Universiteit Gent

Academiejaar 2001 — 2002

Discrete Wiskunde

1ste kandidatuur Informatica

Collegenota's

Prof. Dr. Frank De Clerck

Herhalingsoefeningen

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

(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 $C_8 =< a >$. 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