

Hoe los ik een examen Discrete Wiskunde op?

Contents

1	Velden	1
1.1	Het algoritme van Euclides	1
1.2	Berekenen van een primitieve wortel	2
1.3	De baby-step, giant-step techniek	2
1.4	Irreducibele veeltermen	3
1.5	Elliptische krommen	3
1.5.1	Berekening van de punten	6
1.5.2	Verdubbeling van de punten	7
1.5.3	Soort bepalen	7
2	Groepen	7
2.1	Partitionering van de groepselementen in conjugatieklassen . . .	7
2.2	Cykelindex bepalen	7

Het examen Discrete Wiskunde verandert weinig en bestaat altijd uit zeven vragen. Zes van deze vragen zijn analoog met elke examenperiode en één vraag is willekeurig vanuit heel de cursus. In dit document wil ik technieken toelichten om het examen op een goede manier op te lossen. Dit gaat vooral over trukjes in Excel en de Antiview die je kan gebruiken in plaats van alles manueel te doen.

1 Velden

1.1 Het algoritme van Euclides

Het algoritme van Euclides komt altijd terug dus dit moet heel goed gekend zijn. Het is nuttig om Excel het meeste werk te laten doen. Stel dat we 97 willen delen door 53. Je begint met de startopstelling.

	A	B	C
1	53		
2			97
3			

Daarna gebruik je de functie `FLOOR.MATH` om **todo**

1.2 Berekenen van een primitieve wortel

Een primitieve wortel is het kleinste getal dat niet deelbaar is door een bepaald getal voor een bepaald veld. Het berekenen van een primitieve is heel eenvoudig. Er is slechts één gegeven nodig en dat is het veld. We nemen het volgende voorbeeld: Bereken de primitieve wortel over \mathbb{Z}_{4051} .

1. Trek 1 af van het veldgetal en ontbindt dit in factoren. Gebruik het programma *factor* dat ook beschikbaar is op het examen. (Ingeven: *factor 4050*)

$$4051 - 1 = 4050 = 2 * 3^4 * 5^2$$

Het getal 4050 wijst simpelweg op het aantal elementen in dit veld.

2. We hebben het getal 4050 ontbonden in factoren. De bedoeling is om een excel-bestand op te maken zodat de primitieve wortel redelijk eenvoudig kan berekend worden. Het excel-bestand heeft volgende opmaak:

x	x ⁵	x ²⁵
x ³	x ^{3*5}	x ^{3*25}
x ⁹	x ^{9*5}	x ^{9*25}
x ²⁷	x ^{27*5}	x ^{27*25}
x ⁸¹	x ^{81*5}	x ^{81*25}
x ²	x ^{2*5}	x ^{2*25}
x ^{2*3}	x ^{2*3*5}	x ^{2*3*25}
x ^{2*9}	x ^{2*9*5}	x ^{2*9*25}
x ^{2*27}	x ^{2*27*5}	x ^{2*27*25}
x ^{2*81}	x ^{2*81*5}	x ^{2*81*25}

Dit stellen allemaal delers voor van het getal 4050. Nu is het de bedoeling dat we x vervangen door oplopende getallen startend vanaf 2. **todo**

1.3 De baby-step, giant-step techniek

De baby-step, giant-step techniek wordt gebruikt om een index van een getal ten opzichte van een primitieve wortel in een bepaald veld te berekenen. Hier moet de Euclidische deling ook uitgevoerd worden dus zorg dat je dit al goed kunt. Bij dit soort vraagstukken zijn er 3 gegevens.

- Het veld \mathbb{Z}
- Een getal in dit veld waarvan de index moet berekend worden.
- De primitieve wortel w

Op het examen zal er staan hoe groot één giant-step moet zijn. In dit voorbeeld nemen we giant-steps die 10 baby-steps groot zijn. We beschouwen het veld \mathbb{Z}_{71} en de primitieve wortel $w = 7$. We willen de index van 5 berekenen. Begin met de eerste 10 baby-steps te genereren. Je begint met de primitieve wortel, en daarna gebruik je Formule 1. De letter b stelt de n -de baby-step voor. Bekijk ook Figuur 1 waarop dit gevisualiseerd staat (p. 4).

$$b_n = b_{n-1} * w \% 71 \quad (1)$$

Nadat de eerste 10 baby-steps genereerd zijn moet je het inverse element, ten opzichte van 71, van de laatste baby-step bepalen. Dit doe je door het algoritme van Euclides toe te passen (Figuur 2).

