

Elementaire Getaltheorie
Inleveropgaven deel 1

Jan-Jaap Oosterwijk

Herfst Semester, 2005

Opgave 1

Bepaal de ggd d van 20785 en 44350. Bepaal tevens gehele getallen x, y zó dat $d = 20785x + 44350y$.

Uitwerking:

Definieer $a := 20785$ en $b := 44350$. Dan geeft het Euclidisch algoritme

$$\begin{array}{rclcl} 44350 & = & 0a & + & 1b; \\ 20785 & = & 1a & + & 0b; \\ 44350 & = & 2 \cdot 20785 & + & 2780; & 2780 & = & -2a & + & 1b; \\ 20785 & = & 7 \cdot 2780 & + & 1325; & 1325 & = & 15a & - & 7b; \\ 2780 & = & 2 \cdot 1325 & + & 130; & 130 & = & -32a & + & 15b; \\ 1325 & = & 10 \cdot 130 & + & 25; & 25 & = & 335a & - & 157b; \\ 130 & = & 5 \cdot 25 & + & 5; & 5 & = & -1707a & + & 800b; \\ 25 & = & 5 \cdot 5 & + & 0; & 0 & = & 8870a & - & 4157b. \end{array}$$

Dus $d := \text{ggd}(20785, 44350) = 5$ en $x = -1707$ en $y = 800$ voldoen aan de lineaire vergelijking $d = 20785x + 44350y$.

Opgave 2

Zij a, b een tweetal verschillende natuurlijke getallen, en relatief priem. Laat zien dat voor elke $n \in \mathbb{N}$ geldt

$$\text{ggd}\left(\frac{a^n - b^n}{a - b}, a - b\right) = \text{ggd}(n, a - b)$$

Uitwerking:

Definieer $c := a - b$. Dan geldt dat

$$a^n - b^n = (b + c)^n - b^n = \sum_{k=0}^n \binom{n}{k} b^k c^{n-k} - b^n = \sum_{k=0}^{n-1} \binom{n}{k} b^k c^{n-k},$$

dus

$$\frac{a^n - b^n}{a - b} = \frac{(b + c)^n - b^n}{c} = \sum_{k=0}^{n-1} \binom{n}{k} b^k c^{n-k-1} = nb^{n-1} + \sum_{k=0}^{n-2} \binom{n}{k} b^k c^{n-k-1}.$$

Aangezien a en b relatief priem zijn, hebben $c = a - b$ en b ook geen delers gemeen. Dus

$$\text{ggd}\left(\frac{a^n - b^n}{a - b}, a - b\right) = \text{ggd}\left(\frac{(b + c)^n - b^n}{c}, c\right) = \text{ggd}(nb^k, c) = \text{ggd}(n, c) = \text{ggd}(n, a - b).$$

Opgave 3

Een natuurlijk getal n heet *overvloedig* als $\sigma(n) > 2n$.

- (a) Zij n een overvloedig getal. Laat zien dat elk veelvoud van n ook overvloedig is.

Uitwerking:

Zij $n \in \mathbb{N}$ zodanig dat $\sigma(n) > 2n$. Aangezien n een unieke priemfactorisatie $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ heeft, is elk veelvoud m van n van de vorm $m = p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r} a$ met $j_i \geq k_i$ en $a \in \mathbb{N}$ waarbij $\text{ggd}(n, a) = 1$. Aangezien voor elke i ,

$$\sigma(p_i^{j_i}) = \frac{p_i^{j_i+1} - 1}{p_i - 1} \geq \frac{p_i^{j_i+1} - p_i^{j_i-k_i}}{p_i - 1} = p_i^{j_i-k_i} \cdot \frac{p_i^{k_i+1} - 1}{p_i - 1} = p_i^{j_i-k_i} \sigma(p_i^{k_i}),$$

en aangezien $\sigma(a) \geq 1 + a > a$, vinden we dat

$$\begin{aligned} \sigma(m) &= \left(\prod_{i=1}^r \sigma(p_i^{j_i}) \right) \sigma(a) \\ &\geq \left(\prod_{i=1}^r p_i^{j_i-k_i} \sigma(p_i^{k_i}) \right) \sigma(a) \\ &= \left(\prod_{i=1}^r p_i^{j_i-k_i} \right) \sigma(n) \sigma(a) \\ &> \left(\prod_{i=1}^r p_i^{j_i-k_i} \right) 2na \\ &= 2m. \end{aligned}$$

(b) Laat zien dat er een oneven overvloedig getal is.

Uitwerking:

We kunnen er vrij gemakkelijk een vinden. Als we simpelweg het product van de eerste zoveel oneven priemgetallen proberen, vinden we al snel dat

$$\begin{aligned} \sigma(15015) &= \sigma(3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) \\ &= \sigma(3)\sigma(5)\sigma(7)\sigma(11)\sigma(13) \\ &= (1+3)(1+5)(1+7)(1+11)(1+13) \\ &= 32256, \end{aligned}$$

dus 15015 is bijvoorbeeld zo'n getal.

