkant maakt, met een rij en een kolom meer, dus $(n+1)\times(n+1)$.

1	3	5	4	2
2	1	3	5	4
3	2	4	1	5
4	5	2	3	1
5	4	1	2	3

1	3	5	4	2	6
2	1	3	5	6	
3	2	4	6		
4	5	6			
5	6				
6					

Figuur 3

Dit gaat op de volgende manier. Uit het gegeven $n \times n$-vierkant wordt een driehoek gelicht,

bestaande uit een diagonaal en alle elementen erboven. Aan deze driehoek wordt een diagonaal vastgeplakt, uitsluitend bestaande uit n+1-en. Onder deze nieuwe diagonaal wordt het vierkant weer aangevuld. Figuur 3 illustreert het idee.
Het lastigste deel van het bewijs is het algoritme om het vergrote vierkant aan te vullen. Men moet

1) het algoritme bedenken en
2) bewijzen dat het altijd werkt.

Verder bestaat het bewijs uit volledige inductie, enzovoorts.

7.3 Orthogonal Arrays

Men zou kunnen vragen hoeveel verschillende Latijnse vierkanten van orde n er zijn. Eerst moet men dan afspreken wat onder *verschillend* verstaan moet worden. Als we afspreken dat we de eerste rij en kolom permuteren tot 1, 2, . . . , n, dan wordt het aantal genoteerd met l_n. Voor $n \leq 9$ is l_n bekend. Zie de tabel.

n	l_n
1	1
2	1
3	1
4	4
5	56
6	9408
7	16942080
8	535281401856
9	377597570964258816

Tabel van de aantallen gereduceerde Latijnse vierkanten van ordes 1 tot en met 9.

Dit is niet de goede definitie van wat verschillende Latijnse vierkanten zijn, zoals we al zien uit onze driedimensionale opzet. We hebben alleen rijen en kolommen verwisseld. We zouden ook nog symbolen moeten verwisselen.
Als we denken aan de kubus uit 7.1, dan zien we dat de x, y en z-as ook van rol kunnen wisselen. Dit leidt tot het volgende begrip.

7.3.1 Definitie. Een $OA(n,3)$ (Orthogonal Array of order n and depth 3) is een matrix met 3 rijen en n^2 kolommen met elementen 1 tot en met n zodanig dat voor *ieder paar* rijen geldt: de n^2 verticale paren getallen in deze twee rijen zijn allemaal verschillend. []

1	2	3
3	1	2
2	3	1

1	1	1	2	2	2	3	3	3
1	2	3	1	2	3	1	2	3
1	2	3	3	1	2	2	3	1

Figuur 4

Een dergelijke matrix codeert een Latijns vierkant! De kolommen van het $OA(n,3)$ zijn de plaatsvectoren van de enen in de $n \times n \times n$-kubus, waar we de blokjes van de kubus opvatten

als

genummerd van 1 tot en met n.
Figuur 4 toont een Latijns vierkant van orde 3 en een $OA(3,3)$ die bij dat Latijnse vierkant hoort. In de vierde kolom van die 3×9-matrix lezen we af dat het element op rij nummer 2 en kolom nummer 1 van het Latijnse vierkant 3 is.

7.4 Orthogonale Latijnse vierkanten

7.4.1 Definitie. Twee Latijnse vierkanten A, B heten *orthogonaal* (notatie $A \perp B$) indien de n^2 paren (a_{ij}, b_{ij}) verschillend zijn. Een stelsel $L_1, L_2, \ldots, L_r$ heet een stelsel van r orthogonale Latijnse vierkanten (MOLS: Mutually Orthogonal Latin Squares), als ieder paar L_i, L_j met $i \neq j$ orthogonaal is.
Ook hier is een betere definitie, namelijk weer als Orthogonal Array.

7.4.2 Definitie. Een $OA(n,s)$ is een $s \times n^2$-matrix zodanig dat voor ieder paar rijen alle n^2 verticale paren elementen verschillend zijn. We zien dat we in een $OA(n,s)$ één rij kunnen kiezen als rij van rijnummers en een andere als rij van kolomnummers; elk van de overige rijen geeft dan een Latijns vierkant. Op die manier vinden we $s - 2$ MOLS.

7.4.3 Stelling. Als $L^{(1)}, L^{(2)}, \ldots, L^{(t)}$ een stelsel MOLS van orde n is, dan geldt $t \leq n - 1$.
Bewijs. Als we in een van twee orthogonale Latijnse vierkanten de symbolen permuteren, dan vinden we een nieuw paar orthogonale Latijnse vierkanten. Dat is eenvoudig in te zien. In iedere $L^{(k)}$ permuteren we de symbolen zodanig dat de eerste rij $1, 2, \ldots, n$ is. We hebben dan nog steeds een stelsel van t MOLS van orde n $(n > 1)$, zeg met elementen $l_{ij}^{(k)}$ $(k = 1, 2, \ldots, t)$.
Als we nu naar de elementen $l_{21}^{(k)}$ kijken, dan zien we dat deze voor verschillende k verschillend moeten zijn. Immers voor verschillende k en l komen de paren (1,1), (2,2) tot en met (n,n) al voor onder de n^2 paren $(l_{ij}^{(k)}, l_{ij}^{(l)})$, namelijk bij $i = 1$. Daarom bestaan de paren $(l_{21}^{(k)}, l_{21}^{(l)})$ alle uit verschillende leden. Bovendien geldt voor elke k dat $l_{21}^{(k)} \neq 1$. []

7.4.4 Stelling. Als $n = p^{\alpha}$, met p priem en $\alpha > 0$, dan bestaan er $n - 1$ MOLS van de orde n.
Bewijs. We nummeren de elementen van $GF(n)$ als volgt: $a_0 = 0$, $a_1 = 1$, verder $a_2, \ldots, a_{n-1}$ willekeurig. Definieer $L^{(k)}$ door

$$l_{ij}^{(k)} = a_k \cdot a_i + a_j \quad (0 \leq i, j < n, 0 < k < n) \quad .$$

We bewijzen eerst dat dit Latijnse vierkanten zijn. De i-de rij in $L^{(k)}$ bevat allemaal verschillende elementen, want stel

$$a_k \cdot a_i + a_j = a_k \cdot a_i + a_{j'} \quad ,$$

dan volgt zonder moeite dat $a_j = a_{j'}$, en dus $j = j'$. Evenzo bevat de j-de kolom n verschillende elementen. Daartoe gebruiken we dat $a_k \neq 0$.
Vervolgens tonen we aan dat $L^{(k)}$ en $L^{(l)}$ voor $k \neq l$ orthogonaal zijn. Stel daartoe voor willekeurige i, j, r, s:

$$(l_{ij}^{(k)}, l_{ij}^{(l)}) = (l_{rs}^{(k)}, l_{rs}^{(l)}) \quad ,$$

dan volgt

$$a_k \cdot a_i + a_j = a_k \cdot a_r + a_s$$
$$a_l \cdot a_i + a_j = a_l \cdot a_r + a_s$$

Als we de ene vergelijking van de andere aftrekken en alles naar een kant brengen, vinden we

$(a_k - a_l)\cdot(a_i - a_r) = 0$. Omdat $a_k - a_l \neq 0$, volgt dat $a_i - a_r = 0$ (we rekenen immers in een lichaam), dus $a_i = a_r$. Daaruit volgt dan weer $a_j = a_s$. Bijgevolg geldt $i = r$ en $j = t$. Hiermee is bewezen dat $L^{(k)} \perp L^{(l)}$. □

7.4.5 Stelling. Als er t MOLS van orde n en ook t MOLS van orde m bestaan, dan bestaan er ten minste t MOLS van de orde $n\,m$.

Bewijs. Laten $A^{(l)}$ en $B^{(l)}$ $(1 \leq l \leq t)$ de MOLS van orde n respectievelijk m zijn, met als elementen de getallen 1 tot en met n en 1 tot en met m respectievelijk. Vervang het element $a_{ij}^{(l)}$ in rij i en kolom j van $A^{(l)}$ door een vierkant ter grootte $m \times m$, met daarin de elementen van $B^{(l)}$, elk vermeerderd met $(a_{ij}^{(l)} - 1)m$. Doe dit voor elke $l = 1, \ldots, t$. Noem de nieuwe matrices $C^{(l)}$ $(1 \leq l \leq t)$. Als het paar (x, y) te schrijven is als $(c_{rs}^{(k)}, c_{rs}^{(l)})$, dan geldt

$$\left(\left\lceil \frac{x}{m} \right\rceil , \left\lceil \frac{y}{m} \right\rceil \right) = (a_{ij}^{(k)}, a_{ij}^{(l)})$$

voor precies één paar (i, j). Uit de orthogonaliteit van $B^{(k)}$ en $B^{(l)}$ kunnen we dan vervolgens r en s eenduidig bepalen. Daaruit volgt dat de $C^{(l)}$ orthogonaal zijn. □

Uit Stelling 7.4.4 en Stelling 7.4.5 trekken we de volgende conclusie.

7.4.6 Stelling (MacNeish). Als $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, dan is het aantal MOLS van orde n ten minste gelijk aan

$$\min \{ p_i^{\alpha_i} - 1 \mid 1 \leq i \leq k \} \quad .$$

□

0	6	5	4	7	8	9
9	1	0	6	5	7	8
8	9	2	1	0	6	7
7	8	9	3	2	1	0
1	7	8	9	4	3	2
3	2	7	8	9	5	4
5	4	3	7	8	9	6

Figuur 5
De matrix A

7.4.7 Het vermoeden van Euler. Voor $n \equiv 2 \pmod 4$ zegt Stelling 7.4.6 niets. Het is triviaal dat er maar één Latijns vierkant van orde 2 bestaat. De eerste vraag is of er twee orthogonale Latijnse vierkanten van de orde 6 zijn. Deze vraag werd al in 1782 door Euler gesteld als het (nu beroemde) *probleem van de 36 officieren.* Is het mogelijk om 36 officieren van 6 verschillende rangen en uit 6 verschillende regimenten zodanig in een vierkant op te stellen dat iedere rang en ieder regiment in elke rij en in elke kolom precies één keer voorkomt?
Dit lukte geen der generaals aan het Russische hof, en Euler kwam tot de overtuiging - door tamelijk uitvoerige gevalsonderscheiding - dat het inderdaad onmogelijk was. Hij opperde het vermoeden dat er voor geen enkele n met $n \equiv 2 \pmod 4$ twee orthogonale Latijnse vierkanten van orde n bestaan.
In zijn analyse van het probleem gaf Euler de rang van een officier met een Latijnse letter aan, en diens regiment met een Griekse letter. Sindsdien heten tweetallen MOLS dan ook wel Grieks-Latijnse vierkanten, en de term Latijns vierkant gaat eveneens terug op de terminologie van Euler.

In 1900 is het geval $n = 6$ door Tarry bewezen. Pas in 1957 bewezen Bose, Shrikhande en Parker dat er ten minste twee orthogonale Latijnse vierkanten van de orde n bestaan als n ongelijk is aan 1, 2 of 6. Het voorbeeld met $n = 10$ staat bekend als de *Euler spoiler*.
We geven de constructie van een paar orthogonale Latijnse vierkanten van orde 10. De 7×7 matrix van Figuur 5 noemen we A. Merk op dat de matrix A uit twee delen bestaat, het ene deel met constante diagonalen, en het andere deel met cyclische diagonaal. Men stelle zich A voor, aan alle zijden door kopieën van zichzelf geflankeerd.
Voor de constructie hebben we ook nog de cyclische matrices B, C, D en E nodig, van Figuur 6 en 7.

$$B^T = \begin{array}{|ccccccc|}\hline 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ \hline\end{array} \qquad C = \begin{array}{|ccccccc|}\hline 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline\end{array}$$

Figuur 6

$$D = \begin{array}{|ccc|}\hline 7 & 8 & 9 \\ 9 & 7 & 8 \\ 8 & 9 & 7 \\ \hline\end{array} \qquad E = \begin{array}{|ccc|}\hline 7 & 8 & 9 \\ 8 & 9 & 7 \\ 9 & 7 & 8 \\ \hline\end{array}$$

Figuur 7

Het volgende paar matrices vormt een tweetal MOLS van orde 10. Ga dit zelf na.