Het inverse element is hier dus 30. Nu moeten de giant-steps gegenereerd worden. Je vertrekt vanaf het getal waarvan we de index zoeken. Daarna gebruik je Formule 1 maar vervang je de baby-step door de giant-step. Dit wordt voorgesteld in Figuur 3.

Merk op dat het getal 27 zowel bij de baby-steps als bij de giant-steps voorkomt. Dit stelt de index voor die we zoeken. Het getal 27 is het achtste getal in de baby-step verzameling. Bij de giant-step verzameling is dit het derde getal. Aangezien elke giant-step een grootte heeft van tien babysteps, wordt dit nog eens vermenigvuldigd met tien. De index wordt

$$8 + (3 * 10) = 8 + 30 = 38$$

De oplossing is formeel: De index van 5 over het veld \mathbb{Z}_{71} met primitieve wortel $w = 7$ is 38. Er zijn 3 giant-steps en 8 baby-steps nodig.

1.4 Irreducibele veeltermen

Een irreducibele veelterm is een veelterm dat niet meer deelbaar is over een bepaald veld. Op het examen wordt een priemveld gegeven en een bepaalde veelterm. Beschouw het veld F_{32} en de veelterm $x^5 + x^4 + 2x^3 + 2x + 1$. We weten dat $2^5 = 32$, dus $p = 2$ en $n = 5$. De test moet uitgevoerd worden met elke veelterm $x^{p^i} - x$ met $i \leq \frac{n}{2}$. Het komt erop neer dat je n deelt door 2 en dit getal afrondt naar beneden. Dus $\text{floor}(\frac{5}{2}) = 2$.

De test moet dus uitgevoerd worden met $i = 1$ en $i = 2$. We moeten de veelterm dus delen door $x^{2^1} - x$ en $x^{2^2} - x$. Indien geen gemeenschappelijke deler werd gevonden dan is de veelterm irreducibel. Je kan eenvoudig de euclidische deling uitvoeren. Je moet enkel elke graad als een 'getal' zien. Zo is $4x^3 + x + 7$ gelijk aan 4017. Onze veelterm wordt dus 112021. **in excel pls**

$$\begin{array}{cc|cc} 110 & & 10010 & \\ & 112021 & & 112021 \end{array}$$

1.5 Elliptische krommen

Bij een vraag over een elliptische kromme krijg je zeker drie gegevens:

Figure 1: Voorstelling van Formule 1 voor de berekening van de baby-steps

Clipboard		Font			
SUM		\times \checkmark f_x	<code>=MOD(C14*\$B\$7,\$B\$6)</code>		
	A	B	C	D	E
1					
2					
3					
4					
5					
6	veld	71			
7	w	7			
8	g	5			
9					
10			7		
11			49		
12			59		
13			58		
14			51		
15			=MOD(C14*		
16			14		
17			27		
18			47		
19			45		
20					
21					

Figure 2: Algoritme van Euclides bij de baby-step, giant-step techniek

45			1			0		
0	0	71	0	0	0	0	0	1
45	1	-45	1	1	-1	0	1	0
-26	1	26	1	1	-1	-1	1	1
19	1	-19	2	1	-2	-1	1	1
-14	2	7	6	2	-3	-4	2	2
5	1	-5	8	1	-8	-5	1	5
-4	2	2	22	2	-11	-14	2	7
1	2	-2	30	2	-60	-19	2	38
		0			-71			45

Figure 3: Voorstelling van Formule 1 voor de berekening van de giant-steps

SUM :: ✕ ✓ f _x =MOD(E15*\$B\$9, \$B\$6)					
	A	B	C	D	E
4					
5					
6	veld	71			
7	w	7			
8	g	5			
9	invers element	30			
10			7		5
11			49		8
12			59		27
13			58		29
14			51		18
15			2		43
16			14		=MOD(E15 ⁴³)
17			27		5
18			47		8
19			45		27
20					

1. Het veld en de vergelijking van de elliptische kromme
2. De irreducibele veelterm
3. De primitieve wortel
4. Een groepstabel

Op het examen worden er slides gegeven (meer specifiek, slide 6 en 10 van het bestand 1d.pptx). Dit zijn de slides waarop de berekening voor het verdubbelen van de punten ontstaan, dus deze moet je niet vanbuiten kennen. Je moet wel weten welke slide je nodig hebt, maar dit is gewoon naar de vergelijking kijken en zien welke er overeenkomt met die op de slide. Voor de verdere uitwerking van dit onderdeel worden de gegevens van het examen gebruikt.