Opmerking:

Een ander makkelijk soort getal om te proberen zou een macht van een enkel priemgetal, zeg p^k , zijn. Echter, stel dat

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1} = ap^k$$

voor zekere $a \in \mathbb{R}$. Dan is

$$a = \frac{p^{k+1} - 1}{p^{k+1} - p^k} = 1 + \frac{p^k - 1}{p^{k+1} - p^k}.$$

Maar $p^{k+1} - 2p^k = p^k(p - 2) \geq 0$, dus in het bijzonder $p^{k+1} - 2p^k > -1$. Hieruit volgt dat $p^{k+1} - p^k > p^k - 1$ en dus dat $\sigma(p^k) < 2p^k$. (Merk op dat dit zich zelfs niet beperkt tot een oneven getal.)

(c) Laat zien dat er oneindig veel oneven overvloedige getallen zijn.

Uitwerking:

Een makkelijke manier om vanuit één gevonden oneven overvloedig getal er oneindig veel te krijgen is m.b.v. onderdeel (a) van deze vraag. Stel n is een overvloedig oneven getal. Dan is voor elke $k \in \mathbb{N}$, n^k in het bijzonder een veelvoud van n en dus ook overvloedig.

Opgave 4

Vindt alle oplossingen $x \in \mathbb{Z}$ van de congruentievergelijking

$$987x \equiv 610 \pmod{1597}$$

Uitwerking:

Bij het bepalen van $\text{ggd}(987, 1597)$ geeft het Euclidisch algoritme

		1597 =	0 · 987	(mod 1597);
		987 =	1 · 987	(mod 1597);
1597 =	1 · 987 + 610;	610 ≡	-1 · 987	(mod 1597);
987 =	1 · 610 + 377;	377 ≡	2 · 987	(mod 1597);
610 =	1 · 377 + 233;	233 ≡	-3 · 987	(mod 1597);
377 =	1 · 233 + 144;	144 ≡	5 · 987	(mod 1597);
233 =	1 · 144 + 89;	89 ≡	-8 · 987	(mod 1597);
144 =	1 · 89 + 55;	55 ≡	13 · 987	(mod 1597);
89 =	1 · 55 + 34;	34 ≡	-21 · 987	(mod 1597);
55 =	1 · 34 + 21;	21 ≡	34 · 987	(mod 1597);
34 =	1 · 21 + 13;	13 ≡	-55 · 987	(mod 1597);
21 =	1 · 13 + 8;	8 ≡	89 · 987	(mod 1597);
13 =	1 · 8 + 5;	5 ≡	144 · 987	(mod 1597);
8 =	1 · 5 + 3;	3 ≡	233 · 987	(mod 1597);
5 =	1 · 3 + 2;	2 ≡	377 · 987	(mod 1597);
3 =	1 · 2 + 1;	1 ≡	610 · 987	(mod 1597).

Dus $\text{ggd}(987, 1597) = 1$, i.e. de restklasse $987 \pmod{1597}$ is inverteerbaar. In het bijzonder geldt dat $610 \cdot 987 \equiv 1 \pmod{1597}$, dus $x \equiv 610^2 = 372100 = -1 + 233 \cdot 1597 \equiv -1 \pmod{1597}$. Dus alle oplossingen van de oorspronkelijke congruentievergelijking worden gegeven door $\{x \in \mathbb{Z} \mid x \equiv -1 \pmod{1597}\}$.

Opmerking:

Ik heb de berekening geheel uitgeschreven omdat ik een beredeneerd en algemeen toepasbaar antwoord wilde geven. Echter, al in de eerste stap van het algoritme is een oplossing van het oorspronkelijke probleem (toevallig) direct herkenbaar ($610 \equiv -1 \cdot 987 \pmod{1597}$).

Opgave 5

Bewijs door inductie dat voor alle $n \in \mathbb{N}$ geldt,

$$5^n \equiv 1 + 4n \pmod{16}$$

Vindt een analoge formule voor $5^n \pmod{32}$.

Uitwerking:

De congruentiegleichheid geldt duidelijk voor $n = 1$. Stel nu dat zij geldt voor een zekere $n \in \mathbb{N}$. Dan is $5^{n+1} \equiv 5 + 20n \equiv 5 + 4n \equiv 1 + 4(n+1) \pmod{16}$. Volgens het principe van volledige inductie is hiermee de gelijkheid bewezen voor alle $n \in \mathbb{N}$.

Stel dat er $a, b \in \mathbb{Z}$ bestaan zodanig dat $5^n \equiv 1 + an + bn^2 \pmod{32}$. Dan volgt uit $5 \equiv 1 + a + b \pmod{32}$ en $25 \equiv 1 + 2a + 4b \pmod{32}$ dat $10 \equiv 2 + 2a + 2b \pmod{32}$ en dus dat $15 \equiv 2b - 1 \pmod{32}$. We vinden dat $b \equiv 8 \pmod{32}$ en $a \equiv -4 \pmod{32}$. Ons vermoeden is dus dat $5^n \equiv 1 - 4n + 8n^2 \pmod{32}$ voor alle $n \in \mathbb{N}$.

