Relaties en Structuren
Examenvragen theorie

Over het theorie-examen

Het theorie-examen *Relaties en structuren* is mondeling, met schriftelijke voorbereiding. Het zal bestaan uit vier hoofdvragen, komende uit de lijst hieronder. Op deze vragen is het antwoord terug te vinden in de cursusnota's van *Relaties en structuren*. Nogmaals dient eraan herinnerd te worden dat het van buiten leren van bewijzen zonder deze te begrijpen, volstrekt zinloos is.

Tijdens het examen zal gepeild worden of alles begrepen is en hierbij zal ook naar andere delen van de cursus worden overgestapt. Deze opgelijste theorievragen vormen dus **niet** de oplijsting van te kennen leerstof. Deze te kennen leerstof is in een afzonderlijke pagina opgenomen en geeft van verschillende syllabusonderdelen aan of en hoe die moeten gekend zijn.

1. Geef een definitie van het axioma van de goede ordening in $\mathbb{N}$ en leg uit dat als gevolg van dit axioma het inductieprincipe in $\mathbb{N}$ gebruikt mag worden.

2. Geef de definitie van een aftelbare verzameling. Bewijs dat de verzameling $\mathbb{Q}$ aftelbaar is en dat $\mathbb{R}$ niet aftelbaar is.

3. Bewijs dat er voor elke twee getallen $a \in \mathbb{Z} \setminus \{0\}$ en $b \in \mathbb{Z}$ unieke gehele getallen $q \in \mathbb{Z}$ en $r \in \mathbb{N}[0, |a| - 1]$ bestaan waarvoor $b = a \cdot q + r$.

4. Leg het algoritme van Euclides uit voor het berekenen van de grootste gemene deler d van twee gehele getallen a en b. Bewijs dat er steeds gehele getallen m en n kunnen gevonden worden zodanig dat $a \cdot m + b \cdot n = d$.

5. Wat is een priemgetal? Bewijs dat de verzameling van de priemgetallen een oneindige verzameling is. Bewijs dat elk getal $n \in \mathbb{N} \setminus \{0, 1\}$ kan geschreven worden als een product van priemfactoren en dat dit kan op een unieke manier op de orde van de factoren na.

6. Bewijs dat indien een priemgetal p een product van gehele getallen deelt, het ten minste één van deze gehele getallen deelt.

7. Geef de definitie van de eulerfunctie φ en leg uit hoe de formule voor $\varphi(n)$ uit de multiplicativiteit van φ volgt. Bewijs dat

$$\sum_{d|n} \varphi(d) = n.$$

8. Geef de definitie van inverteerbaar element in $\mathbb{Z}_m$. Formuleer en bewijs de nodige en voldoende voorwaarde opdat een element in $\mathbb{Z}_m$ inverteerbaar zou zijn.

9. Bewijs de stelling van Euler: als $\text{ggd}(y, m) = 1$ dan geldt

$$y^{\varphi(m)} \equiv 1 \pmod{m}.$$

   Bewijs hieruit de kleine stelling van Fermat.

10. Bespreek en bewijs het aantal oplossingen van een lineaire congruentie $ax \equiv b \pmod{m}$.

11. Bewijs de stelling van Wilson: Als p een priemgetal is, dan is $(p-1)! \equiv -1 \pmod{p}$.

12. Veronderstel dat p een oneven priemgetal is. Bewijs dan dat -1 een kwadraat is modulo p dan en slechts dan als $p \equiv 1 \pmod{4}$.

13. Formuleer en bewijs de Chinese reststelling. Leg het algoritme uit voor het oplossen van een stelsel lineaire congruenties. Leg uit waarom φ multiplicatief is als gevolg van de Chinese reststelling.

14. Veronderstel dat a en m twee natuurlijke getallen zijn die onderling ondeelbaar zijn. Veronderstel dat a de orde t bezit modulo m en bewijs dan de nodige en voldoende voorwaarde opdat a^k eveneens de orde t modulo m zou hebben.

15. Bespreek het aantal oplossingen van een kwadratische congruentie $x^2 \equiv a \pmod{p}$, met p een oneven priemgetal. Formuleer en bewijs het criterium van Euler voor kwadratische congruenties.

16. Formuleer en bewijs de stelling van Lagrange voor de orde van een deelgroep van een eindige groep.

17. Geef de definitie van een cyclische groep en bewijs dat elke twee cyclische groepen van dezelfde orde isomorf zijn. Zoek alle deelgroepen van de groep S_3.