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

\oplus	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	∞

1.5.1 Berekening van de punten

De eerste stap is altijd het berekenen van alle punten op deze elliptische kromme.

1.5.2 Verdubbeling van de punten

1.5.3 Soort bepalen

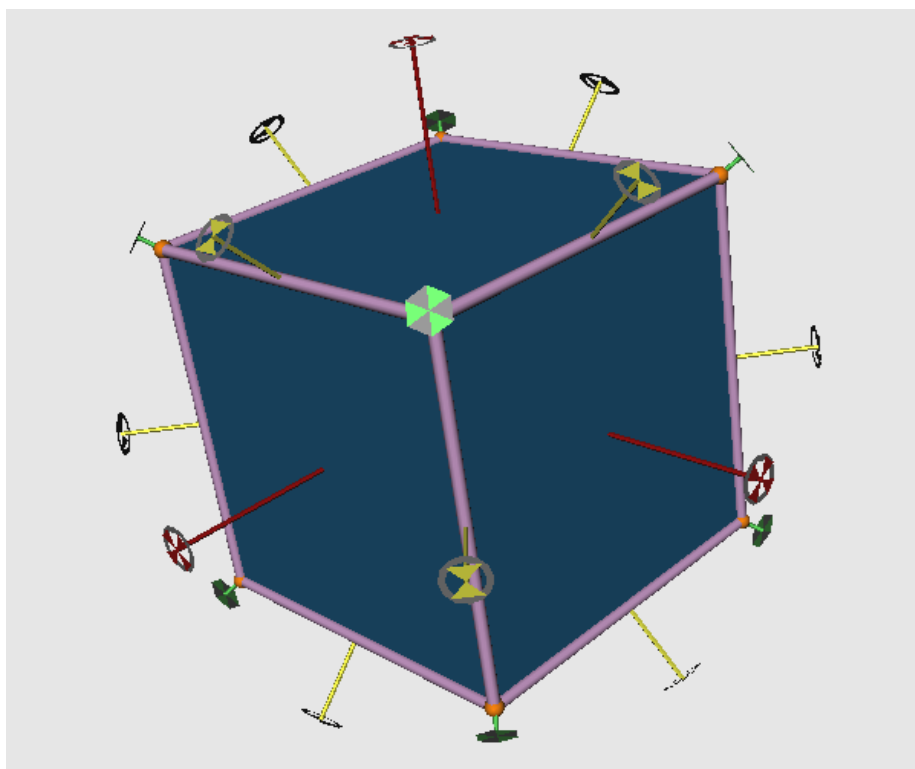
2 Groepen

2.1 Partitionering van de groepselementen in conjugatieklassen

2.2 Cykelindex bepalen

Op het examen wordt er gevraagd om de cykelindex van een willekeurige drie dimensionele veelhoek te bepalen. Daarna wordt er gevraagd om het aantal configuraties te bepalen waarbij een X aantal kleuren Y maal gebruikt worden.

Op deze vraag moet de AntiView gebruikt worden die standaard al open staat op het examen met de figuur. Dit programma toont default de symmetrie en rotatie-assen niet. Zonder dit hulpmiddel is deze vraag haast onmogelijk. Je kan de assen tonen door op de knop 'Y' te drukken op het toetsenbord. In de voorbeelden gebruiken we een kubus. Je kan deze figuur ook bekomen door het programma AntiView via de commandolijn op te starten met als argument cube.



Normaal zie je 3 soorten assen verschijnen: rode, gele en groene. Elke kleur heeft zijn eigen betekenis.

- Rood:
- Geel:
- Groen: