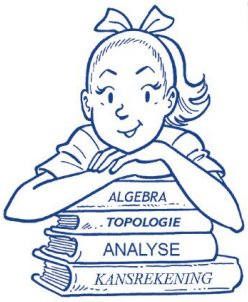
WISKUNNEND WISKE

DE VERBIJSTERENDE VERCIJFERING

FINALE 2020 - RODE DRAAD C



Herhaal dat we a mod n noteren voor de rest van a bij deling door n. We noemden a **inverteerbaar** modulo n als er een geheel getal b bestaat zodat $a \cdot b$ mod $n = 1$. Dit geheel getal b bestaat als en slechts als ggd$(a, n) = 1$.
Zulke inverse was te vinden zoals in het voorbeeld.
Voorbeeld: We berekenden de grootst gemene deler van 23 en 18 met het algoritme van Euclides:

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

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

$$1 = 3 - 2 = (18 - 3 \cdot \underline{5}) - (\underline{5} - \underline{3})$$

$$= (18 - 3 \cdot \underline{(23 - 18)}) - (\underline{(23 - 18)} - \underline{(18 - 3 \cdot 5)}) = 9 \cdot 18 - 7 \cdot 23.$$

We herhalen ook hoe RSA werkt: we hebben een getal $n = pq$ waar p en q oneven priemgetallen zijn (n publiek, p en q geheim). Verder is e (publiek) zodanig gekozen dat het inverteerbaar is modulo $(p - 1)(q - 1)$, en de inverse noemen we d (moet geheim blijven).
We stellen een bericht m voor door een getal tussen 0 en $n - 1$. Om het te **vercijferen**, berekenen we $c = m^e$ mod n. Om c te **ontcijferen**, berekenen we c^d mod n, wat opnieuw m geeft.

Opdracht (20 minuten)

Zij $n = 33$, $e = 7$. We stellen de letters van A tot Z (in alfabetische volgorde) voor door de getallen van 0 tot en met 25 (van klein naar groot). Verder hebben we:

Teken	.	?	!	-	(	)	:
Getal	26	27	28	29	30	31	32

Een spatie vercijferen we ook gewoon met een spatie.

Ontcijfer het volgende met RSA vercijferde bericht:

JQ (SIUHQO CG JQOQ-NT