18. Geef een definitie van even en oneven permutatie. Bewijs dat deze definitie onafhankelijk is van de ontbinding in transposities.

19. Wat is een veeltermring in één veranderlijke over een veld? Bewijs: als $a(x), b(x) \in F[x]$, dan bestaan er unieke $q(x), r(x) \in F[x]$ zodanig dat $a(x) = b(x)q(x) + r(x)$, met de graad van $r(x)$ kleiner dan de graad van $b(x)$ of met $r(x) = 0$.

20. Leg het algoritme van Euclides uit om de grootste gemene deler in de veeltermring $F[x]$, F een veld, te bepalen.

21. Leg uit hoe een eindig veld $\mathbb{F}_q$ geconstrueerd wordt, aan de hand van een voorbeeld, met $q = \ldots$ en als primitief polynoom $\ldots$. Leg aan de hand van deze veldconstructie het principe van de Zech-log-tabel uit. (Orde en polynoom zullen gegeven worden)

22. Bewijs dat een eindig veld steeds orde $q = p^h$ heeft, voor een p priem en $h \geq 1$.

23. Onderzoek het aantal kwadraten in een eindig veld.

24. Wanneer is -1 een kwadraat in $\mathbb{F}_q$? Bewijs.

25. Geef de definitie van variaties met en zonder herhaling. Bewijs de formules voor het aantal variaties met en zonder herhaling. Doe hetzelfde voor permutaties.

26. Geef de definitie van combinaties met en zonder herhaling. Bewijs de formules voor het aantal combinaties met en zonder herhaling. Stel de driehoek van Pascal op en bewijs de gebruikte eigenschappen.

27. Formuleer en bewijs het veralgemeende inclusie-exclusieprincipe. Leg uit hoe je met dit principe $\varphi(30)$ kan berekenen door enkel de definitie van Euler's φ te gebruiken.

28. Geef de definitie van het Stirlinggetal $S(n, k)$ van de tweede soort. Bewijs dat deze getallen recursief kunnen gedefinieerd worden door $S(n, k) = S(n - 1, k - 1) + kS(n - 1, k)$, $(2 \leq k \leq n - 1)$, $S(n, 1) = S(n, n) = 1$.

29. Geef de definitie van een multinomiaalgetal. Bewijs de formule voor een multinomiaalgetal in termen van permutaties. Bewijs de multinomiaalstelling.

30. Geef de definitie van de möbiusfunctie μ en bewijs de möbiusinversieformule.

31. Bewijs dat de multiplicatieve groep van een eindig veld cyclisch is.

Relaties en Structuren
Leerstofafbakening

De te kennen leerstof valt in principe samen met de inhoud van de syllabus *Relaties en Structuren*, academiejaar 2012-2013, behoudens de uitzonderingen die hieronder worden opgesomd. De leidraad op pagina (iii) van de cursusnota's legt het onderscheid uit tussen essentiële kennis en bijkomende informatie.

1 Elementen van de verzamelingenleer

De paragrafen 1.1, en 1.2 worden als parate kennis beschouwd. Er worden geen vragen gesteld die uitsluitend over elementen in deze paragrafen staan.

3 Getaltheorie

Stelling 3.15: een bewijs zal niet op het theorie-examen gevraagd worden.

Lemma 3.25: kennen, maar niet het bewijs zoals in de cursus. Wel kunnen uitleggen waarom deze formule volgt uit de Chinese reststelling.

5 Inleiding tot de groepentheorie

Stelling 5.41: een alternatief bewijs werd gegeven en kan gevonden worden op Minerva. Indien gevraagd, worden beide bewijzen als correct gerekend.

6 Ringen, lichamen en velden

Stelling 6.9: niet kennen
Gevolg 6.10: niet kennen
Definitie 6.12: niet kennen
Stelling 6.13: niet kennen
Constructie van $\mathbb{R}$ door sneden van Dedekind (p. 109 – 110): niet kennen
Stelling 6.24: bewijs niet kennen.
Stelling 6.27: niet kennen

7 Combinatoriek

Paragraaf 7.4.5. werd niet gegeven en is niet te kennen.

8 Inleiding tot de grafentheorie

Het ganse hoofdstuk werd niet gegeven en is volledig niet te kennen.