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad \text{en} \quad \begin{pmatrix} A^T & C^T \\ B^T & E^T \end{pmatrix} .$$

Het is niet bekend of er drie MOLS van orde 10 zijn. Wel bekend is, dat voor $n \geq 14$ er ten minste drie MOLS van orde n zijn.

7.5 Toepassingen

7.5.1 Proefvelden

Op een vierkant stuk bouwland wil men n soorten graan zaaien en de oogst vergelijken. Hiertoe verdeelt men het stuk land in n^2 vierkanten. We nemen aan dat de grond misschien niet overal even vruchtbaar is, maar dat de afhankelijkheid zodanig is dat de verwachtingswaarde van de oogst per vierkante meter voor de k-de graansoort gezaaid in de i-de rij en de j-de kolom gelijk is aan

$$\rho + \mu_i + \nu_j + \rho_k \quad ,$$

waarbij $\sum\mu_i = \sum\nu_j = \sum\rho_k = 0$. Als de vruchtbaarheid bijvoorbeeld lineair van de plaats afhangt, dan is dit het geval. De grootheid ρ is kennelijk de verwachtingswaarde van de opbrengst per vierkante meter.
Men stelt vragen van het type "zijn de graansoorten verschillend in kwaliteit?", "is er verschil in vruchtbaarheid tussen de rijen of de kolommen onderling?". Als men de k-de graansoort zó zaait dat in iedere rij en in iedere kolom juist één subvierkant met deze soort voorkomt, dan is de verwachtingswaarde van de oogst van de k-de soort over deze proefveldjes $\rho + \rho_k$ omdat $\sum\mu_i = \sum\nu_j = 0$. Dat wil zeggen dat de invloed van de plaats geëlimineerd is. Om alle soorten op zo'n manier te zaaien, moet men van het proefveld een Latijns vierkant maken.
Juist in deze context zijn Latijnse vierkanten voor het eerst, omstreeks 1922, gebruikt voor statistische proefopzetten, en wel door Fisher.

(R.A. Fisher (1890-1962) was een van de grondleggers van de moderne statistiek en de moderne genetica. Hij werkte tussen 1919 en 1933 bij het landbouwkundig proefstation te Rothamsted, en daarna was hij hoogleraar in de genetica in Londen. Hij was de eerste na Euler die de waarde van l_5 (zie 7.3) correct berekende).

7.5.2 Statistische analyse van buizenfabricage

Dit voorbeeld is afkomstig van een plaatselijke fabriek waar radiobuizen werden gemaakt. Er waren vier bewerkingen, te weten (a) maken van wolframdraad, (b) maken van de spiraal, (c) aanbrengen van een laag aluminiumoxide en (d) de buizenmontage.
De produktie vertoonde een veel te grote spreiding in de gloeistroom van de buizen. De vier afdelingen die elk voor een der vier bewerkingen verantwoordelijk waren gaven elkaar de schuld, en door middel van een experiment moest worden uitgemaakt welke van de vier factoren oorzaak van het verschijnsel was.
In verband met de tijd en de kosten wilde men niet te veel buizen testen. Voor dit soort experimenten is een Grieks-Latijns vierkant het hulpmiddel. Men nam een Latijns vierkant van orde 7, met elementen A, B, C, D, E, F en G, en een ander met elementen a, b, c, d, e, f en g, zodanig dat ze een orthogonaal paar vormden.
Op 7 verschillende dagen werd een partij wolframdraad gemaakt, en van elke partij maakte men op 7 verschillende dagen spiralen. Een steekproef van 15 spiralen uit elke partij gaf een groep van 49 keer 15 spiralen. Deze plaatste men op het Grieks-Latijns vierkant, en wel zo dat een draad van de i-de dag in de i-de rij terecht kwam en een spiraal die op de j-de dag geproduceerd was in de j-de kolom. De 7 partijen op een A-plaats werden op één dag van een laag aluminiumoxide voorzien, de 7 partijen op een B-plaats eveneens, enzovoorts. Tot slot werden op 7 verschillende dagen buizen gemonteerd met alle partijen van een a-plaats op één dag, evenzo die van een b-plaats, enzovoorts. Na 28 dagen had men zo 49 maal 15 buizen, en aan elke groep werden gloeistroommetingen gedaan.
Met deze opzet bereikte men dat voor elke fase de produktie van één dag voor iedere andere fase over 7 dagen was verspreid. Het experiment toonde duidelijk aan dat de spreiding (voor verschillende dagen) bij de buizenmontage te groot was.

7.5.3 Effecten van buurexperimenten

Bij een onderzoek gedaan op het Instituut voor Perceptie-Onderzoek (IPO) werd bij proefpersonen nagegaan hoe het oog reageerde als op een TV-scherm vierkantjes van verschillende lichtsterkte naast elkaar lagen en als dan het beeld werd uitgeschakeld. Daarbij bleek de reactie voor "donker onder helder" anders dan voor "donker boven helder". Men wilde dit voor veel verschillende lichtsterkten tegelijk meten. Vertaald in onze terminologie kwam het probleem neer op het volgende.
Bepaal een Latijns vierkant van de orde n zodanig dat de $n(n-1)$ horizontale paren $(a_{ij}, a_{i\,j+1})$ verschillend zijn, en evenzo voor de verticale paren $(a_{ij}, a_{i+1\,j})$. Dit soort Latijnse vierkanten heet row complete column complete. De constructie ervan is nog onderwerp van onderzoek.
We geven een voorbeeld. Stel dat we de elementen van $\mathbf{Z}_n$ zodanig kunnen ordenen als $x_1, x_2, \ldots, x_n$ dat alle verschillen $x_{i+1} - x_i$ verschillend zijn. Neem nu $r_i = k_i = x_i$, $(1 \leq i \leq n)$ en construeer een Latijns vierkant als in Voorbeeld 1 van 7.1. Veronderstel dat

$$(r_i + k_j, r_i + k_{j+1}) = (r_{i'} + k_{j'}, r_{i'} + k_{j'+1}) \quad ,$$

dan geldt $k_{j+1} - k_j = k_{j'+1} - k_{j'}$. Daaruit volgt $j = j'$ en dus ook $i = i'$. Voor de verticale paren gaat men analoog te werk.

Opgaven

30. a) Maak het Latijnse vierkant van Voorbeeld 7.1.2 af.
b) Ga op een verstandige manier na hoeveel antwoorden onderdeel a) heeft.

31. Hoeveel Latijnse vierkanten zijn er van de vorm

1	2	3	4
2			
3			
4			

a) Zijn deze te maken zoals in Voorbeeld 7.1.1, dat wil zeggen met een groep en zo ja, hoe?
b) Hoeveel groepen van orde 4 zijn er?

32. Construeer voor willekeurige $n > 1$ een partieel Latijns vierkant van de orde n, waarin precies n elementen staan die onderling verschillend zijn, en bovendien zodanig dat dit partieel Latijns vierkant niet is af te maken tot een Latijns vierkant.

33. a) Ga na dat het vierkant van Figuur 3 op allerlei manieren is af te maken. Merk op dat het niet zo eenvoudig is een "natuurlijke" wijze van voltooien te vinden.
b) (Zeer lastig; als u een oplossing heeft stelt de auteur het zeer op prijs daar kennis van te mogen nemen.) Bedenk een *algoritme* met bewijs dat het werkt. Dit geeft een idee van de moeilijkheidsgraad van sommige combinatorische problemen.

34. Neem de oplossingen van Opgave 31. Als we daarin symbolen mogen verwisselen en tevens rijen en kolommen permuteren, hoeveel verschillende blijven er dan over?

35. Construeer drie MOLS van de orde 4 die allemaal 1,2,3,4 als eerste rij hebben. Schrijf het antwoord ook als orthogonal array.

36. Construeer twee MOLS van orde 9.
a) Gebruik de methode van Stelling 7.4.4.
b) Gebruik de methode van Stelling 7.4.5.

37. Construeer vier MOLS van de orde 5.

38. Construeer drie MOLS van de orde 4.

39. Construeer drie MOLS van de orde 20.

40. Bewijs dat er geen Latijns vierkant van de orde 4 is dat met

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

een orthogonaal paar vormt.

41. Maak een Latijns vierkant van de orde 4 met de eigenschap dat ieder paar (i, j) met $i \neq j$ eenmaal voorkomt in naast elkaar staande hokjes.

42. Toon aan dat de constructie van 7.5.3 mogelijk is voor even n en *niet* voor oneven n.

43. Twee Latijnse vierkanten heten *isomorf* als er een permutatie van rijen, kolommen, en symbolen bestaat die de ene in de andere overvoert.
a) Bewijs dat als een Latijns vierkant een orthogonale partner heeft, zulks ook geldt voor elk

ermee isomorf Latijns vierkant.
b) Laat zien dat er ten minste twee niet-isomorfe Latijnse vierkanten van de orde 4 zijn.
c) (Moeilijker). Laat zien dat er precies twee niet-isomorfe Latijnse vierkanten zijn.

44. a) Laat zien dat het Latijnse vierkant gevormd door de tabel van de optelgroep $\mathbf{Z}_6$ geen orthogonale partner heeft. Zie ook Opgave 40.
b) Onderdeel a) en opgave 40 zijn een speciaal geval van de stelling dat het Latijns vierkant gevormd door de optelgroep $\mathbf{Z}_{2n}$ geen orthogonale partner heeft. Bewijs deze stelling (lastig).

Hoofdstuk 8 Hadamardmatrices

8.1 Inleiding

EEN *Hadamardmatrix* van de orde n is een $n \times n$ matrix H met coëfficiënten $+1$ en -1, met de eigenschap dat het inwendig produkt van elk tweetal rijen nul is; daaruit volgt dat ook elk tweetal kolommen orthogonaal is (ga dat na!). We kunnen dit ook in formulevorm uitdrukken door te zeggen dat

$$H H^T = nI \quad .$$

Als we de rijen van H permuteren of sommige rijen van H met -1 vermenigvuldigen, dan is het resultaat weer een Hadamardmatrix; evenzo voor de kolommen.
J. Hadamard (1865-1963) was omstreeks de eeuwwisseling een van de belangrijkste wiskundigen. Hij droeg veel bij tot de theorie van de analytische functies, de mathematische fysica en partiële differentiaalvergelijkingen. In 1896 bewees hij de priemgetalstelling, tegelijk met C.J. De La Vallée-Poussin (zie 5.6.2). Ook op het gebied van bijvoorbeeld onderwijs, logica, waarschijnlijkheidstheorie en op vele andere gebieden was zijn invloed groot.
Hadamard bestudeerde dit soort matrices in verband met het volgende probleem. Gevraagd de grootste waarde die $|\det H|$ kan aannemen op de verzameling van alle $n \times n$ matrices H waarvan de coëfficiënten absoluut ten hoogste 1 zijn. Als er een Hadamardmatrix bestaat van orde n, dan geeft die ook de oplossing $n^{n/2}$.
We kunnen een Hadamardmatrix altijd normaliseren, dat wil zeggen door bovengenoemde bewerkingen op rijen en kolommen zorgen dat de eerste rij en de eerste kolom louter uit elementen $+1$ bestaan. Voorbeelden:

$$\begin{bmatrix} 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{en} \quad \begin{bmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & + & + \end{bmatrix}$$

zijn Hadamardmatrices, waarbij we in de laatste alleen het teken + of − hebben geschreven en de 1 hebben weggelaten.

8.1.1 Stelling. Als H een Hadamardmatrix van de orde n is, dan geldt $n = 1$ of $n = 2$ of $n \equiv 0 \pmod 4$.

Bewijs. Laat $n > 2$. Normaliseer H. We kunnen de kolommen van H zodanig permuteren, dat de eerste drie rijen van H er als volgt uitzien.

