

Universiteit Gent

Academiejaar 2001 — 2002

Discrete Wiskunde

1ste kandidatuur Informatica

Collegenota's

Prof. Dr. Frank De Clerck

Herhalingsoefeningen

- Bepaal het quotiënt en de rest van de deling van $a(x)$ door $b(x)$ over het veld \mathbb{F} .
 - $\mathbb{F} = \mathbb{F}_5$; $a(x) = 3x^4 + 4x^3 - x^2 + 1$; $b(x) = 2x^2 + x + 1$
 - $\mathbb{F} = \mathbb{F}_8$ met $\alpha^3 + \alpha + 1 = 0$; $a(x) = x^4 + \alpha^2x^3 + \alpha^6x^2 + \alpha x + \alpha^5$; $b(x) = \alpha^4x^2 + \alpha^3x + 1$
 - $\mathbb{F} = \mathbb{F}_2$; $a(x) = x^3 + x^2 + 1$; $b(x) = x^2 + x + 1$.
 - $\mathbb{F} = \mathbb{F}_5$; $a(x) = x^2 + 2x + 3$; $b(x) = x^5 + x^4 + 2x^3 + x^2 + 4x + 2$.
 - zelfde als voor (d), maar nu over \mathbb{F}_7 en over \mathbb{F}_{73} .
- Bepaal de inverse veelterm in $\mathbb{F}_3[x]$ van $2x^4 + 2$ modulo $x^5 + 2$.
- Bereken de som en het product in $\mathbb{Z}[x]$ van $3x + 4$ en $5x - 2$ modulo $x^2 - 7$.
 - Beschouw het veld van de rationale getallen \mathbb{Q} . Bereken de som en het product van $3x/2$ en $-x^2/2$ modulo $x^2 + 2$ in $\mathbb{Q}[x]$.
- Waarom is $x^2 + 3$ irreduciebel over \mathbb{F}_5 ?
 - Zoek de inverse veelterm van $x + 1$ modulo $x^2 + 3$ in $\mathbb{F}_5[x]$.
- Welk irreduciebel polynoom met coëfficiënten in \mathbb{F}_2 heeft precies de elementen van orde 3 van \mathbb{F}_{16} als nulpunten?
 - Welk irreduciebel polynoom met coëfficiënten in \mathbb{F}_2 heeft de elementen van orde 5 van \mathbb{F}_{16} als nulpunten?
- Welk polynoom, dat een deler is van $x^{15} - 1$, heeft precies alle primitieve elementen van \mathbb{F}_{16} als nulpunten?
- Bewijs dat alle elementen van $\mathbb{F}_{2^{11}}$ derdemachten zijn.
- Hoeveel koppels $(a, b) \in \mathbb{F}_{16} \times \mathbb{F}_{16}$ zijn er die voldoen aan $a^2 + b^3 = 1$?
- Los de volgende kwadratische vergelijkingen op over \mathbb{F}_8 waarbij $t^3 + t + 1 = 0$.
 - $tx^2 + (t^2 + t + 1)x + t^2 + t = 0$

(b) $(1 + t + t^2)x^2 + t^2x + 1 + t = 0$

10. Beschouw de kwadratische vergelijking

$$x^2 + 8x + 3 \equiv 0 \pmod{p}.$$

waarbij p een priemgetal is. Bewijs dat deze vergelijking een gehele oplossing x heeft als p modulo 13 congruent is met één der zes getallen $\pm 1, \pm 3, \pm 4$ en uiteraard priem is.

11. (a) Bepaal het kleinste getal $x \in \mathbb{N}$ met $x \equiv 15 \pmod{59}$ en $x \equiv 52 \pmod{61}$.

(b) Bewijs dat er gehele getallen y en z bestaan die voldoen aan

$$y^2 \equiv 15 \pmod{59} \text{ en } z^2 \equiv 52 \pmod{61}.$$

12. Laat $p \geq 5$ een priemgetal zijn. Bewijs dat de vergelijking

$$x^2 \equiv 6 \pmod{p}$$

een oplossing heeft dan en slechts dan als $p \equiv \pm 1 \pmod{24}$ of $p \equiv \pm 5 \pmod{24}$.

13. Bewijs de elfproef. Een getal is deelbaar door 11 dan en slechts dan als de som van de cijfers op de even posities een elfvoud verschilt van de som van de cijfers op de oneven posities.

14. In een vereenvoudigd model van de werkelijkheid heeft ieder jaar 365 dagen, en is het om de 29 dagen (precies) volle maan. Gegeven is dat er een volle maan viel op donderdag 17 augustus 1989. In welk jaar zal er voor het eerst weer volle maan zijn op een zondag 27 augustus?

