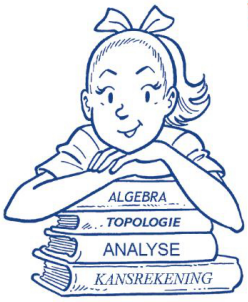
WISKUNNEND WISKE

DE VERBIJSTERENDE VERCIJFERING

FINALE 2020 - RODE DRAAD A



Wij gebruiken het internet tegenwoordig voor talrijke activiteiten. Denk bijvoorbeeld aan e-mails verzenden, wachtwoorden intypen, foto's delen en betalingen uitvoeren. Maar we staan er niet altijd bij stil dat bij het ingeven of uitwisselen van deze informatie er een derde partij betrokken kan geraken die deze informatie wil stelen of misbruiken. We moeten dus verzekeren dat het internet gebruiken op een **veilige** manier kan.

Hiervoor hebben we zogenaamde **cryptosystemen**. Een **cryptosysteem** is een mechanisme dat toelaat om informatie in een bepaald alfabet te **vercijferen** naar tekst in een ander alfabet, maar ook **omgekeerd**: iedere tekst in het ander alfabet moet terug te vertalen zijn naar een tekst in het oorspronkelijk alfabet.

Om boodschappen te kunnen vercijferen of ontcijferen hebben beide personen die het cryptosysteem gebruiken een geheime **sleutel** nodig. Niemand anders mag weten hoe deze geheime sleutel eruit ziet, en dit zorgt ervoor dat een derde persoon die een boodschap, bedoeld voor iemand anders, kan onderscheppen de boodschap niet kan begrijpen.

De geschiedenis kent tal van voorbeelden van zulke cryptosystemen, al sinds de tijd van Julius Caesar! Maar in 1977 beschreven

Ron Rivest, Adi Shamir en **Leonard Adleman** een cryptosysteem dat we tot de dag van vandaag nog steeds gebruiken, genaamd **RSA**. De bedoeling van deze opdracht is om jullie te leren hoe RSA werkt.

Hiervoor hebben we wat wiskundige achtergrond nodig. Zo noteren we de rest van a bij deling door n (met $a \in \mathbb{N}$ en $n \in \mathbb{N} \setminus \{0, 1\}$) als a mod n. Zo is bijvoorbeeld 13 mod 3 gelijk aan 1, want $13 = 3 \cdot 4 + 1$. Dus 1 is de rest van 13 bij deling door 3.

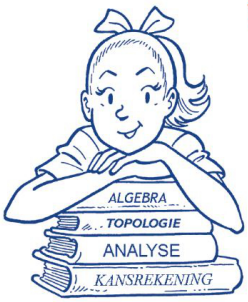
We zeggen dat een geheel getal a **inverteerbaar** is modulo n als er een ander geheel getal b bestaat zodat $a \cdot b$ mod $n = 1$. We noemen b de **inverse** van a mod n. Zo is bijvoorbeeld 3 inverteerbaar modulo 14 omdat $3 \cdot 5 = 15$ en 15 mod 14 = 1.

Hoe bereken je dan zo een inverse, als ze al bestaat? Zonder bewijs mogen jullie het volgende gebruiken:

a is inverteerbaar modulo n **als en slechts als** $\text{ggd}(a, n) = 1$.

Hier staat "ggd" voor de **grootst gemene deler**. Om deze te berekenen gebruiken we best het **algoritme van Euclides**:

1. Stel $a > n$ (wissel anders a en n om).
2. Bereken a mod n, noem het r.
3. Als $r = 0$, dan is de grootst gemene deler gelijk aan n.
4. Anders, herhaal stappen 2 en 3 waar je a vervangt door n en n door r.



Voorbeeld: we berekenen ggd$(312, 594)$. Stapsgewijs krijgen we: ggd$(594, 312)$ = ggd$(312, 282)$ = ggd$(282, 30)$ = ggd$(30, 12)$ = ggd$(12, 6) = 6$

We kennen ook de volgende eigenschap van **Bézout**:

Voor de grootst gemene deler d van a en b bestaan er gehele getallen x en y zodat $ax + by = d$.

Dit getal d is bovendien ook het kleinste strikt positieve getal dat aan deze eigenschap voldoet.

Voorbeeld: We berekenen de grootst gemene deler van 23 en 18 met het algoritme van Euclides, maar we maken een tabel waar we ook de quotiënten bijhouden:

r	23	18	5	3	2	1	0
q		1	3	1	1	2	

We zien dus dat ggd$(23, 18) = 1$ en

$$1 = 3 - \not{1} \cdot 2 = (18 - 3 \cdot \underline{5}) - (\underline{5} - \not{1} \cdot \underline{3})$$

$$= (18 - 3 \cdot \underline{(23 - \not{1} \cdot 18)}) - (\underline{(23 - \not{1} \cdot 18)} - \underline{(18 - 3 \cdot 5)}) = 9 \cdot 18 - 7 \cdot 23$$

door in de laatste stap 5 te vervangen door 23-18.

Hieruit volgt dat $1 = 9 \cdot 18 \bmod 23$ En dus is 18 inverteerbaar modulo 23 met 9 als inverse.

Opdracht (40 minuten)

1. Wat is 579 mod 13?
2. Wat is 21474 mod 11?
3. Wat is 2^{2020} mod 7?
4. Wat is de inverse van 23 modulo 101?