++ · · · +	++ · · · +	++ · · · +	++ · · · +
++ · · · +	++ · · · +	−− · · · −	−− · · · −
++ · · · +	−− · · · −	++ · · · +	−− · · · −
a kolommen	b kolommen	c kolommen	d kolommen

In deze drie rijen zijn maar vier types kolommen, in aantallen a, b, c en d respectievelijk. Uit het feit dat de drie inwendige produkten tussen deze drie rijen nul zijn, leiden we af

$$\begin{aligned} a + b - c - d &= 0 \\ a - b + c - d &= 0 \\ a - b - c + d &= 0 \quad . \end{aligned}$$

Tevens weten we

$$a + b + c + d = n \quad .$$

Uit deze vier vergelijkingen vinden we $n = 4a$ $(= 4b = 4c = 4d)$. □

8.1.2 Definitie. Een *conferentiematrix* C van de orde n is een matrix met diagonaalelementen 0 en alle andere elementen +1 of −1, zodanig dat

$$C\,C^T = (n-1)I \quad .$$

□

8.1.3 Definitie. Een matrix A noemen we *antisymmetrisch* of ook wel *scheef* als

$$A^T = -A \quad .$$

□

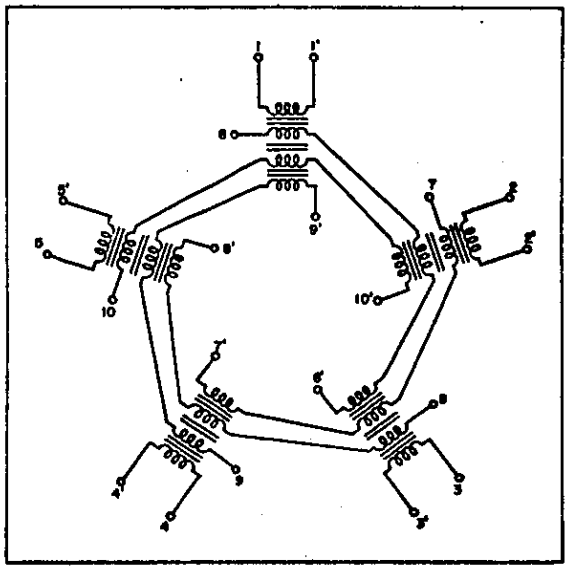
8.1.4 Stelling. Als C een scheve conferentiematrix is, dan is $I + C$ een Hadamardmatrix.
Bewijs. $(I + C)(I + C)^T = I + C + C^T + C\,C^T = I + (n-1)I) = nI$. □

8.1.5 Stelling. Als C een symmetrische conferentiematrix van de orde n is, dan is

$$H = \begin{bmatrix} I+C & -I+C \\ -I+C & -I-C \end{bmatrix}$$

een Hadamardmatrix van de orde $2n$.
Bewijs. Narekenen. □

De naam conferentiematrix is afkomstig van een van de toepassingsgebieden, namelijk de constructie van netwerken voor zogeheten "telephone conferences". In het ideale geval bestaat zo'n netwerk geheel uit ideale transformatoren zoals in Figuur 8 (ontleend aan V. Belevitch, *Theory of 2n-terminal networks with applications to conference telephony*, Electrical Communication, **27** (1950), 231-244).



Figuur 8
Een ideaal conferentienetwerk met 20 poorten.

De theorie berust op de constructie van een symmetrische matrix S waarin de elementen s_{ij} op het teken na de transmissiecoëfficiënten tussen twee poorten van het netwerk voorstellen. De eis dat alle getallen $|s_{ij}|$ hetzelfde zijn, komt er ongeveer op neer dat als één persoon spreekt,

de andere $n-1$ hem of haar allemaal even hard horen. Verder moeten de zogeheten reflectiecoëfficiënten s_{ii} nul zijn. Tenslotte betekent behoud van energie dat $S\,S^T = cI$.

8.2 Een produktconstructie voor Hadamardmatrices

Veel combinatorische constructies bestaan uit het maken van een nieuw groot object uit kleinere. Een voorbeeld van zo'n constructie zagen we al in Stelling 7.4.5. We geven thans weer zo'n stelling.

8.2.1 Definitie. Laat $A = (a_{ij})$ een $n \times n$ matrix zijn en $B = (b_{rs})$ een $m \times m$ matrix. Dan bestaat het *Kroneckerprodukt* $A \otimes B$ uit n^2 blokken van m bij m als volgt

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{pmatrix} .$$

□

Men gaat eenvoudig na dat

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$

en

$$(A \otimes B)^T = A^T \otimes B^T \quad .$$

8.2.2 Stelling. Als H_m en H_n Hadamardmatrices van ordes m en n respectievelijk zijn, dan is $H_m \otimes H_n$ een Hadamardmatrix van de orde mn.

Bewijs.

$$\begin{aligned}(H_m \otimes H_n)(H_m \otimes H_n)^T &= H_m H_m^T \otimes H_n H_n^T \\ &= mI_m \otimes nI_n = mnI_{mn} \quad ,\end{aligned}$$

waar een notatie zoals I_n de $n \times n$ eenheidsmatrix voorstelt. □

8.3 Constructie van een conferentiematrix van de orde $q+1$

Laat q een macht van een oneven priemgetal zijn. Definieer χ op $GF(q)$ net zoals het Legendresymbool in $GF(q)$ als q een oneven priemgetal is, zie ook 5.7.1 tot en met 5.7.4 en 6.12 en Opgave 29. Dat wil zeggen

$$\chi(x) := \begin{cases} 0 & \text{als } x = 0, \\ 1 & \text{als } x \text{ een kwadraat is,} \\ -1 & \text{als } x \text{ geen kwadraat is.} \end{cases}$$

We herhalen nog eens wat we over het Legendresymbool vertelden. De functie χ heeft de eigenschap dat $\chi(x)\chi(y) = \chi(xy)$ voor alle x en y in $GF(q)$. Omdat er evenveel kwadraten als niet-kwadraten zijn in $GF(q) \setminus \{0\}$ geldt

$$\sum_{a \in GF(q)} \chi(a) = 0 \quad .$$

We resumeren de discussie in 5.7.4 door middel van het volgende Lemma.

8.3.1 Lemma. Als $c \in GF(q)$, en $c \neq 0$, dan geldt

$$\sum_{b \in GF(q)} \chi(b)\chi(b+c) = -1 \quad . \qquad (*)$$

Bewijs. De term met $b = 0$ is 0. We geven met $\sum'$ sommatie over de elementen ongelijk nul aan. Het linkerlid van $(*)$ wordt dan

$$\sum_{b \in GF(q)}' \chi(b)\chi(b)\chi(1+cb^{-1}) = \sum_{b \in GF(q)}' \chi(1+cb^{-1}) \quad .$$

Als b alle elementen ongelijk 0 van $GF(q)$ doorloopt, dan doorloopt cb^{-1} eveneens alle elementen van $GF(q)$ ongelijk 0. Daaruit volgt dat het linkerlid van $(*)$ gelijk is aan de som van alle $\chi(a)$ met $a \neq 1$. Omdat uiteraard $\chi(1) = 1$, is het bewijs hiermee voltooid. □

De elementen van $GF(q)$ nummeren we op de een of andere manier, waarbij $a_0 = 0$. De matrix $Q = (q_{ij})$ definiëren we door

$$q_{ij} := \chi(a_i - a_j) \quad , \quad 0 \leq i, j < q \quad .$$

Q is symmetrisch als $q \equiv 1 \pmod 4$ en scheef als $q \equiv 3 \pmod 4$. Immers, in het ene geval bevat het lichaam $GF(q)$ een element van orde 4, waarvan het kwadraat -1 is, en in het andere geval is -1 geen kwadraat.

In het vervolg stelt J een matrix voor waarvan alle elementen 1 zijn. We zullen meestal nalaten de afmetingen van J aan te geven. Uit het Lemma volgt

$$Q\,Q^T = qI_q - J \quad ,$$

(ga na) en omdat de som van alle $\chi(a)$ gelijk is aan nul, geldt eveneens

$$Q\,J = J\,Q = 0 \quad .$$

Uit Q maken we een matrix C van afmetingen $q+1$ bij $q+1$ als volgt

$$C := \begin{bmatrix} 0 & 1 & 1 & \cdots & 1 \\ \pm 1 & & & & \\ . & & Q & & \\ . & & & & \\ \pm 1 & & & & \end{bmatrix} \quad ,$$

waarbij we ervoor zorgen dat C ook scheef of symmetrisch is.

Nu geldt

$$C\,C^T = qI \quad ,$$

dat wil zeggen, we hebben een conferentiematrix gemaakt. Deze constructie is bedacht door Paley, en deze matrices worden ook wel Paleymatrices genoemd.

R.E.A.C. Paley (1907-1933) publiceerde in de vier jaar van zijn wetenschappelijke loopbaan 26 artikelen van hoge kwaliteit, voornamelijk over Fouriertheorie. Hij kwam tijdens het skiën om het leven door een lawine.

8.4 De eerste orde Reed-Mullercode

Uitgaande van

$$\begin{bmatrix} + & + \\ + & - \end{bmatrix} \quad .$$

en Stelling 8.2.2 maken we achtereenvolgens Hadamardmatrices van ordes 4, 8, 16, 32, enzovoorts. Zo vinden we bijvoorbeeld H_8 van de vorm van Figuur 9.

+	+	+	+	+	+	+	+
+	−	+	−	+	−	+	−
+	+	−	−	+	+	−	−
+	−	−	+	+	−	−	+
+	+	+	+	−	−	−	−
+	−	+	−	−	+	−	+
+	+	−	−	−	−	+	+
+	−	−	+	−	+	+	−

Figuur 9
Een Hadamardmatrix van orde 8

De zo verkregen matrices noteren we met H_n, waar n de orde is. Kennelijk geldt telkens $n = 2^m$ voor zekere m. In H_n vervangen we de +1 door 0 en de −1 door 1. We vinden dan n rijen die we opvatten als rijvectoren uit $\mathbf{F}_2^n$. We nummeren de rijen van 0 tot en met $n - 1$ $(= 2^m - 1)$.
Wat gebeurt er bij de stap van m naar $m + 1$, dat wil zeggen bij verdubbeling van n? De nieuwe rijen hebben de vorm $(\mathbf{c}_i, \mathbf{c}_i)$ voor $0 \leq i < n$ en $(\mathbf{c}_i, \mathbf{c}_i + \mathbf{1}^n)$ voor $n \leq i < 2n$, waarbij $\mathbf{1}^n$ de vector (1, 1, . . . , 1) (n enen) voorstelt.

8.4.1 Stelling. Laat $R'(1,m)$ de collectie rijvectoren uit $\mathbf{F}_2^n$ zijn, verkregen uit de H_n van hierboven. Dan is $R'(1,m)$ een vectorruimte van dimensie m.
Bewijs. Voor $m = 1$ is de bewering triviaal. We gaan verder met volledige inductie naar m. Als $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ een basis van $R'(1,m)$ voorstelt, dan bestaat $R'(1,m+1)$ uit alle lineaire combinaties van de vectoren $(\mathbf{v}_i, \mathbf{v}_i)$, waar $1 \leq i \leq m$, en $(\mathbf{0}^n, \mathbf{1}^n)$, zoals we hierboven al gezien hebben. □

8.4.2 Definitie. De eerste orde *Reed-Mullercode* $R(1,m)$ van lengte $n = 2^m$ en dimensie $m + 1$ is de vectorruimte over $\mathbf{F}_2$ die wordt opgespannen door $R'(1,m)$ en de basisvector $\mathbf{1}^n$. □
De lezer die de symbolen + en − verkiest boven 0 en 1, kan de rijen van H_n en $-H_n$ als vectoren nemen. In dat geval heeft het object geen natuurlijke structuur van vectorruimte.

