Examenvragen Theorie
over
de cursus "Relaties en Structuren"

Voorafgaande opmerkingen

De hierna volgende vragen over de cursus zijn vragen die rechtstreeks terug te vinden zijn in de cursusnota's. Ik wil er nogmaals aan herinneren dat van buiten leren van de antwoorden zonder deze te begrijpen, volledig zinloos is. Tijdens het examen zal gepeild worden of alles begrepen is en het is hierbij niet uitgesloten dat naar andere delen van de cursus wordt overgestapt.
Zoals hieronder mag blijken, worden geen vragen gesteld over basisbegrippen uit de verzamelingsleer (1.1 en 1.2 uit hoofdstuk 1) en uit het volledige hoofdstuk 2. Het is echter duidelijk dat deze items voor het bijwerken van de parate kennis en voor het begrijpen van de volgende hoofdstukken best eens worden doorgenomen.

1. Geef een definitie van het axioma van de goede ordening 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. Geef de definitie van variaties met en zonder herhaling. Bewijs de formules voor het aantal variaties met en zonder herhaling.

4. 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.

5. Geef de definitie van een wanorde van $\mathbb{N}[1, n]$. Bewijs dat het aantal wanordes d_n recursief kan gedefinieerd worden door $d_n = (n-1)(d_{n-1} + d_{n-2}),\ n > 2,\ d_1 = 0,\ d_2 = 1$.

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

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

8. Bewijs dat er voor elke 2 getallen $a \in \mathbb{N}_0$ en $b \in \mathbb{Z}$ unieke gehele getallen q en $r \in \mathbb{N}[0, a-1]$ bestaan waarvoor $b = a \cdot q + r$. Bewijs dat elk natuurlijk getal op een unieke manier ontwikkeld kan worden in een willekeurig gekozen basis $t \in \mathbb{N} \setminus \{0, 1\}$.

9. 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 op een unieke manier kan op de orde van de factoren na.

10. Bewijs het algoritme van Euclides voor het berekenen van de grootste gemene deler d van 2 gehele getallen a en b. Bewijs dat er steeds gehele getallen m en n kunnen gevonden worden zodanig dat $a \cdot m + b \cdot n = d$.

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

12. Geef de definitie van de Euler functie Φ en bewijs de formule voor $\Phi(n)$. Bewijs dat
$$\sum_{d|n} \Phi(d) = n.$$

13. Geef de definitie van de Möbius functie μ en bewijs de Möbius inversieformule.

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

15. Bewijs de stelling van Euler: als $\text{ggd}(y, m) = 1$ dan geldt
$$y^{\Phi(m)} \equiv 1 \pmod{m}.$$
Bewijs hieruit de stelling van Fermat voor congruenties.

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

17. Bewijs de stelling van Wilson: $(p-1)! \equiv -1 \pmod{p}$ voor een willekeurig priemgetal p.

18. Veronderstel dat p een oneven priemgetal is, bewijs dan dat er een $a \in \mathbb{Z}_p$ bestaat waarvoor $a^2 \equiv -1 \pmod{p}$ dan en slechts dan als $p \equiv 1 \pmod{4}$.

19. Formuleer en bewijs de Chinese reststelling. Leg het algoritme uit voor het oplossen van een stelsel van lineaire congruenties.

20. Veronderstel dat a en m 2 natuurlijke getallen zijn die onderling priem zijn. Veronderstel a de orde t bezit modulo m, bewijs de nodige en voldoende voorwaarde opdat a^k eveneens de orde t zou bezitten.

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

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

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

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

25. Geef de constructie van een eindig veld, pas dit toe op ....

26. Leg het principe van de Zech log tabel uit.

27. Onderzoek het aantal kwadraten van een eindig veld.

28. Wanneer is -1 een kwadraat in $\mathbb{F}_q$ (+ bewijs).