De congruentiegleichheid geldt duidelijk voor $n = 1$ (sterker nog, dat uit dat gegeven hebben we a en b afgeleid). Stel nu dat zij geldt voor een zekere $n \in \mathbb{N}$. Dan is $5^{n+1} \equiv 5 - 20n + 40n^2 \equiv 5 + 12n + 8n^2 \pmod{32}$. Tegelijkertijd geldt ook dat $1 - 4(n+1) + 8(n+1)^2 = 1 - 4n - 4 + 8n^2 + 16n + 8 = 20n + 5 + 12n + 8n^2$. Volgens het principe van volledige inductie is hiermee de gelijkheid bewezen voor alle $n \in \mathbb{N}$.

Opmerking:

Het kwadratische verband probeerde ik in eerste instantie omdat uit

$$\left\{ \begin{array}{ll} 5^n \equiv 1 & \pmod{2}; \\ 5^n \equiv 1 & \pmod{4}; \\ 5^n \equiv 1 + 4n & \pmod{8}; \\ 5^n \equiv 1 + 4n & \pmod{16}, \end{array} \right.$$

de graad van de vergelijking leek te stijgen. Later kwam ik tot het inzicht dat in het algemene geval de graad van het juiste polynoom ook af te leiden is uit

$$5^n = (1 + 4)^n = \sum_{k=0}^n \binom{n}{k} 4^k.$$

Zij $i \in \mathbb{N}$ vast. Dan wordt op een gegeven moment $4^k \equiv 0 \pmod{2^i}$, dus je krijgt sowieso een eindig polynoom. De coëfficiënten hangen dus af van de waarden van $\binom{n}{k} \pmod{2^i}$.

Opgave 6

Geef de volledige oplossing van het stelsel congruentievergelijkingen

$$x \equiv 7 \pmod{9} \quad x \equiv 2 \pmod{10} \quad x \equiv 3 \pmod{12} \quad x \equiv 6 \pmod{15}$$

in $x \in \mathbb{Z}$.

Uitwerking:

Als we elke modulus schrijven als product van priem machten krijgen we het equivalente stelsel

$$\begin{aligned} x \equiv -2 \pmod{3^2}, \quad x \equiv 0 \pmod{2}; \quad x \equiv 0 \pmod{3}; \quad x \equiv 0 \pmod{3}; \\ x \equiv 2 \pmod{5}, \quad x \equiv -1 \pmod{2^2}, \quad x \equiv 1 \pmod{5}. \end{aligned}$$

Hieruit is makkelijk (op drie manieren zelfs) een tegenspraak af te leiden: ($x \equiv 0 \pmod{2}$ en $x \equiv 1 \pmod{2}$), ($x \equiv 1 \pmod{3}$ en $x \equiv 0 \pmod{3}$) en ($x \equiv 2 \pmod{5}$ en $x \equiv 1 \pmod{5}$). Dit stelsel heeft dus absoluut geen oplossingen, dus $x \in \emptyset$.

Opgave 7

Zij p, q een tweetal priemgetallen. Hoeveel restklassen modulo pq heeft de vergelijking $x^2 \equiv 1 \pmod{pq}$ als oplossing?

Uitwerking:

Zij p een priemgetal. Zij $x \in \mathbb{Z}$ zodanig dat $x^2 \equiv 1 \pmod{p}$. Dan is $(x-1)(x+1) = x^2 - 1 \equiv 0 \pmod{p}$. Als $p = 2$, dan is $x \equiv 1 \pmod{p}$ de enige oplossing en als p oneven is, dan is $x \equiv \pm 1 \pmod{p}$.

Voor ons oorspronkelijk probleem moeten we dus een paar gevallen onderscheiden. Als $p = q = 2$, dan zijn er precies twee oplossingen voor de vergelijking $x^2 \equiv 1 \pmod{pq}$, nl. $x \equiv \pm 1 \pmod{4}$. Als $p = 2$ en q oneven is, dan heeft $x^2 \equiv 1 \pmod{p}$ één oplossing en $x^2 \equiv 1 \pmod{q}$ twee. Aangezien 2 en p relatief priem zijn volgt er dan m.b.v. de Chinese reststelling dat er $2 \cdot 1 = 2$ oplossingen van de vergelijking $x^2 \equiv 1 \pmod{pq}$ zijn.

Stel tenslotte dat p en q beide oneven zijn. Dan zijn er weer twee gevallen te onderscheiden. Als $p \neq q$ dan zijn er voor elk van de vergelijkingen $x^2 \equiv 1 \pmod{p}$ en $x^2 \equiv 1 \pmod{q}$ twee oplossingen. Omdat p en q verschillend zijn, zijn ze relatief priem, dus volgt er weer dat er $2 \cdot 2 = 4$ oplossingen van de vergelijking $x^2 \equiv 1 \pmod{pq}$ zijn. Als echter $p = q$ dan heeft $x^2 \equiv 1 \pmod{p^2}$ weer slechts twee oplossingen, $x \equiv \pm 1 \pmod{p^2}$.