8.5 De Marsfoto's

De code $R(1,5)$ bestaande uit 64 woorden van 32 "letters" (elk 0 of 1) is gebruikt voor het verzenden van foto's van de planeet Mars.
De foto's worden verdeeld in vele zeer kleine vierkantjes (pixels geheten), en van elk wordt de zwartingsgraad gemeten in een schaal van 0 tot en met 63. Binair is dat zes bits. In de zes kolommen van $R(1,6)$ uit Opgave 53 wordt dit getal opgezocht en vervolgens wordt de hele bijbehorende rij van 32 bits uitgezonden. Dit duurt dus iets meer dan vijf maal zo lang als wanneer alleen maar de zwartingsgraad wordt verzonden.
Ten gevolge van ruis wordt het signaal verminkt ontvangen, waardoor de ontvanger nogal eens een 1 als 0 of een 0 als 1 interpreteert. We kunnen ons nu in elk zo'n rij van 32 bits zelfs *zeven* fouten veroorloven, zonder dat er iets misgaat.
Het zogeheten decoderen gaat als volgt. Ga eerst weer over op de representatie met ±1 en vermenigvuldig het ontvangen signaal $\mathbf{c}$ met H_{32}^T. Als er niets fout is, is het ontvangen signaal een rij van H_{32} of van $-H_{32}$, en dus is $\mathbf{c}H_{32}^T$ een vector met 31 coördinaten 0. Zo kunnen we dus zien dat $\mathbf{c}$ goed is. We bespreken niet hoe het decoderen verloopt bij een foute $\mathbf{c}$.

Figuur 10
De krater Arandas op Mars.

Opgaven

45. a) Laat C een conferentiematrix zijn. Bewijs met de methode van Stelling 8.1.1 dat C door middel van permutaties van rijen of kolommen of beide, alsmede door vermenigvuldigen van rijen of kolommen met -1 op antisymmetrische vorm gebracht kan worden als $n \equiv 0 \pmod 4$ en op symmetrische vorm als $n \equiv 2 \pmod 4$.
b) Als n oneven is en groter dan 1, dan bestaat er geen conferentiematrix van de orde n.

46. Construeer een conferentiematrix van de orde 6.

47. Laat $H = (h_{ij})$ een Hadamardmatrix van de orde n zijn, en veronderstel dat de linker kolom en de bovenste rij beide geheel uit +1-en bestaan. Nummer de rijen en kolommen van 0 tot en met $n-1$. Laat voor elke i, $1 \leq i \leq n-1$ de deelverzameling B_i van $\{1, 2, \ldots, n-1\}$ voldoen aan

$$j \in B_i \iff h_{ij} = 1 \text{ voor alle } j,\ 1 \leq j \leq n-1 \quad .$$

Bewijs dat alle B_i uit evenveel elementen bestaan, en dat iedere verzameling $\{a, b\} \subset \{1, 2, \ldots, n-1\}$ met $a \neq b$ in evenveel verzamelingen B_i is bevat.

48. Zie Definitie 8.2.1.
a) In welke rij en kolom staat het getal $a_{32}b_{23}$ in $A \otimes B$?
b) Verifieer de identiteiten die na Definitie 8.2.1 vermeld staan.

49. Bewijs dat als A en B permutatiematrices zijn, $A \otimes B$ het ook is.

50. Construeer met behulp van Stelling 8.2.2 een Hadamardmatrix van de orde 8.

51. Construeer Hadamardmatrices van de orde 24 door de constructie van 8.3 toe te passen met $q = 5$ en ook met $q = 23$.

52. Voor welke $n \leq 25$ kunnen we nu een Hadamardmatrix van de orde $4n$ construeren?
Men vermoedt dat er voor elke n die een viervoud is, een Hadamardmatrix van de orde n bestaat. (De kleinste n waarvoor men nog niet weet of er een Hadamardmatrix van die orde bestaat, is 428).

53. Bewijs dat er in de lijst van $2n$ rijen ("woorden") van $R(1,m)$ een $m+1$-tal kolommen is zodanig dat op deze $m+1$ plaatsen iedere mogelijke rij van nullen en enen precies één keer voorkomt.
(Men zegt wel dat $R(1,m)$ *systematisch* is op deze $m+1$ plaatsen).

54. Bewijs dat er bij 7 fouten of minder in c precies één goede keuze is van het gezonden signaal. (Een goede keuze is er een waarbij het veronderstelde gezonden signaal op een zo klein mogelijk aantal bits afwijkt van het feitelijk ontvangen signaal).

55. Definieer voor $n = 2^m$ en alle i, $1 \leq i \leq m$ de matrix $M_n^{(i)}$ door

$$M_n^{(i)} := I_{2^{m-i}} \otimes H_2 \otimes I_{2^{i-1}} \quad .$$

a) Hoe ziet $M_8^{(2)}$ eruit?
b) Bewijs dat $H_n = M_n^{(1)} M_n^{(2)} \cdots M_n^{(m)}$.

56. De bovengeschetste methode voor decoderen is nog te langzaam. Dit vraagstuk gaat over een manier om het decoderen vlugger te doen verlopen.
a) Als we $\mathbf{x}H_n^T$ bepalen, hoeveel *vermenigvuldigingen* met ± 1 moeten dan worden uitgevoerd?
b) Als we hetzelfde doen met de representatie uit Opgave 55 (vermenigvuldigen met 0 telt dan niet mee) hoeveel vermenigvuldigingen moeten dan worden uitgevoerd?

Hoofdstuk 9 Block designs

9.1 Balanced incomplete block designs

EEN *balanced incomplete block design* is een collectie P van v *punten* tezamen met een collectie B van b deelverzamelingen van P, *blokken* genaamd, zodanig dat voor zekere positieve gehele k, r en λ geldt:

(i) ieder blok bevat k punten,
(ii) ieder punt zit in r blokken,
(iii) ieder paar punten zit in λ blokken.

Vaak eisen we bovendien

(iv) $2 < k < v - 1$.

9.2 Terminologie en notatie

We korten "balanced incomplete block design" wel af tot BIBD, en we noemen het ook wel een 2-design. Als we de parameters van het design ook willen noemen, spreken we van BD($v,k;b,r,\lambda$) of van een 2-(v,k,λ)-design. De reden waarom we de parameters b en r mogen weglaten zal aanstonds blijken.
Volgens onze definitie ligt een blok vast door zijn punten, maar sommige auteurs gebruiken een iets ruimere definitie, waarin het toegestaan is dat er herhaalde blokken voorkomen.
In de theorie van de designs hebben v, k, b, r, λ altijd dezelfde betekenis. Veel auteurs houden in parameterlijsten zoals hierboven ook de hier gebruikte volgorde aan. De letter v voor het aantal punten (variëteiten) verraadt de landbouwkundige oorsprong van deze theorie.
Als niet voldaan is aan eis (iv), dan spreken we van een *triviaal* design. Welke zijn de triviale designs?

9.3 De incidentiematrix

Om een BD($v,k;b,r,\lambda$) te beschrijven voeren we de zogeheten *incidentiematrix* A van het design in. We nummeren de punten van P als $P_1,P_2,\ldots,P_v$ en de blokken van B als $B_1,B_2,\ldots,B_b$. Merk op dat we kleine hoofdletters gebruiken voor de punten en blokken en grote hoofdletters voor de verzamelingen van alle punten respectievelijk alle blokken. De matrix A heeft b rijen en v kolommen, heeft uitsluitend nullen en enen als elementen, en wel

$$a_{ij} = 1 \quad \text{als } P_j \in B_i$$
$$a_{ij} = 0 \quad \text{anders} \quad .$$

De definitie van een BIBD kunnen we als volgt vertalen in eigenschappen van A.

(i) Iedere rij van A heeft k enen,
(ii) iedere kolom van A heeft r enen,
(iii)twee verschillende kolommen van A hebben inprodukt λ.

Dit kunnen we ook als volgt schrijven:

$$AJ = kJ$$

in plaats van (i), en in plaats van (ii) en (iii) samen:

$$A^TA = (r - \lambda)I + \lambda J \quad .$$

We brengen de conventie betreffende J van het vorige hoofdstuk in herinnering (zie 8.3).

9.3.1 Stelling. Voor de parameters van een BD($v,k;b,r,\lambda$) geldt

(i) $bk = vr$,
(ii) $\lambda(v-1) = r(k-1)$.

Bewijs. (i) Tel het aantal enen in A op twee manieren, eerst per rij en daarna per kolom. Dit geeft respectievelijk het linkerlid en het rechterlid van (i).
(ii) We tellen het aantal *horizontale* paren (1,1) in de matrix A met de voorste 1 in kolom 1. Dit doen we op twee manieren. Er zijn r rijen met een 1 in de eerste kolom, immers de eerste kolom heeft precies r enen. Elk van die r rijen heeft nog $k-1$ andere enen. In totaal zijn er dus $r(k-1)$ paren (i,j) met $j \neq 1$ en $a_{i1} = a_{ij} = 1$.
Anderzijds, er zijn $v-1$ kolommen met nummers 2 tot en met v. Elk van die kolommen heeft inprodukt λ met de eerste, dat wil zeggen, in elk van die kolommen staan λ enen die een bijbehorende 1 in de eerste kolom hebben. Op deze manier tellende vinden we $\lambda(v-1)$ horizontale paren (1,1) met een 1 in de eerste kolom. □

9.3.2 Stelling. (Fisher) Voor de parameters van een niet-triviaal BD$(v,k;b,r,\lambda)$ geldt

$$b \geq v \quad .$$

Bewijs. We bepalen de determinant van de v bij v matrix A^TA. Op de hoofddiagonaal staat overal r, en elders λ. Trek eerst de bovenste rij van alle volgende rijen af. Tel daarna kolom 2 tot en met kolom v bij de eerste kolom op. Zo ontstaat een bovendriehoeksmatrix, met in de linkerbovenhoek $r + (v-1)\lambda$, dat wil zeggen rk wegens Stelling 9.3.1 (ii), en verder $r - \lambda$ langs de diagonaal.
De determinant van A^TA is dus $rk(r-\lambda)^{v-1}$, hetgeen niet nul is, omdat $\lambda=r$ zou betekenen $v = k$. Dus de rang van A^TA is v, en daarom rang$(A) \geq v$. Dus A heeft ten minste v rijen, waarmee het bewijs voltooid is. □

9.4 Symmetrische designs

Het is een gewoonte geworden om een block design *symmetrisch* te noemen als $b = v$ (en dus ook $r = k$). Merk op dat dit betekent dat de bijbehorende matrix A *vierkant* is, maar *niet* dat A noodzakelijk symmetrisch is.
In een symmetrisch design zijn de begrippen punt en blok in zekere zin verwisselbaar. De volgende stelling gaat daarover.

9.4.1 Stelling. Laat A de incidentiematrix van een symmetrisch 2-(v,k,λ) design zijn. Dan geldt

$$AA^T = (k-\lambda)I + \lambda J \quad .$$

Bewijs. We gaan aantonen dat A^T eveneens incidentiematrix is van een 2-(v,k,λ) design. Dat elke rij en elke kolom van A^T precies k enen heeft, spreekt vanzelf.
We gaan nu door verstandig tellen het inprodukt van een willekeurige rij van A met een andere berekenen. Laat B een willekeurig blok van het gegeven design zijn. Laat verder voor elke i $(0 \leq i \leq v)$ a_i het aantal van de overige blokken voorstellen dat precies i punten met B gemeen heeft.
Omdat er $v-1$ overige blokken zijn, geldt

$$\sum_i a_i = v - 1 \quad . \tag{i}$$

Als we in de kolommen waar B een 1 heeft, enen in de overige rijen gaan tellen, eerst per rij (blok) en dan per kolom, vinden we

$$\sum_i i a_i = k(k-1) \quad . \tag{ii}$$

Tenslotte tellen we, wederom in de rijen ongelijk B, horizontale paren (1,1) met beide enen in

dezelfde kolom als een 1 uit B. We vinden dan

$$\sum_i \binom{i}{2} a_i = \binom{k}{2} \quad . \tag{iii}$$

Als we 2 maal (iii), $(1 - 2\lambda)$ maal (ii) en λ^2 maal (i) bij elkaar tellen, vinden we met gebruikmaking van Stelling 9.3.1 (ii):

$$\sum_i (i - \lambda)^2 a_i = 0 \quad , \tag{iv}$$

waaruit volgt dat $a_i = 0$ tenzij $i = \lambda$. Met andere woorden, alle overige blokken van het design hebben precies λ punten gemeen met B. In termen van de incidentiematrix wil dit zeggen dat de met B corresponderende rij van A met alle andere rijen inprodukt λ heeft. □

Zoals al opgemerkt in het bewijs van Stelling 9.4.1 is in geval van een vierkante incidentiematrix A van een block design, de matrix A^T eveneens incidentiematrix van een block design (maar in het algemeen niet hetzelfde). We noemen dit design het *duale* design van het oorspronkelijke design.

