Technische Universiteit Delft
Faculteit Elektrotechniek, Wiskunde en Informatica
Mekelweg 4, Delft

Tentamen Toegepaste Algebra, TW2560
vrijdag 21 april 2017, 13:30-16:30 uur.

Naam: Cijfer :

Studienummer:

Dit werk bestaat uit twee delen: kort-antwoord-vragen en open vragen. Bij de open vragen dient elk antwoord te worden beargumenteerd. Er mogen geen hulpmiddelen als mobiele telefoons, laptops, formulebladen en dergelijke gebruikt worden. Alleen een eenvoudige niet-programmeerbare, niet-grafische rekenmachine (de TI-30 en de Casio FX-82, en de verschillende varianten van deze machines) is toegestaan. Het cijfer wordt bepaald door bij het aantal behaalde punten 5 op te tellen en vervolgens te delen door 5.

deel kort antwoord vragen

(2) **K1.** (a) Gegeven is dat C een Hammingcode is van dimensie 10 over F_3. Dan geldt

$n =$ $|C| =$ $d =$

(2) (b) Geef een Parity-Check matrix van een extended Ham$(2, 3)$ code.

Geef vanwege de ruimte de getransponeerde

(2) **K2.** (a) Bepaal de kleinste q waarvoor geldt dat het lichaam F_q een element van multiplicatieve orde 9 bevat.

(2) (b) Bepaal de kleinste q waarvoor geldt dat het lichaam F_q van karakteristiek 2 een element van multiplicatieve orde 9 bevat.

K3. Zij β een primitief element van F_{125}.

(1) (a) Wat is het karakteristiek van F_{125}?

(2) (b) Wat is de multiplicatieve orde van β?

(2) (c) Wat is de graad van het minimaalpolynoom van β over F_5?

(2) (d) Wat is de graad van het minimaalpolynoom van β^{12} over F_5?

K4. C is een Reed-Solomon code met parameters $q = 256$ en $\delta = 13$.

(2) (a) Wat is de dimensie k van C?

(2) (b) Hoe lang mag een burst zijn opdat deze met zekerheid goed verbeterd wordt?

EINDE KORT-ANTWOORD-VRAGEN

TW2560, vrijdag 21 april 2017, open vragen

1. (2) (a) Bestaat er een code $C \subset F_2^8$ die uit zeven codewoorden bestaat en een minimum afstand 8 heeft?

(3) (b) Gegeven is een lineaire $[n = 7, k = 3, d = 2]$ code over F_2. De code C' ontstaat uit C door van elk codewoord het laatste bit te verwijderen. Geef de mogelijkheden voor de parameters n', k' en d' van C' en laat voor elke mogelijkheid met een voorbeeld zien dat zo'n code ook echt bestaat.

2. (3) Hoeveel cyclische codes van lengte 24 zijn er over F_3?

3. Zij C de binaire cyclische code van lengte 9 met generatorpolynoom $g(x) = m_1(x)m_\alpha(x)$. Hierbij is α een primitieve 9^{e} eenheidswortel, m_1 het minimaalpolynoom van 1 en m_α het minimaalpolynoom van α.

(3) (a) Bepaal de dimensie k van C.

(2) (b) Laat zien dat C een BCH-code is met $\delta = 6$.
AANWIJZING: Dit lukt niet als narrow sense BCH code!!

4. Een bepaald communicatienetwerk vereist dat authenticatie van berichten is gewaarborgd. Daarom wordt RSA gebruikt.
Veronderstel dat Alice een of ander data bestand M naar Bob wil sturen (bijvoorbeeld de sleutel van een symmetrische cryptosysteem). Ze genereert als volgt een cijfertext

$$C_1 = E_{K_{publB}}(D_{K_{privA}}(M||A)).$$

Hierbij zijn K_{publB} en K_{privA} respectievelijk de publieke sleutel van Bob en de geheime sleutel van Alice. A is persoonlijke informatie van Alice (bijvoorbeeld naam, adres enzovoorts) die wordt toegevoegd aan M, wat het bericht oplevert dat genoteerd wordt met $M||A$. Uiteraard zijn M en A hierbij omgezet naar getalswaarden.

(2) (a) Leg uit waarom de persoonlijke informatie A aan M wordt toegevoegd. En weet Bob zeker dat het bericht van Alice komt?

Alice gebruikt de priemgetallen $p = 2$ en $q = 11$ om haar publieke modulus te bepalen. Haar publieke exponent is $e = 7$. Uiteraard heeft Bob zijn eigen p, q, and e.

(1) (b) Stel dat Alice en Bob toevallig dezelfde priemgetallen p en q hebben geselecteerd, maar dat dat niet weten van elkaar. Heeft dat dan effect op de veiligheid van het systeem? Leg uit!

Neem nu aan dat Bob $p = 5$ en $q = 13$ selecteert en dat zijn geheime sleutel gelijk is aan $d = 29$.

(3) (c) Bepaal de publieke sleutel van Bob en de geheime sleutel van Alice.

(2) (d) Bepaal C_1 als $M = 1$ en $A = 7$ (dus $M||A = 17$).

(1) (e) Wat moet Bob doen om het bericht te ontcijferen en te verifiëren?

5. Zij n een geheel getal dat geen Carmichael-getal is en ook geen priemgetal.
Bij de behandeling van de priemtest van Fermat heb ik (de docent van dit mooie vak) verteld dat in dat geval tenminste de helft van alle $0 < a < n$ de eigenschap heeft dat $a^{n-1} \neq 1 \pmod{n}$. In deze opgave laten we dat dat inderdaad waar is. We definiëren $A = \{a \in \mathbb{Z} \mid 0 < a < n\}$.

(1) (a) Waarom is er een $a_0 \in \mathbb{Z}/n\mathbb{Z}^*$ zo dat $a_0^{n-1} \neq 1 \pmod{n}$?

Laat $S = \{s \in A \mid s^{n-1} = 1 \pmod{n}\}$.

(2) (b) Toon aan: als $s \in S$ dan $a_0 s \pmod{n} \notin S$.

(2) (c) Toon aan: het aantal elementen van $A \setminus S = \{a \in A \mid a^{n-1} \neq 1 \pmod{n}\}$ is tenminste even veel als $|S|$.

ZIE VOLGENDE BLADZIJDE