

Het Raadsel Enigma

Uitwerkingen

Het laatste woord in de instructies is turing.

Opgave 1.

derfuehreristtotxderkampfggehtweiterxdoenitzx

Dit is een bericht verstuurd door Admiraal Dönitz nadat Hitler zichzelf had omgebracht:

Der Führer ist tot. Der Kampf geht weiter. Dönitz.

Opgave 2 (Walzenlage). (a) $3! = 3 \cdot 2 \cdot 1 = 6$

(b) $5 \cdot 4 \cdot 3 = 5!/2! = 60$

(c) $n \cdot (n - 1) \cdot (n - 2) = n!/(n - 3)!$

Opgave 3 (Grundstellung). $26^3 = 17576$

Opgave 4 (Steckerbrett). *Voor deze opgave zijn er meerdere manieren op tot het goede antwoord te komen. We geven er hier drie. Met de algemene formule kan vervolgens de tabel als volgt worden ingevuld:*

k	Aantal manieren	k	Aantal manieren
0	1	7	$1.3 \cdot 10^{12}$
1	325	8	$1.1 \cdot 10^{13}$
2	44580	9	$5.4 \cdot 10^{13}$
3	3453450	10	$1.5 \cdot 10^{14}$
4	$1.6 \cdot 10^6$	11	$2.0 \cdot 10^{14}$
5	$5.0 \cdot 10^9$	12	$1.0 \cdot 10^{14}$
6	$1.0 \cdot 10^{11}$	13	$7.9 \cdot 10^{12}$

Methode 1 We kunnen op $26!/(26 - 2k)!$ manieren k kabels leggen, maar hierbij zijn sommige kabels wel dubbel geteld. Daarom delen we nog een aantal combinaties weg. Zo is A met B verbinden hetzelfde als B met A verbinden. Hierom delen we nog

door 2^k . Ook maakt het niet uit of we eerst AB en dan CD verbinden of eerst CD en dan AB. De volgorde van de kabels maakt niet uit. Hierom delen we nog door $k!$. De uiteindelijke formule wordt

$$\frac{26!}{(26 - 2k)! \cdot 2^k \cdot k!}.$$

(Voor de liefhebber: dit is precies het aantal involuties in de permutatiegroep S_{26} die k 2-cykels bevatten)

Methode 2 We kiezen eerst het aantal letters dat niet verbonden wordt, dit is $\binom{26}{26-2k} = \binom{26}{2k}$. De letters om verbonden te worden zetten we op een rijtje. Vervolgens nemen we voor de eerste kabel de eerste letter in dit rijtje, en kiezen een letter om mee te verbinden. Dit kan op $2k - 1$ manieren. Vervolgens nemen we de eerstvolgende (niet al gekozen) letter voor de tweede kabel, en kiezen een letter om mee te verbinden. Dit kan op $2k - 3$ manieren. We komen dan uit op

$$\binom{26}{2k} \cdot (2k - 1)!!$$

Methode 3 Dit is een recursieve methode. Neem aan dat we weten op hoeveel manieren we het stekkerbord met $k - 1$ kabels kunnen bestekkeren. Voor de volgende kabel kiezen we dan twee letters. Voor de eerste letter zijn $26 - 2k + 2$ mogelijkheden en voor de tweede $26 - 2k + 1$. Er zijn namelijk al $2k - 2$ letters 'bezet'. Let op dat de volgorde van de letters in deze kabel niet uitmaakt, dus we delen door 2. Verder maakt de volgorde waarin deze kabel voorkomt niet uit, dus we delen door k . We krijgen dan

$$\# \text{ mogelijkheden } k - 1 \text{ kabels} \cdot \frac{(26 - 2k + 2)(26 - 2k + 1)}{2k}.$$

Extra opgave: laat zien dat de algemene formule voor alle drie de methodes hetzelfde antwoord geven!

Opgave 5 (Complexiteit). (a) Om het totaal aantal mogelijke instellingen te berekenen, vermenigvuldigen we het aantal mogelijkheden voor de Walzenlage, Grunstellung en Steckerbrett. Hiervoor gebruiken we de antwoorden van de vorige opgaven:

$$\text{aantal mogelijkheden} = 60 \cdot 17565 \cdot 1.5 \cdot 10^{14} \approx 1.58 \cdot 10^{20}.$$

- (b) We delen het aantal mogelijkheden door de 7000 codekrakers, en vermenigvuldigen dit met 5 om het aantal seconden te berekenen. Dit geeft

$$\frac{1.58 \cdot 10^{20}}{7000} \cdot 5 \approx 1.13 \cdot 10^{17} \text{ seconden.}$$

Dit kunnen we nog omrekenen naar jaren:

$$\frac{1.13 \cdot 10^{17}}{60 \cdot 60 \cdot 24 \cdot 365} \approx 3.58 \cdot 10^9 \text{ jaar.}$$

Het zou dus meer dan 3.5 miljard jaar duren om alle instellingen te proberen!