We kunnen uit een symmetrisch block design nog op twee andere manieren nieuwe block designs maken en wel als volgt. Kies een van de blokken. De nieuwe puntenverzameling bestaat dan uit hetzij de punten van het uitverkoren blok, hetzij die van het complement. In beide gevallen nemen we voor de nieuwe blokken de doorsnede van de overige oude blokken met de nieuwe puntenverzameling. In het ene geval spreken we van een *derived* design (een 2-$(k, \lambda, \lambda - 1)$ design) en in het andere geval van een *residual* design (een 2-$(v-k, k-\lambda, \lambda)$ design). Merk op dat in het derived design en in het residual design herhaalde blokken kunnen voorkomen, zoals in de eerder vermelde ruimere definitie ook is toegestaan. De incidentiematrices D en R van het derived design en het residual design verkrijgen we uit die van A, door de kolommen van A om te schikken totdat een van de rijen (zeg de bovenste) bestaat uit een rij enen, gevolgd door een rij nullen. Dan bestaat de matrix A uit vier delen als volgt

1 1 1 . . . 1	0 0 0 . . . 0
D	R

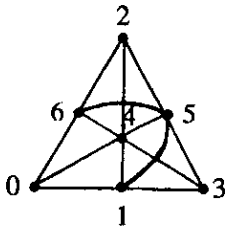
9.5 Voorbeelden

9.5.1 Een 2-(7,3,1) design

Neem als punten de elementen van $\mathbf{F}_7$. We beginnen met het blok $B_0 = \{0,1,3\}$. Voor elke i met $1 \leq i \leq 6$ vormen we B_i door i bij ieder element van B_0 op te tellen (modulo 7).

Merk op dat de zes *verschillen* van paren elementen uit B_0 juist de elementen van $\mathbf{F}_7 \setminus \{0\}$ zijn. Bij gegeven ongelijke x en y is er één paar (a,b) in B_0 met $a - b = x - y$. Dat wil zeggen dat x en y samen in B_{x-a} zitten. We hebben dus een symmetrisch 2-(7,3,1) design geconstrueerd. Dit design wordt vaak aangegeven als in Figuur 11. Het wordt ook wel het *Fano-vlak* genoemd.

G. Fano (1871-1952), een Italiaans wiskundige, was een pionier op het gebied van de eindige meetkundes.

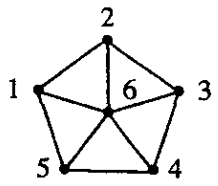


Figuur 11
Het Fano-vlak

Op dezelfde wijze kunnen we een 2-(13,4,1) design maken met behulp van $\mathbf{F}_{13}$. De lezer wordt aangeraden dit te proberen; we zullen nog enkele malen op dit 2-(13,4,1) design terugkomen.

9.5.2 Een 2-(6,3,2) design

Beschouw de graaf† van Figuur 12.



Figuur 12

Op de verzameling {1,2,3,4,5,6} van hoekpunten van G maken we een design door als blokken alle verzamelingen $\{x,y,z\}$ van drie hoekpunten te nemen, die één of drie ribben van G bevatten. Bijvoorbeeld {1,2,6} en {1,2,4} zijn blokken. Op deze manier ontstaat een 2-(6,3,2) design. Ga dit na. Hoeveel blokken zijn er? De drietallen die geen blok vormen in het zojuist geconstrueerde design, vormen samen ook een 2-(6,3,2) design.

9.5.3 Een 2-(16,6,2) design

Op de puntverzameling $\{1,2,\ldots,16\}$ maken we een design met 16 blokken. In Figuur 13 vormen de vetgedrukte getallen juist B_{10}; merk op dat 10 zelf geen element is van B_{10}.
Voor elke i, $1 \leq i \leq 16$ bestaat B_i uit de zes getallen ongelijk i die in dezelfde rij en kolom staan als i. Ga na dat dit een symmetrisch 2-(16,6,2) design oplevert.

9.5.4 Hadamard 2-designs

Een *Hadamard* 2-design is een 2-$(4m-1, 2m-1, m-1)$ design dat op de volgende manier is verkregen uit een genormaliseerde Hadamardmatrix van orde $4m$ (zie 8.1). Laat de eerste rij en kolom (die geheel uit +1 bestaan) weg. Vervang dan alle −1 door 0. Zo verkrijgen we de incidentiematrix van het design. Dat dit inderdaad een design is volgt uit het telargument in

† Dit woord (meervoud: grafen) is gevormd naar analogie met paragraaf, autograaf, epigraaf en holograaf, die allemaal een geschrift betekenen.

Verwante woorden zijn fotograaf, lexicograaf, kalligraaf, biograaf en geograaf, alsmede telegraaf, seismograaf, pantograaf en nog ongeveer 100 andere, die allemaal een schrijvende mens of machine betekenen.

Met rijksgraaf, dijkgraaf, meigraaf of zelfs loopgraaf heeft het woord niets uit te staan. Sommige auteurs prefereren daarom het Engelse *graph* (meervoud: graphen) of zelfs graf (meervoud: ?).

1	**2**	3	4
5	**6**	7	8
9	10	**11**	**12**
13	**14**	15	16

Figuur 13

het bewijs van Stelling 8.1.1.

9.5.5 Een 2-(10,4,2) design
Beschouw het symmetrische 2-(16,6,2) design van 9.5.3. Kies hierin een willekeurig blok. Het bijbehorende residual design is een BD(10,4;15,6,2). Het bijbehorende derived design is triviaal, want het bestaat uit alle $\binom{6}{2}$ paren uit zes elementen.

9.5.6 Een 2-(15,3,1) design
Neem als puntenverzameling de vijftien elementen ongelijk 0 uit GF(2^4). Blokken zijn verzamelingen $\{x,y,z\}$ met $x+y+z=0$. Men gaat eenvoudig na (doen!) dat dit een BD(15,3;35,7,1) is.

9.6 Projectieve en affiene vlakken

Een symmetrisch block design met $\lambda = 1$ noemt men ook wel een *projectief vlak*. In dit geval heten de blokken ook wel *lijnen*. Uit Stelling 9.3.1 volgt dat $v = k(k-1)+1$. De eisen (i) tot en met (iii) van de definitie in 9.1 kunnen we nu zó formuleren:

(i) iedere lijn bevat k punten,
(ii) ieder punt ligt op k lijnen,
(iii)door twee verschillende punten gaat precies één lijn.

Uit Stelling 9.4.1 volgt dat ieder tweetal lijnen in een projectief vlak een snijpunt heeft; er zijn dus *geen* "evenwijdige" lijnen.
Het is gebruikelijk om het getal $n := k-1$ de *orde* van het vlak te noemen. Het aantal punten is dan n^2+n+1, het aantal lijnen eveneens, en op iedere lijn liggen $n+1$ punten.
In 9.5.1 zagen we het projectieve vlak van de orde 2, het Fano-vlak. Bedenk dat in Figuur 11 de verzameling {1,6,5} een van de "lijnen" is.

Stelling 9.6.1. Als n-de macht van een priemgetal is ($n \neq 1$), dan bestaat er ten minste één projectief vlak van de orde n.
Bewijs. We gebruiken als hulpverzameling de verzameling X_n van drietallen $(x,y,z) \in \mathbf{F}_n^3$ die voldoen aan de volgende eisen:

(*) ten minste één van de drie coördinaten x, y, z is ongelijk 0,
(**)de eerste coördinaat die niet 0 is, is 1.

Dus X_n bevat alle drietallen $(0,0,1)$, $(0,1,x)$, $(1,x,y)$, waarbij x en y verder willekeurig zijn in $\mathbf{F}_n$. Merk op dat geen punt in X_n een scalair veelvoud is van een ander punt in X_n, en dat elk punt van $\mathbf{F}_n^3 \setminus \{(0,0,0)\}$ scalair veelvoud is van precies één punt van X_n.
Deze hulpverzameling X_n gebruiken we voor het parametriseren van zowel de verzameling punten als de verzameling lijnen. Een punt noteren we als $P(x,y,z)$, met $(x,y,z) \in X_n$ en een lijn als $L(a,b,c)$, met $(a,b,c) \in X_n$. We spreken af dat $L(a,b,c)$ juist die punten $P(x,y,z)$ bevat, die voldoen aan

$$ax + by + cz = 0 \quad .$$

(i) Als we punten zoeken die (voor gegeven $(a,b,c) \in X_n$) op $L(a,b,c)$ liggen, moeten we één vergelijking met drie onbekenden oplossen. Er zijn in totaal n^2 oplossingen, maar als we de verboden (0,0,0) niet meerekenen, $n^2 - 1$. Bij iedere oplossing (x,y,z) is ook $(\lambda x, \lambda y, \lambda z)$ met $\lambda \in \mathbf{F}_n \setminus \{0\}$ een oplossing. De totale verzameling oplossingen ongelijk (0,0,0) valt dus uiteen in $(n^2 - 1)/(n - 1)$ groepjes van oplossingen. Binnen elk zo'n groepje zijn de oplossingen scalaire veelvouden van elkaar, en elk zo'n groepje bevat precies één element van onze hulpverzameling X_n. Het aantal punten $P(x,y,z)$ in $L(a,b,c)$ is dus gelijk aan het aantal van die groepjes, dat wil zeggen aan $n + 1$.
Precies op dezelfde manier vinden we dat elk punt $P(x,y,z)$ op $n + 1$ lijnen $L(a,b,c)$ ligt.
(ii) Als we een lijn $L(a,b,c)$ zoeken, die twee verschillende punten $P(x_1,y_1,z_1)$ en $P(x_2,y_2,z_2)$ bevat, moeten we twee vergelijkingen met drie onbekenden oplossen. Omdat (x_1,y_1,z_1) en (x_2,y_2,z_2) onafhankelijk zijn, zijn alle oplossingen (a,b,c) ongelijk (0,0,0) scalaire veelvouden van elkaar. Daarom is er maar één lijn $L(a,b,c)$ die beide punten bevat.
Hiermee is aan alle eisen voldaan. □
Het zojuist geconstrueerde projectieve vlak wordt meestal $PG(2,n)$ genoemd, dat wil zeggen "Projective Geometry of dimension 2 and order n". Wat er eigenlijk in het bewijs van Stelling 9.6.1 gebeurt is het volgende. Beschouw in de 3-dimensionale vectorruimte over $GF(n)$ alle *lijnen* door de oorsprong en alle *vlakken* door de oorsprong. Een lijn P geven we door haar richtingsvector (x,y,z) en een vlak L door de normaal (a,b,c) ervan. Dan ligt P in L als $ax + by + cz = 0$. Het enige wat dan verder gebeurt is naamsverandering. Lijnen worden punten genoemd en vlakken worden lijnen. Daarom worden coördinaten in $PG(2,n)$ meestal anders gedefinieerd dan wij het hebben gedaan. Men gebruikt *alle* drietallen $(x,y,z) \neq (0,0,0)$ en men spreekt af dat de drietallen (x,y,z) en $(\lambda x, \lambda y, \lambda z)$ hetzelfde punt van het vlak bepalen als $\lambda \neq 0$. Ze stellen immers dezelfde lijn door de oorsprong voor. Men noemt dit *homogene* coördinaten. Wij zullen deze methode in het vervolg ook gebruiken.
Er zijn ook andere projectieve vlakken dan degene die volgens deze methode geconstrueerd worden. Alle bekende voorbeelden hebben echter wel een orde die een macht is van een priemgetal. Een beroemd open probleem is of er ook andere ordes zijn dan priemmachten. Bekend is, dat er geen projectief vlak van orde 6 bestaat. Men vermoedt dat er geen projectief vlak van orde 10 bestaat.

9.6.2 Definitie. Een BD$(n^2, n; n^2+n, n+1, 1)$ wordt een *affien vlak* van orde n genoemd. □
Een voorbeeld is uit de lineaire algebra bekend voor het geval dat n macht is van een priemgetal, namelijk de collectie van n^2 punten en $n^2 + n$ rechten uit het vlak $\mathbf{F}_n^2$.
Een punt is een paar $(x,y) \in \mathbf{F}_n^2$ en een rechte wordt gegeven door een vergelijking $ax + by = c$, waarbij $(a,b) \neq (0,0)$. Er zijn inderdaad $n^2 + n$ rechten, zoals men eenvoudig nagaat (doen!).
Voor het zojuist geconstrueerde affiene vlak geldt het zogeheten *parallellenaxioma*. Dit luidt:

> Bij iedere lijn l en ieder punt $P \notin l$ is er precies één lijn m door P zodanig dat l en m geen punt gemeenschappelijk hebben, dat wil zeggen zodanig dat l en m *evenwijdig* zijn.

We gaan nu met behulp van een telargument bewijzen dat dit voor elk affien vlak geldt.

9.6.3 Stelling. Laat B een 2-$(n^2, n, 1)$ design zijn, met andere woorden, B is een affien vlak van de orde n. Laat B_1 een blok zijn van B en P een punt met $P \notin B_1$. Dan is er precies één blok B_2 zodanig dat $P \in B_2$ en $B_1 \cap B_2 = \emptyset$.
Bewijs. Laat $B = \{P_1, P_2, \ldots, P_n\}$. Voor elke i, $1 \leq i \leq n$ is er precies één blok dat P en P_i bevat. Bij verschillende i horen zo verschillende blokken, omdat door ieder tweetal $\{P_i, P_j\}$ slechts één blok gaat, namelijk B, en $P \notin B$. Door P gaan echter $n + 1$ blokken, waaronder dus precies één dat geen enkel punt met B gemeen heeft. □

9.7 De Stelling van Singer

We zagen in 9.5.1 een constructie van $PG(2,2)$; met $\mathbf{F}_{13}$ verkrijgt men een analoge constructie van $PG(2,3)$. De bijbehorende incidentiematrices waren in beide gevallen cyclisch. Dat wil zeggen, elke rij kan uit de vorige gevormd worden door alle elementen een positie op te schuiven en de laatste vooraan te zetten.

We zullen nu aantonen dat dit voor iedere $PG(2,p)$ kan met p priem. Het bewijs voor $PG(2,q)$ met q een macht van een priemgetal is analoog, maar het is eenvoudiger om ons tot priemgetallen p te beperken.

We beschouwen nog eens de logaritmentafel van het lichaam $GF(p^3)$ zoals in 6.11. Laat α een primitief element zijn, en definieer

$$\beta := \alpha^{p^2+p+1} \quad .$$

Dan geldt

$$\beta^{p-1} = (\alpha^{p^2+p+1})^{p-1} = \alpha^{p^3-1} = 1 \quad ,$$

en dus is β een element van $\mathbf{F}_p$. Laat V (zie Figuur 14) het stuk van de logaritmentafel zijn, behorende bij de machten α^i met $0 \leq i \leq p^2+p$.

	1	α	α^2
$1 =$	1	0	0
$\alpha =$	0	1	0
$\alpha^2 =$	0	0	1
	.	.	.
	.	.	.
	.	.	.
$\alpha^{p^2+p} =$	.	.	.

Figuur 14

De volgende rij van de tafel behoort bij β, en omdat $\beta \in \mathbf{F}_p$, is deze rij blijkbaar $(\beta\ 0\ 0)$. Dit betekent dat de rijen behorende bij α^i met

$$p^2 + p + 1 \leq i < 2(p^2 + p + 1)$$

verkregen kunnen worden door alle rijen van V met β te vermenigvuldigen. De daarop volgende $p^2 + p + 1$ rijen ontstaan door de rijen van V met β^2 te vermenigvuldigen, enzovoorts.

De rijen van de volledige logaritmentafel representeren juist alle vectoren ongelijk aan (0,0,0) uit de ruimte $\mathbf{F}_p^3$. De rijen van V representeren precies de $p^2 + p + 1$ punten van $PG(2,p)$. Immers, waar een vector (x,y,z) ook in de logaritmentafel staat, het is een veelvoud van een vector in V.

We gaan nu een incidentiematrix maken voor $PG(2,p)$. De puntenverzameling heeft al een natuurlijke nummering omdat elk punt met een element van V correspondeert en elk element van V is de coëfficiëntenrij van een zekere α^i. Die i is het nummer van zo'n punt.

Kies nu een lijn in $PG(2,p)$. De gekozen lijn laten we corresponderen met de eerste rij van onze incidentiematrix. Elk drietal punten op die lijn correspondeert met een drietal rijtjes uit V, die horen bij zekere machten van α, zeg α^i, α^j en α^k. Omdat de bijbehorende punten van $PG(2,p)$ op één lijn liggen, zullen deze drie rijtjes uit V afhankelijk zijn. Dat betekent dat voor zekere c_1, c_2 en c_3 in $\mathbf{F}_p$ geldt

$$c_1\alpha^i + c_2\alpha^j + c_3\alpha^k = 0 \quad .$$

Maar dan geldt ook

$$c_1\alpha^{i+1} + c_2\alpha^{j+1} + c_3\alpha^{k+1} = 0 \quad .$$

Dat wil zeggen, ook α^{i+1}, α^{j+1} en α^{k+1} corresponderen met een drietal punten op één lijn. Als we de volgende rij in de incidentiematrix voor deze lijn bestemmen, dan zal die rij ten opzichte van de eerste een positie naar rechts geschoven zijn. Immers, met elk drietal enen in kolommen i, j en k van de eerste rij correspondeert een drietal enen in kolommen $i+1$, $j+1$ en $k+1$ in de tweede rij. Vanzelfsprekend, als $k = p^2 + p$, dan $\alpha^{k+1} = \beta$, en dus zal in dat geval de volgende rij in de incidentiematrix met een 1 beginnen, omdat β en α^0 hetzelfde punt voorstellen. Eveneens vanzelfsprekend is dat we de derde, en volgende rijen in de incidentiematrix op dezelfde manier uit hun voorgangers kunnen vormen. De onderste rij zal, cyclisch verschoven, weer de bovenste zijn.
Hiermee is een stelling bewezen, die voor het eerst door J. Singer in 1938 werd geformuleerd en bewezen:

9.7.1 Stelling van Singer. Voor ieder priemgetal p bestaat er een projectief vlak van de orde p met een cyclische incidentiematrix. □

9.7.2 Voorbeeld. Over $\mathbf{F}_3$ is $x^3 - x + 1$ primitief. Van de logaritmentafel van $GF(27)$ ziet het stuk dat we V genoemd hebben, er uit als in Figuur 15.

	1	x	x^2
$x^0 =$	1	0	0
$x^1 =$	0	1	0
$x^2 =$	0	0	1
$x^3 =$	2	1	0
$x^4 =$	0	2	1
$x^5 =$	2	1	2
$x^6 =$	1	1	1
$x^7 =$	2	2	1
$x^8 =$	2	0	2
$x^9 =$	1	1	0
$x^{10} =$	0	1	1
$x^{11} =$	2	1	1
$x^{12} =$	2	0	1

Figuur 15

De 13 machten van x vormen de punten van het projectieve vlak $PG(2,3)$. In de vectorruimte $\mathbf{F}_3^3$ vormen de vier vectoren met laatste coördinaat 0 een vlak. Dit wil zeggen dat de vier rijen van V behorende bij x^i, voor $i = 0, 1, 3, 9$, (juist de vier rijen die op een 0 eindigen) vier punten van $PG(2,3)$ vormen op één lijn, namelijk de lijn $L(0,0,1)$. Hiermee hebben we een van de oplossingen van de vraag in 9.5.1, namelijk het viertal $\{0,1,3,9\}$ modulo 13, gevonden.

9.8 Steinersystemen

We beginnen met een methode die het idee van 9.5.1 generaliseert. Ook deze methode maakt gebruik van eindige lichamen.

9.8.1 Stelling. Laat $v = 6t + 1 = q$, waar q een macht is van een priemgetal. Laat α een primitief element zijn van $GF(q)$. Laat voor elke i met $0 \leq i < t$ en elke $\xi \in GF(q)$ het blok $B_{i,\xi}$ door

$$B_{i,\xi} := \{\alpha^i + \xi\ ,\ \alpha^{2t+i} + \xi\ ,\ \alpha^{4t+i} + \xi\}$$

gedefinieerd zijn. Dan vormen deze blokken een 2-$(v,3,1)$ design.
(De blokken $B_{i,\xi}$ met $\xi = 0$ heten basisblokken).
Bewijs. Het idee is hetzelfde als in 9.5.1. Bij elk tweetal elementen x en y van $GF(q)$ moeten we een i vinden en een a en b in $B_{i,0}$, zodanig dat $x - y = a - b$. Immers, dan is $B_{i,x-a}$ juist het blok dat x en y bevat.
Om in te zien dat we zo'n i kunnen vinden, gaan we beredeneren dat alle elementen van $GF(q)$ elk precies één maal voorkomen als verschil van elementen in een basisblok.
Om te beginnen bepalen we de zes verschillen uit $B_{0,0}$, dat wil zeggen uit $\{1,\alpha^{2t},\alpha^{4t}\}$. We merken op dat $\alpha^{6t} = 1$, dus $\alpha^{3t} = -1$, omdat α primitief is. Verder is $\alpha^{2t} - 1$ te schrijven als macht van α,zeg als α^s, wederom omdat α primitief is. De verschillen zijn

$$\alpha^{2t} - 1 = \alpha^s \qquad \text{en } -(\alpha^{2t}-1) = \alpha^{s+3t}\ ,$$

$$\alpha^{4t} - \alpha^{2t} = \alpha^{s+2t} \qquad \text{en } -(\alpha^{4t} - \alpha^{2t}) = \alpha^{s+5t}\ ,$$

$$1 - \alpha^{4t} = \alpha^{6t} - \alpha^{4t} = \alpha^{s+4t} \quad \text{en } -(1 - \alpha^{4t}) = \alpha^{s+t}\ .$$

De zes verschillen van een basisblok $B_{i,0}$ zijn gelijk aan het produkt van de verschillen van $B_{0,0}$ en α^i, waarbij $0 \leq i < t$. We vinden dus elke macht α^j $(0 \leq j < 6t)$ ergens als verschil van basisblokelementen. □
Merk op dat we op deze manier $tv = t(6t + 1)$ blokken construeren, maar dat Stelling 9.3.1 al impliceert dat een 2-$(6t+1,3,1)$ design precies zoveel blokken heeft.
De andere constructies gebruiken een idee dat we in vorige hoofdstukken al enkele keren hadden gezien, namelijk uit twee kleintjes een grote maken.

9.8.2 Definitie. Een *Steiner Triple System* is een 2-$(v,3,1)$ design. We schrijven ook wel STS(v). □
J. Steiner (1796-1863), Zwitsers boerenzoon en autodidact, was een van de toonaangevende meetkundigen in Duitsland. Hij herstelde de zuivere begrippelijke meetkunde in ere, en moest niets hebben van berekeningen met coördinaten en van tekeningen.
De term Steiner System werd overigens voor het eerst in 1938 gebruikt door E. Witt, die zich evenmin als Steiner realiseerde dat de Engelse wiskundigen W.S.B. Woolhouse en de Reverend T.P. Kirkman eerder dan Steiner waren met respectievelijk de definitie en belangrijke resultaten.
Uit Stelling 9.3.1 volgt dat voor de parameter v van een STS(v) geldt $v \equiv 1 \pmod 6$ of $v \equiv 3 \pmod 6$, en dat verder $b = v(v-1)/6$ voor het aantal blokken.

9.8.3 Voorbeelden.

(i) Het triviale design bestaande uit één blok van drie punten voldoet niet aan de eis $k < v - 1$, maar is wel een STS(3).
(ii) $PG(2,2)$ is een STS(7).
(iii)Het affiene vlak van de orde 3 uit 9.5.1 is een STS(9).

(iv)In Opgave 75 wordt een STS(13) geconstrueerd.
(v) In 9.5.6 gaven we een voorbeeld van een STS(15).
(vi)Uit Stelling 9.7.1 volgt dat een STS(v) bestaat voor $v = 19, 25, 31, 37$.

Van de mogelijke waarden van v onder de 40 hebben we nu alleen 21, 33 en 39 nog niet gehad. Daar deze getallen verschillende priemfactoren hebben, is wellicht een produktconstructie mogelijk.

We beginnen met het eenvoudigste voorbeeld, 21. We hebben al een STS(7), zeg op de verzameling $\{1,2,3,4,5,6,7\}$. We vormen een verzameling van 21 punten die we a_i, b_i en c_i noemen, waar $1 \leq i \leq 7$. Als blokken nemen we nu de zeven tripels $\{a_i, b_i, c_i\}$, met $1 \leq i \leq 7$, en verder alle tripels $\{a_i, b_j, c_k\}$ met $\{i, j, k\}$ in het gegeven STS(7). We hebben nu al $7 + 42$ blokken. Tenslotte nemen we als blokken alle 21 tripels $\{a_i, a_j, a_k\}$, $\{b_i, b_j, b_k\}$, $\{c_i, c_j, c_k\}$, waar $\{i, j, k\}$ weer uit het gegeven STS(7) komen. Ieder tweetal punten komt nu in precies één blok samen voor, en het totaal aantal blokken is inderdaad 70.

Op dezelfde manier is een STS(39) te construeren. Algemener hebben we de volgende Stelling.

9.8.4 Stelling. Als een STS(v_1) en een STS(v_2) beide bestaan, dan bestaat er ook een STS($v_1 v_2$).

Bewijs. Neem aan dat voor $i = 1, 2$ een STS(v_i) gegeven is op de puntverzameling V_i met blokkenverzameling S_i. Neem nu als puntverzameling $V_1 \times V_2$. Als blokkenverzameling nemen we alle drietallen $\{(x_1,y_1), (x_2,y_2), (x_3,y_3)\}$, waar hetzij $x_1 = x_2 = x_3$ hetzij $\{x_1, x_2, x_3\} \in S_1$, en waar bovendien voor de y iets dergelijks geldt: $y_1 = y_2 = y_3$ of $\{y_1, y_2, y_3\} \in S_2$. (Als zowel de x-en als de y's onderling gelijk zijn, dan hebben we geen drietal, dus die gevallen doen niet mee).

Daar ieder tweetal punten (x,y) en (x',y') precies één maal in een van onze zojuist gedefinieerde blokken voorkomt, vormt deze blokkenverzameling een STS($v_1 v_2$) op $V_1 \times V_2$. []

9.8.5 Voorbeeld. Een STS(63) is zo uit het STS(7) en het STS(9) te maken.

We hebben nog geen STS(33); we gaan nu een STS(33) maken met een wat ingewikkelder constructie.

Stel dat S een STS(v_1) is op een verzameling V_1. Het kan gebeuren dat er een deelverzameling V van V_1 is met de eigenschap dat bij ieder tweetal punten uit V het derde element van het bijbehorende tripel ook in V ligt. In dat geval vormen deze tripels zelf een STS op de verzameling V. Dat STS noemen we dan een *deelsysteem* op V. Een triviaal voorbeeld is een lijn in $PG(2,2)$. Dat is een STS(3) in een STS(7).

9.8.6 Stelling. Als er een STS(v_1) bestaat met een deelsysteem op v punten en als er verder een STS(v_2) bestaat, dan is er een STS($v + v_2(v_1 - v)$).

Bewijs. Definieer $s := v_1 - v$. Laat S_1 de blokkenverzameling van een STS(v_1) zijn op $V_1 := \{1, \ldots, v_1\}$ en veronderstel dat S_1 een deelsysteem heeft op de v punten van $V := \{s + 1, \ldots, v_1\}$. Laat verder S_2 de blokkenverzameling van een STS(v_2) op $V_2 := \{1, \ldots, v_2\}$ zijn.

De puntenverzameling van ons te construeren STS bestaat uit

(a) de getallen van V;
(b) de getallenparen (x,y) met $1 \leq x \leq s$ en $1 \leq y \leq v_2$.

De eerste coördinaat van zo'n punt van type (b) zit dus nooit in het deelsysteem. Het aantal punten klopt nu. Er zijn vier soorten blokken:

(i) de blokken van het deelsysteem op V, deze blokken bestaan dus geheel uit punten van type (a);

(ii) $\{(a,y), (b,y), c\}$ met $\{a,b,c\} \in S_1$ en $y \in V_2$;
(iii)$\{(a,y), (b,y), (c,y)\}$ met $\{a,b,c\} \in S_1$ en $y \in V_2$.
We zouden deze drie soorten kunnen samenvatten door in alle tripels $\{(a,y), (b,y), (c,y)\}$ met a,b,c *willekeurig* in V_1 maar uiteraard wel $\{a,b,c\} \in S_1$ en $y \in V_2$, de paren (x,y) met $x \in V$ (die helemaal niet in onze puntenverzameling voorkomen) te vervangen door hun eerste coördinaat x (die wel in onze puntenverzameling voorkomt).
De vierde soort bestaat uit blokken van de vorm
(iv)$\{(x_1,y_1), (x_2,y_2), (x_3,y_3)\}$ met y_1,y_2,y_3 onderling verschillend.
Van deze soort blijken we er (als we netjes tellen)

$$\frac{v_2(v_2-1)}{6}s^2$$

nodig te hebben. We moeten nog een geschikte regel bedenken die er voor zorgt dat ieder paar punten in één tripel voorkomt.
De eis $y_1,y_2,y_3 \in S_2$ ligt voor de hand. Voor gegeven y_1 en y_2 ligt dan y_3 vast. Voor de x kiezen we de regel

$$x_1 + x_2 + x_3 \equiv 0 \pmod{s} \quad .$$

Op die manier zijn er bij gegeven y_1 en y_2 juist de gewenste s^2 mogelijkheden, en het is eenvoudig in te zien dat ieder tweetal uit onze merkwaardige puntenverzameling in precies één tripel voorkomt. □

9.8.7 Voorbeeld. We maken een STS(33) door $v_1 = 13$ en $v_2 = 3$ te nemen. Op S_1 nemen we een blok als triviaal deelsysteem.
Het is mogelijk om met dit soort constructies aan te tonen dat een STS(v) bestaat voor iedere $v \geq 3$ met $v \equiv 1$ of $v \equiv 3 \pmod 6$.

9.9 Enige toepassingen

9.9.1 Een proefopzet met twee factoren

Een object kan uit zeven verschillende metalen worden gemaakt, en er zijn zeven verschillende fabricageprocessen voor dit object. Men wil een keuze maken. Het is te duur om alle 49 combinaties te onderzoeken. Als men twee metalen met elkaar vergelijken wil, dan moeten die met hetzelfde fabricageproces verwerkt worden. Iets dergelijks geldt voor de processen. We gebruiken het Fano-vlak voor de constructie van de proefopzet. We krijgen dan voor de incidentiematrix A die van Figuur 16.

	0	1	2	3	4	5	6
0	1	1		1			
1		1	1		1		
2			1	1		1	
3				1	1		1
4	1				1	1	
5		1				1	1
6	1		1				1

Figuur 16

Zie ook 9.5.1. Men doet 21 experimenten in plaats van 49 en wel zó: we gebruiken het i-de

metaal en het j-de fabricageproces alleen als er een 1 staat in rij i en kolom j van A. We kunnen nu ieder tweetal metalen en ieder tweetal processen eerlijk vergelijken. Dat wil zeggen, elk metaal wordt met drie verschillende processen beproefd, en elk proces met drie verschillende metalen. Op deze manier (de vergelijking van kwalitatief verschillende zaken) worden block designs vaak toegepast in de statistiek.

9.9.2 Een proefopzet met drie factoren

Stel men wil 13 soorten tandpasta laten vergelijken door 13 proefpersonen. De proefpersonen kunnen niet teveel vergelijkingen maken. We besluiten gebruik te maken van het symmetrische 2-(13,4,1) design dat wij als $PG(2,3)$ kennen. Iedere proefpersoon krijgt 4 tubes tandpasta en iedere soort tandpasta wordt door 4 personen beoordeeld. Op dezelfde manier als in het vorige voorbeeld maken we nu een matrix A, deze maal met 13 rijen en 13 kolommen. We besluiten echter de proef uit te breiden. We willen weten of de *kleur* van de tube ook een rol speelt. Het komt goed van pas dat het design cyclisch is (zie Stelling 9.6.3). De proefpersonen 0 tot en met 12 krijgen tubes van soort 0 tot en met 12 in de kleuren Rood, Wit, Blauw en Geel, volgens het schema van Figuur 17.

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	R	W		B						G			
1		R	W		B						G		
2			R	W		B						G	
3				R	W		B						G
4	G				R	W		B					
5		G				R	W		B				
6			G				R	W		B			
7				G				R	W		B		
8					G				R	W		B	
9						G				R	W		B
10	B						G				R	W	
11		B						G				R	W
12	W		B						G				R

Figuur 17

Nu komt iedere tandpasta in elk van de vier mogelijke tubes en elke proefpersoon krijgt één tube van elke kleur.

9.9.3 Staving van berichten

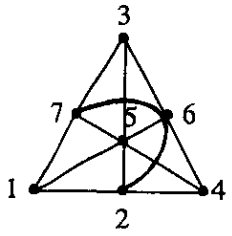
De matrix van Figuur 17 is ook geschikt voor authenticatie van berichten. Als een bericht verstuurd wordt van de ene instantie (Zender) naar de andere (Ontvanger), kan het gebeuren dat zo'n bericht onderschept wordt door een derde instantie (Saboteur) die het bericht vervangt door een ander bericht. Uiteraard wil Zender voorkomen dat Ontvanger zo'n vervangen bericht als authentiek beschouwt.
Stel eens dat Zender maar vier mogelijke berichten te versturen heeft naar Ontvanger. Laten we die berichten aanduiden met R, W, B en G. Zender spreekt een bepaalde rij van de matrix af met Ontvanger, zeg rij 8. In plaats van G, R, W of B te versturen, seint Zender het kolomnummer van het betreffende bericht in rij 8 aan Ontvanger. Ontvanger kan dan aan de hand van de matrix nagaan welk bericht bedoeld wordt.
De charme van deze methode is dat ook als de Saboteur de methode kent (maar niet het heimelijk afgesproken rijnummer), zijn kans om ongemerkt een ander bericht te substitueren maar 1 op 4 is.
Stel eens dat Zender G wil berichten. Zender doet dit door 4 te sturen. Saboteur weet na onderschepping van het bericht alleen maar dat het rijnummer 1, 3, 4 of 8 was. Als Saboteur alleen maar kan raden naar het rijnummer, dan is zijn kans om goed te raden (en dus te saboteren) 1 op 4. Als Saboteur fout raadt, bijvoorbeeld 4, zal hij door de mand vallen. Immers bij rijnummer 4 horen kolomnummers die niet bij rij 8 passen. Ontvanger zal dan weten dat het bericht niet door Zender verstuurd is, dat wil zeggen dat het bericht niet authentiek is, en dat de echtheid niet gestaafd is.

9.9.4 Write once memories

Een digitaal optisch geheugen (ook wel compact disc genoemd) is een schijf met een dunne reflecterende telluriumlaag erop. Hier worden al dan niet zeer kleine putjes in gebrand door een laser. Aanwezigheid van een putje codeert een 1, afwezigheid een 0. De plaatsen waar zo een teken 0 of 1 mag staan zijn van tevoren vastgelegd. De schijf wordt gelezen met behulp van een veel zwakkere laser, die het verschil in reflectievermogen meet. Het nadeel van zo'n geheugen (in vergelijking met een magnetisch geheugen) is het zogeheten *write once* karakter. Als ergens eenmaal een putje zit, dan blijft dat een putje.
Overigens, opslag van gegevens op papier heeft hetzelfde nadeel: een eenmaal aangebracht merkteken op papier is moeilijk te verwijderen als het met potlood is gemaakt, en tekens bestaande uit inkt of in de vorm van een gaatjespatroon zijn praktisch onmogelijk te verwijderen.
Als men een dergelijk geheugen wil gebruiken voor het opslaan van nieuwe gegevens, dan ligt het voor de hand om die nieuwe gegevens op een schoon deel bij te schrijven. De plaats waar oude, niet meer actuele gegevens staan lijkt onbruikbaar voor het opslaan van nieuwe gegevens. Toch lijkt dit maar zo, want we zullen zien dat we met de hulp van het Fano-vlak eenzelfde plek van het geheugen tot viermaal toe kunnen gebruiken. De methode die we zullen beschrijven levert daardoor een ruimtebesparing van ongeveer 40%, tegen een meerprijs van iets meer werk, met name bij het schrijven.
We nemen aan dat ons geheugen uitsluitend getallen 1 tot en met 7 bevat. Elk van de tekens in ons geheugen zou dus kunnen bestaan uit drie bits. Als een gegeven ververst moet worden, dan zouden we het nieuwe gegeven ergens op een blanco plaats kunnen schrijven. Na driemaal verversen van een gegeven van één teken hebben we dan al 12 plaatsen opgebruikt.
Bijvoorbeeld, een gegeven dat achtereenvolgens 6, 3, 4, 7 luidt, zal resulteren in een geheugenbezetting als volgt.

