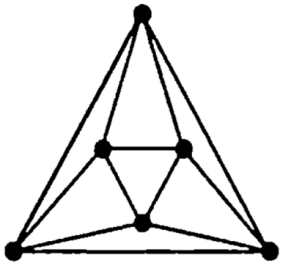
Examen Discrete Wiskunde 22 januari 2018

Het percentageteken voor elke vraag wijst op de relatieve score van die vraag

1. 10% Gebruik de Baby-step, Giant-step techniek om de index van 12 ten opzichte van de primitieve wortel $\omega = 3$ in $(\mathbb{Z}_{46049}, \cdot)$ te berekenen. Gebruik hierbij giant-steps van 200 baby-steps groot. Vermeld ook het aantal giant-steps en de extra baby-steps die nodig zijn. Een oplossing louter gebaseerd op het berekenen van de opeenvolgende machten van ω, wordt als waardeloos beschouwd.

2. 5% Van welke graaf **G** is de hieronder getekende graaf de lijngraaf. Maak een figuur van de graaf **G** en geef de staandaardidentificatie (naam en symbool).



3. 20% Beschouw het veld F_{16} en de elliptische kromme E: $y^2 + xy = x^3 + ③x^2 + ⑤$ over dit veld. De irreducibele veelterm is $\mu = x^4 + x + 1$ en de primitieve wortel $\omega = x$. Gebruik de onderstaande groepstabel:

	⊕	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	∞
1	0	∞	4	8	14	1	10	13	9	2	7	5	12	11	6	3	0
x	1	4	∞	5	9	0	2	11	14	10	3	8	6	13	12	7	1
x^2	2	8	5	∞	6	10	1	3	12	0	11	4	9	7	14	13	2
x^3	3	14	9	6	∞	7	11	2	4	13	1	12	5	10	8	0	3
x+1	4	1	0	10	7	∞	8	12	3	5	14	2	13	6	11	9	4
x^2+x	5	10	2	1	11	8	∞	9	13	4	6	0	3	14	7	12	5
x^3+x^2	6	13	11	3	2	12	9	∞	10	14	5	7	1	4	0	8	6
x^3+x+1	7	9	14	12	4	3	13	10	∞	11	0	6	8	2	5	1	7
x^2+1	8	2	10	0	13	5	4	14	11	∞	12	1	7	9	3	6	8
x^3+x	9	7	3	11	1	14	6	5	0	12	∞	13	2	8	10	4	9
x^2+x+1	10	5	8	4	12	2	0	7	6	1	13	∞	14	3	9	11	10
x^3+x^2+x	11	12	6	9	5	13	3	1	8	7	2	14	∞	0	4	10	11
x^3+x^2+x+1	12	11	13	7	10	6	14	4	2	9	8	3	0	∞	1	5	12
x^3+x^2+1	13	6	12	14	8	11	7	0	5	3	10	9	4	1	∞	2	13
x^3+1	14	3	7	13	0	9	12	8	1	6	4	11	10	5	2	∞	14
0	∞	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	∞

- 8% Het punt $A(x+1, x^3)$ is één van de punten van de elliptische kromme E. Bepaal alle andere punten en duid hierbij aan welke inversen zijn van elkaar. Hoeveel punten heeft deze elliptische kromme?
- 6% Bereken 2A, 4A en 8A en identificeer het resultaat met één van de hiervoor gevonden punten.
- 6% Bereken de overige veelvouden van A, tot je hetzij het neutrale element, hetzij het punt dat zijn eigen inverse is bekomt. Bepaal hieruit de structuur van de overeenkomstige groep. Is de groep cyclisch en zo ja, met hoeveel primitieve elementen.

4. 10% Welk criterium moet, of welke criteria moeten voldaan zijn opdat een veelterm irreducibel is. Ga na of $x^5 + x^4 + 2x^3 + 2x + 1$ hieraan voldoet in het veld F_{32}.

5. 15% Stapelprobleem met Excel (Veralgemeende algoritme X toepassen. Ongeveer 50 kolommen en 2000 rijen, 21 soepele voorwaarden, 32 stricte voorwaarden)

6. 12% Teken het cykeldiagram van de groep, waarvan de groepstabel hieronder gegeven is. Bepaal vervolgens de partitionering van de groepselementen in conjugatieklassen. Stel tenslotte de conjugatievergelijking op.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
B	A	D	C	F	E	H	G	J	I	L	K	N	M	P	O
C	H	E	J	G	L	I	N	K	P	M	B	O	D	A	F
D	G	F	I	H	K	J	M	L	O	N	A	P	C	B	E
E	N	G	P	I	B	K	D	M	F	O	H	A	J	C	L
F	M	H	O	J	A	L	C	N	E	P	G	B	I	D	K
G	D	I	F	K	H	M	J	O	L	A	N	C	P	E	B
H	C	J	E	L	G	N	I	P	K	B	M	D	O	F	A
I	J	K	L	M	N	O	P	A	B	C	D	E	F	G	H
J	I	L	K	N	M	P	O	B	A	D	C	F	E	H	G
K	P	M	B	O	D	A	F	C	H	E	J	G	L	I	N
L	O	N	A	P	C	B	E	D	G	F	I	H	K	J	M
M	F	O	H	A	J	C	L	E	N	G	P	I	B	K	D
N	E	P	G	B	I	D	K	F	M	H	O	J	A	L	C
O	L	A	N	C	P	E	B	G	D	I	F	K	H	M	J
P	K	B	M	D	O	F	A	H	C	J	E	L	G	N	I

7.
- 12% Bepaal de cykelindex om de hoekpunten van een reguliere achthoekige ster (Stellated Octahedron), waarbij zowel rotaties als spiegelingen in beschouwing worden genomen. Je kan deze figuur manipuleren door het programma Antiview op te starten met het argument UC4. (. antiview.exe UC4)
- 10% Hoeveel configuraties zijn er mogelijk waarbij er 2 kleuren 4 maal gebruikt worden. Hoeveel van deze configuraties zijn een spiegelbeeld van elkaar?
- 6% Hoeveel configuraties zijn er mogelijk waarbij er 4 kleuren 2 maal gebruikt worden. Hoeveel van deze configuraties zijn een spiegelbeeld van elkaar?