Hoe los ik een examen Discrete Wiskunde op?

Contents

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. In dit document wil ik technieken toelichten om het examen sneller op te lossen. Dit gaat vooral over trukjes in Excel en de Antiview die je kan gebruiken in plaats van alles manueel te dien.

1 De Euclidische deling

De Euclidische deling komt vaak voor dus is het verstanding om slechts een kleine stap te doen en excel de rest. Deze techniek werkt enkel bij een deling door twee gehele getallen. Veeltermen moet je nog altijd manueel delen. todo

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

2.1 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. 3).

$$b_n = b_{n-1} * w \ \% \ 71 \tag{1}$$

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

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

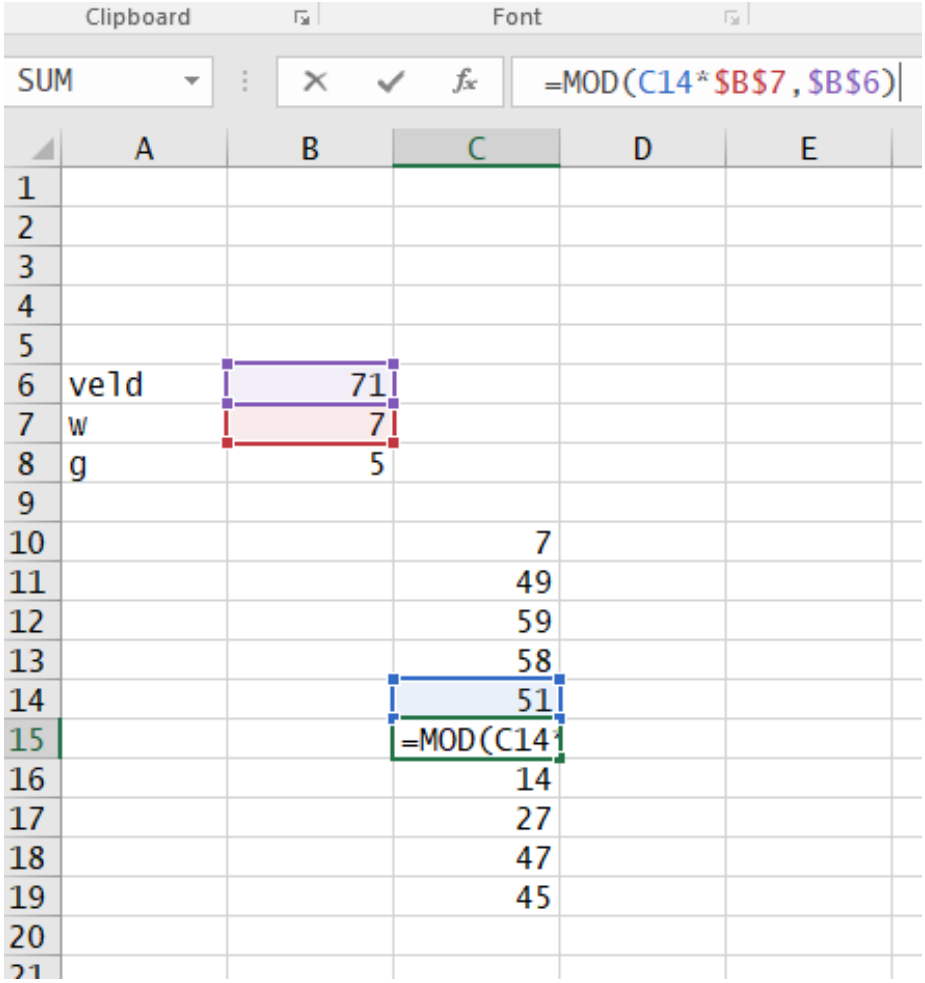
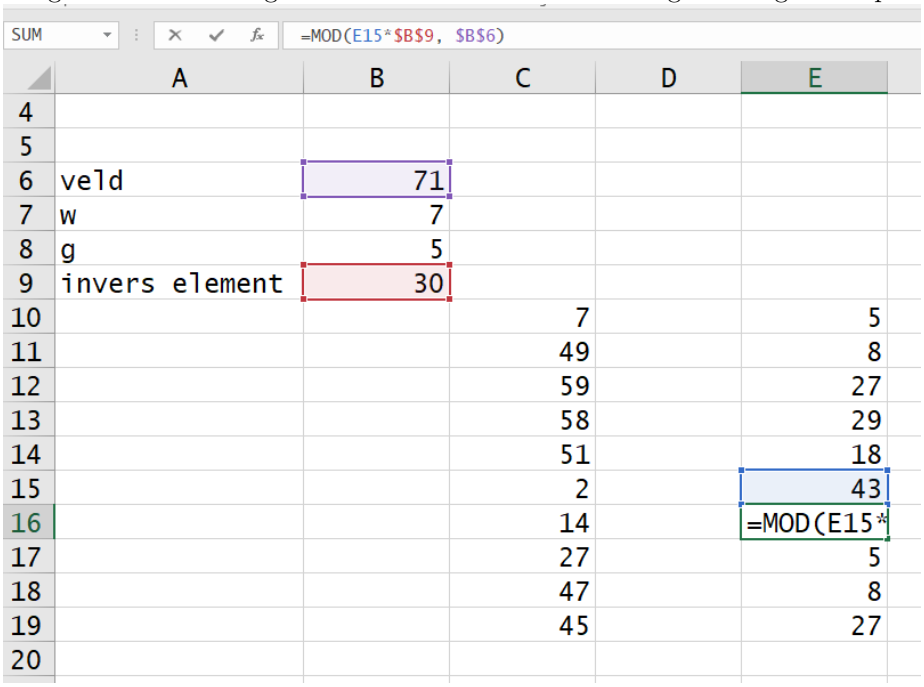


Figure 2: Algoritme van Euclides bij de baby-step, giant-step techniek

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



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 nodig en 8 baby-steps.

2.2 Elliptische krommen