1e keer	2e keer	3e keer	4e keer
6	3	4	7
0 1 1	1 1 0	0 0 1	1 1 1

Merk op dat weliswaar de 4 van de 3e keer makkelijk in een 7 veranderd kan worden door twee putjes bij te branden, maar dat zo'n methode niet erg praktisch is. Bij realistische gegevensopslag zal een typisch gegeven al gauw uit een rij van 30 van die tekens bestaan, en een miljoen maal zoveel is ook niet ondenkbaar. Het gaat natuurlijk niet aan om in een rij van bij elkaar horende tekens sommige te veranderen, en de actuele waarde van andere ergens anders op te slaan.
De zuinige methode werkt als volgt. Voor onze tekens reserveren we zeven bits (in plaats van drie). We denken ons die zeven bits gepositioneerd op de punten van het Fano-vlak. (De nummers bij de punten van het Fano-vlak zijn hier allemaal één hoger dan in Figuur 11).



Figuur 18

Bij het eerste gebruik van deze zeven bits, branden we een putje op bit nummer i, als we i willen opbergen.
Bij het tweede en bij elk volgende gebruik doen we *niets* als het gegeven dat we willen opbergen er al staat. Als we bij het tweede gebruik een j willen opbergen op een plaats waar al een $i \neq j$ staat, brengen we een putje aan in het *derde* punt
Bijvoorbeeld, als in het Fano-vlak één putje gebrand is, zeg bij 4, dan betekent dat ook 4. Maar wanneer er twee putjes gebrand zijn, bijvoorbeeld op posities 6 en 7, dan betekent dat 2.
Bij het derde gebruik staan er al twee putjes en we willen een j opbergen die niet correspondeert met de lege plek op de lijn door de twee bestaande putjes. We branden dan een putje op positie j (als daar niet al iets stond), en we vullen het aantal putjes aan tot 4, en wel zó dat de drie ongelijk j samen een hele lijn vullen (die dan niet door j gaat). Ga na dat dit altijd kan.
De lezer wordt uitgenodigd zelf een regel voor het vierde gebruik te bedenken, dat wil zeggen zowel een methode voor het bepalen van de posities waar gaatjes bijgebrand moeten worden, als een regel om het opgeborgen teken terug te kunnen lezen. Het is nodig twee gevallen te onderscheiden.
Lezen met deze methode kan efficiënt gebeuren. Het beetje rekenwerk dat bij elke leesoperatie moet gebeuren is onbelangrijk. Schrijven is iets minder efficiënt, je moet namelijk eerst kijken wat er staat, voor je erover heen kunt schrijven. Verder is met deze methode de hoeveelheid actuele gegevens die tegelijk beschikbaar kan zijn ongeveer gehalveerd. Dat is ook niet erg belangrijk, want de capaciteit van dit type geheugen is enorm groot. Tegenover dit offer aan schrijfsnelheid en gelijktijdige beschikbaarheid staat een besparing van ongeveer 40% aan geheugenruimte. Dat is net zoveel als arme studenten vroeger bespaarden door kladpapier tweemaal te gebruiken: eenmaal met potlood, en daarna (met het papier omgedraaid) nog eens met een pen.

Opgaven

57. Voor een symmetrisch 2-(v,k,λ) design met even v geldt dat $k-\lambda$ een kwadraat is. Bewijs dit.

58. Laat een niet triviaal BD$(v,k;b,r,\lambda)$ gegeven zijn met puntenverzameling P en blokkenverzameling B. Laat voor elke $p \in P$

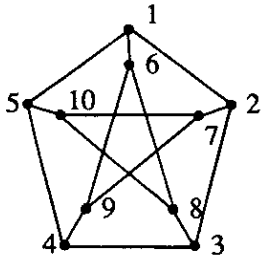
$$P' := \{B \in \mathcal{B} \mid P \in B\} \quad .$$

a) Bewijs dat bij verschillende P ook verschillende P' horen.
b) Geef nodige en voldoende voorwaarden opdat B en de verzameling der P' respectievelijk puntverzameling en blokkenverzameling van een block design zijn.

59. Een algebraïsch bewijs voor Stelling 9.4.1.
a) Laat A de incidentiematrix zijn van een symmetrisch 2-(v,k,λ) design. Bewijs dat A^{-1} bestaat.
b) Gebruik onderdeel a) en de relatie $JA = rJ$ om de vergelijking voor A^TA om te werken tot de vergelijking voor AA^T uit Stelling 9.4.1.

60. Geef de parameters b en r voor het derived design en het residual design.

61. Beschouw de volgende graaf (de zogeheten Petersen-graaf):



a) Op de hoekpunten van de Petersen-graaf maken we een design door als blokken zodanige viertallen $\{x,y,u,v\}$ te nemen, dat in de graaf x en y onderling verbonden zijn en evenzo u en v maar dat er verder tussen de punten van zo'n viertal geen andere verbindingen bestaan. Ga na dat zo een block design ontstaat, en wel een 2-(10,4,2) design. Bepaal de overige parameters van dit design.
b) Is dit een residual design van het design van 9.5.3?

62. Neem een willekeurig drietal x, y en z uit $GF(16) \setminus \{0\}$ met $x + y + z \neq 0$.
a) Ga na dat het zevental

$$\{x, y, z, x+y, y+z, z+x, x+y+z\}$$

met de blokken van het design van 9.5.6 een Fano-vlak vormt; dat wil zeggen dat bijvoorbeeld $\{x,y,x+y\}$ een blok vormen omdat de som van dit drietal 0 is.
b) Ga na dat elk tweetal $\{x,y\}$ in 3 van zulke vlakken ligt, en dat punten en vlakken zo een symmetrisch 2-(15,7,3) design vormen.

63. Construeer een 2-(13,4,1) design op de manier van 9.5.1 met behulp van $\mathbf{F}_{13}$.

64. Vervang alle nullen in de incidentiematrix van het design van 9.5.3 door -1. Bewijs dat zo een Hadamardmatrix van orde 16 ontstaat.

65. Het idee van 9.5.6 werkt niet met $\mathbf{Z}_{15}$. Waarom niet?

66. Block designs noemen we isomorf of equivalent, als hun incidentiematrices door omschikken van rijen of kolommen (of beide) in elkaar overgaan.
Toon aan dat er op isomorfie na precies één 2-(9,3,1) design bestaat.

67. Laat $\mathcal{B}$ een 2-(22,6,5) design zijn.
a) Laat zien dat elk punt in 21 blokken zit.
Veronderstel in de volgende twee onderdelen dat geen twee blokken elkaar in meer dan 2 punten snijden. b) Laat zien dat twee blokken elkaar in 0 of in 2 punten snijden. (Aanwijzing:

direct tellen of via $\sum i(i-2)a_i$).
c) Laat zien dat elk drietal punten in precies één blok zit.

68. a) Laat zien dat het aantal bijecties van $PG(2,2)$ op zichzelf die lijnen in lijnen overvoeren 168 bedraagt. Zulke bijecties heten *collineaties*.
(Tamelijk lastig. Aanwijzing: een gegeven drietal punten niet op een lijn gaat door een collineatie in een soortgelijk drietal over. Daaruit volgt dat het gevraagde aantal ten hoogste 168 is. Anderzijds induceert elke lineaire bijectie van $\mathbf{F}_2^3$ op zichzelf ook een collineatie, waaruit blijkt dat het gevraagde aantal ten minste 168 is.)
b) Hoeveel hiervan laten een gegeven punt op zijn plaats?

69. Toon aan dat de blokken van een 2-$(n^2, n, 1)$ design verdeeld kunnen worden in $n+1$ klassen van elk n blokken, zodanig dat elk tweetal blokken uit eenzelfde klasse disjunct is. (Aanwijzing: laat zien dat evenwijdigheid van blokken transitief is, als onder evenwijdig wordt verstaan disjunct of gelijk. Reflexiviteit en symmetrie van de relatie "evenwijdig met" zijn evident.)

70. a) Toon aan dat voor een projectief vlak van orde n elk residual design een affien vlak is.
b) Toon aan dat elk affien vlak van orde n een residual design is van een projectief vlak van orde n.

71. Laat $n \geq 3$ zijn en laat P een punt zijn in een projectief vlak van orde n, laat voorts $B_1, \ldots, B_s$ verschillende lijnen door P zijn en laat ten slotte $L_1, \ldots, L_{n^2}$ de n^2 lijnen voorstellen die niet door P gaan. Men denkt zich op elk der lijnen $B_1, \ldots, B_s$ de punten ongelijk aan P genummerd van 1 tot en met n. Laat tenslotte een $s \times n^2$ matrix (a_{ij}) gedefinieerd zijn door $a_{ij} :=$ het nummer van het snijpunt van B_i met L_j.
Bewijs dat (a_{ij}) een $OA(n,s)$ is.

72. Laat α en p zijn als in het bewijs van de Stelling van Singer. Laat B_0 bestaan uit alle t met $0 \leq t \leq p^2+p$ en met $a^t \in L(0,0,1)$. Bewijs dat de verschillen (modulo p^2+p+1) van de elementen van B_0 allemaal verschillend zijn.

73. Bepaal zes elementen $x_1, \ldots, x_6$ van $\mathbf{F}_{31}$ zodanig dat alle verschillen $x_i - x_j$, $i \neq j$ verschillend zijn. (Aanwijzing: $31 = 5^2 + 5 + 1$).

74. Laat zien dat er geen 7 elementen $x_1, \ldots, x_7$ van $\mathbf{F}_{43}$ zijn, zodanig dat alle verschillen $x_i - x_j$, $i \neq j$ verschillend zijn. (Aanwijzing: het feit dat er geen projectief vlak van orde 6 bestaat mag bekend worden verondersteld).

75. Construeer een 2-(13,3,1) design.

76. Laat $v = 4t+1 = q$ een macht zijn van een priemgetal. Ga precies als in Stelling 9.7.1 te werk, maar nu met $B_{0,0} = \{1, \alpha^t, \alpha^{2t}, \alpha^{3t}\}$, met α primitief element van $GF(q)$. Construeer zo een 2-$(v,4,3)$ design.

77. Construeer een STS(27) met behulp van $\mathbf{F}_3^3$.

78. Hoeveel blokken zijn er van elke soort in het bewijs van Stelling 9.8.6?

79. Construeer met behulp van een STS(v) een STS($4v+3$).

80. Laat zien dat het idee van Stelling 9.8.6 ook werkt als we in plaats van een deelsysteem van S_1 af te zonderen, een enkel punt apart nemen, bijvoorbeeld v_1. Maak hiermee een STS($3v-2$) uit een STS(v).

81. Maak een STS(49) op twee manieren
a) Gebruik Stelling 9.8.4

b) Ga uit van een affien vlak van de orde 7. Zorg dat elke lijn een deelsysteem wordt. Het resultaat van onderdeel b) is dat er vaak veel vrijheid in de constructie mogelijk is.

82. Zie 9.9.4. Bedenk de regel voor het vierde gebruik.

Register van Trefwoorden

Colofon

Deze syllabus werd gezet uit
Times 11 op 13,
met behulp van een
QMS PostScript-800 Laserprinter,
bestuurd door het programma
troff met ms, tbl, eqn
en additionele programma's,
op basis van op aanwijzing van de auteur
gepreparcerde bestanden.