15. Bewijs dat elke abelse groep van de orde 15 cyclisch is.

16. Stel dat een eindige groep G en een priemgetal p gegeven zijn. Stel dat G precies m deelgroepen heeft van de orde p . Bewijs dat G precies $m(p - 1)$ elementen van de orde p bezit.

17. Gegeven is de cyclische groep $C_8 = \langle a \rangle$. Bewijs dat de volgende afbeeldingen α en β morfismen van C_8 zijn. Bepaal telkens de kern.

(a) $\alpha : a \mapsto a^4$.

(b) $\beta : a \mapsto a^5$.

18. Bewijs dat de volgende producten fout zijn (zonder uit te rekenen).

(a) $5783 \times 40162 = 233256846$

(b) $9787 \times 1258 = 12342046$

(c) $8901 \times 5743 = 52128443$.

19. Los het volgende stelsel op in \mathbb{Z}_7 .

$$\begin{cases} x + 2y & = & 4 \\ 4x + 3y & = & 4 \end{cases}$$

Is er een oplossing in \mathbb{Z}_5 ?

20. Bereken $7^{93} \pmod{10}$.

21. Vind de monische ggd van de polynomen $a(x)$ en $b(x)$ in $\mathbb{F}[x]$ en schrijf het eindresultaat in de gedaante $\lambda(x)a(x) + \mu(x)b(x)$ over $\mathbb{F}[x]$.

(a) $\mathbb{F} = \mathbb{F}_3$; $a(x) = x^3 + x^2 + x + 1$ en $b(x) = x^2 + 2$.

(b) $\mathbb{F} = \mathbb{F}_5$; $a(x) = x^4 + 2x^3 + x^2 + 4x + 2$ en $b(x) = x^2 + 3x + 1$.

(c) $\mathbb{F} = \mathbb{F}_2$; $a(x) = x^4 + 1$ en $b(x) = x^2 + 1$.

(d) $\mathbb{F} = \mathbb{F}_2$; $a(x) = x^5 + 1$ en $b(x) = x^2 + 1$.

(e) $\mathbb{F} = \mathbb{F}_2$; $a(x) = x^9 + 1$ en $b(x) = x^6 + 1$.

22. Factoriseer volgende veeltermen in irreduciebele veeltermen in $\mathbb{F}_5[x]$.

(a) $x^4 + 4$.

(b) $x^4 + 3x^3 + 2x + 4$.

23. Toon aan dat elke kwadratische polynoom in $\mathbb{F}_p[x]$ geschreven kan worden als het product van 2 lineaire polynomen met coëfficiënten in \mathbb{F}_{p^2} .

24. Bewijs dat m een priemgetal is dan en slechts dan als m een deler is van $(m - 1)! + 1$.

Inhoudsopgave

1	Getallen tellen	1
1.1	De gehele getallen	1
1.1.1	Inleiding	1
1.1.2	De optelling en de vermenigvuldiging	3
1.1.3	De ordening van de gehele getallen	4
1.1.4	Het axioma van de goede ordening	4
1.2	Recursieve definities	6
1.3	Het inductieprincipe	7
1.4	Het ladenprincipe van Dirichlet	10
1.5	Eindige en oneindige verzamelingen	11
1.5.1	Definities	11
1.5.2	Opmerking	12
1.5.3	Voorbeelden	12
1.5.4	Kardinaalgetallen	14
1.6	Het vereenvoudigd somprincipe	15
1.7	Het productprincipe	15
1.8	Het eenvoudig inclusie–exclusie principe	17
1.9	Combinatieleer	17
1.9.1	Variaties	17
1.9.2	Permutaties	18
1.9.3	Combinaties	19
1.9.4	Herhalingsvariaties	21
1.9.5	Herhalingscombinaties	22
1.10	Toepassingen op combinatieleer	23
1.10.1	De binomiale kansverdeling	23
1.10.2	Het aantal deelverzamelingen van een verzameling	24
1.10.3	Het binomium van Newton	25
1.10.4	Het (veralgemeend) inclusie–exclusie principe	26
1.10.5	Permutaties zonder fixelementen: wanorde	27
1.11	De Stirling getallen	28
1.12	De multinomiaalgetallen	30

2	Voortbrengende functies	32
2.1	Formele machtreeksen	32
2.1.1	Inleiding	32
2.1.2	Som en product van formele machtreeksen	33
2.1.3	Een andere kijk op het binomium van Newton	35
2.2	Gewone voortbrengende functies	36
2.2.1	Definities	36
2.2.2	De voortbrengende functie voor de herhalingscombinaties	40
2.2.3	Het aantal partities van een natuurlijk getal	43
2.3	Exponentieel voortbrengende functies	44
2.4	De differentiaaloperator	47
2.5	Constructie van voortbrengende functies uit andere voortbrengende functies	48
3	Recurrente betrekkingen	52
3.1	Definitie	52
3.2	Lineaire recurrente betrekkingen met constante coëfficiënten	53
3.2.1	Definitie	53
3.2.2	Homogene lineaire recurrente betrekkingen met constante coëfficiënten	54
3.2.3	Niet-homogene lineaire recurrente betrekkingen met constante coëfficiënten	60
3.3	Recurrente betrekkingen en voortbrengende functies	64
3.4	Zuinig en onzuinig sorteren	66
3.5	Differentierijen	67
4	Getaltheorie	69
4.1	Basisbegrippen	69
4.1.1	Deelbaarheid	69
4.1.2	Priemgetallen	71
4.1.3	Ontbinden in priemfactoren	71
4.2	Grootste gemene deler en kleinste gemeen veelvoud	72
4.3	De Euler functie	77
4.4	De Möbius functie	79
4.4.1	Definitie	79
4.4.2	Een eerste eigenschap	79
4.4.3	De Möbius inversieformule	80
5	Modulo rekenen	82
5.1	Congruenties	82
5.1.1	Definitie	82
5.2	Optelling en vermenigvuldiging in \mathbb{Z}_m	84
5.3	Inverteerbare elementen in \mathbb{Z}_m	85

5.3.1	Definitie	85
5.4	Lineaire congruenties	87
5.4.1	Definities	87
5.5	De stelling van Wilson en toepassingen	90
5.6	Stelsels lineaire congruenties	91
5.7	Primitieve wortels	93
5.7.1	Definitie	93
5.7.2	Definitie	95
5.8	Kwadratische congruenties	96
5.8.1	Definities	96
5.8.2	Definities	97
5.8.3	De kwadratische resten modulo een oneven priemgetal	97
5.8.4	Het Legendre symbool	99
6	Inleiding tot de groepentheorie	103
6.1	Definities	103
6.2	Enkele eenvoudige eigenschappen	105
6.3	Latijnse vierkanten	105
6.4	Groepmorfismen	106
6.5	Deelgroepen	107
6.6	Nevenklassen van een deelgroep	108
6.7	Cyclische groepen	109
6.8	Het direct product van groepen	113
6.9	Elementair abelse groepen	114
6.10	Permutatiegroepen	114
6.10.1	Definities en notaties	114
6.10.2	Even en oneven permutaties	116
7	Ringen, lichamen en velden	120
7.1	Ringen	120
7.1.1	Definities	120
7.1.2	Inverteerbare elementen van een ring	122
7.2	Lichamen en velden	123
7.3	Veeltermringen	124
7.3.1	Definitie	124
7.3.2	Het delingsalgoritme voor veeltermen	125
7.3.3	Het algoritme van Euclides voor veeltermen	127
7.3.4	Ontbinden in factoren	128
7.4	Eindige velden	131
7.4.1	Inleiding	131
7.4.2	Constructie van eindige velden	134
7.4.3	Voorbeelden van eindige velden	135
7.4.4	Enkele belangrijke stellingen	138
7.4.5	Kwadratische vergelijkingen	140

8	Inleiding tot de grafentheorie	148
8.1	Algemene begrippen	148
8.1.1	Een eerste reeks definities	148
8.1.2	Voorstelling van grafen	149
8.1.3	Isomorfisme van grafen	150
8.1.4	Nog enkele definities	151
8.2	Eulerpaden en Euleriaanse grafen	153
8.2.1	Definitie	154
8.2.2	Algoritme van Fleury	155
8.3	Hamiltoniaanse grafen	158
8.3.1	Definitie	158
8.4	Het handelsreizigersprobleem	161
8.5	Systematisch zoeken in een graaf	164
8.5.1	DFS- en BFS-zoekmethodes	164
8.5.2	De uitwisselingsstelling	166
8.5.3	Het verbindingsprobleem in een gewogen graaf	167
8.5.4	Het probleem van het kortste gewogen pad	171
8.6	Koppelingen	174
8.6.1	Definitie	174
8.6.2	Maximumkoppelingen	175
8.7	Toewijzingen	177
8.7.1	Het lesroosterprobleem	178
8.7.2	Maximumtoewijzingen	181
8.7.3	De stelling van König-Egerváry	183