FACULTEIT INGENIEURSWETENSCHAPPEN
EN ARCHITECTUUR

Hoofdstuk 3 – Modulorekenen

Discrete wiskunde

dr. ir. Cedric De Boom
IDLab - imec

UNIVERSITEIT GENT

IDLab INTERNET & DATA LAB

imec

Priemgetallen en deelbaarheid

Deelbaarheid

Een geheel getal a **deelt** een geheel getal b $\Leftrightarrow$ er bestaat een geheel getal c zodat $a \cdot c = b$

a is een **deler** of **factor** van b

b is een (geheel) veelvoud van a

Notaties:

$a \mid b$ (… is deler van …)

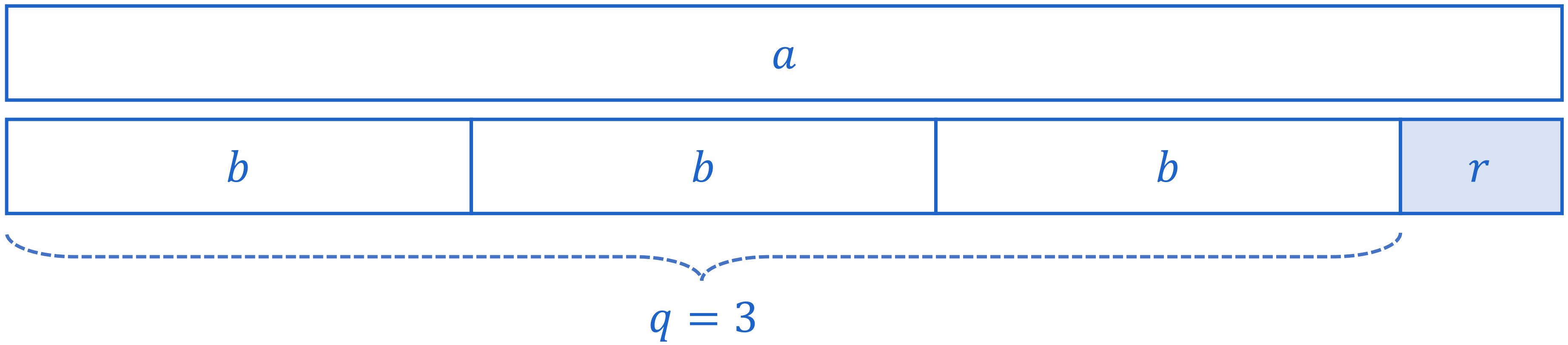
$a \nmid b$ (… is geen deler van …)

Triviale delers van a zijn 1 en a zelf

Het delingsalgoritme

Voor twee gehele getallen a en b bestaan er unieke gehele getallen $q, r \in \mathbb{Z}$ zodat

$$a = b \cdot q + r \qquad \text{met } 0 \leq r < b$$



a = **deeltal**

b = **deler**

q = **quotiënt**

r = **rest**

Het delingsalgoritme

Voor twee gehele getallen a en b bestaan er unieke gehele getallen $q, r \in \mathbb{Z}$ zodat

$$a = b \cdot q + r \qquad \text{met } 0 \leq r < b$$

Er geldt:

$r \neq 0 \Leftrightarrow b \nmid a$ of $r = 0 \Leftrightarrow b \mid a$

Let op:

De rest is steeds positief, ook al is het deeltal negatief!

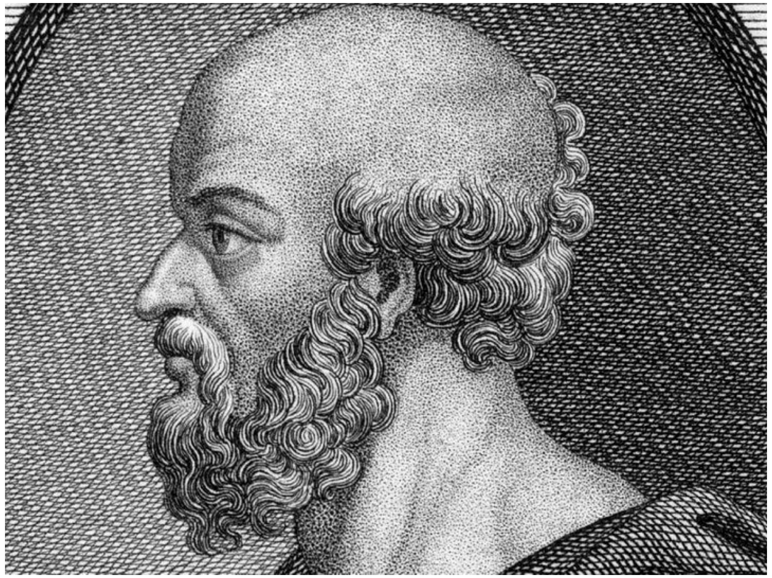
Bijvoorbeeld: $-3 = 4 \cdot (-1) + 1$

Priemgetallen

Een **priemgetal** p heeft twee verschillende delers, nl. zijn triviale delers 1 en p

1 is dus geen priemgetal!

De **Zeef van Eratosthenes** is een algoritme om alle priemgetallen $\leq n$ te vinden



De Zeef van Eratosthenes

Bepaal het aantal priemgetallen kleiner dan $n = 100$:

~~1~~	$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	$\boxed{7}$	~~8~~	~~9~~	~~10~~
$\boxed{11}$	~~12~~	$\boxed{13}$	~~14~~	~~15~~	~~16~~	$\boxed{17}$	~~18~~	$\boxed{19}$	~~20~~
~~21~~	~~22~~	$\boxed{23}$	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	$\boxed{29}$	~~30~~
$\boxed{31}$	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	$\boxed{37}$	~~38~~	~~39~~	~~40~~
$\boxed{41}$	~~42~~	$\boxed{43}$	~~44~~	~~45~~	~~46~~	$\boxed{47}$	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	$\boxed{53}$	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	$\boxed{59}$	~~60~~
$\boxed{61}$	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	$\boxed{67}$	~~68~~	~~69~~	~~70~~
$\boxed{71}$	~~72~~	$\boxed{73}$	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	$\boxed{79}$	~~80~~
~~81~~	~~82~~	$\boxed{83}$	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	$\boxed{89}$	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	$\boxed{97}$	~~98~~	~~99~~	~~100~~

Men mag stoppen
zodra men een getal $\geq \sqrt{n}$ heeft
gemarkeerd (waarom?)

$\boxed{}$ = priemgetal

= geen priemgetal

Fundamentele stelling van de rekenkunde - priemontbinding

Elk natuurlijk getal $n \geq 2$ kan op unieke wijze geschreven worden als product van priemgetallen:

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \dots \cdot p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

Voorbeeld:

$360 = 2^3 \cdot 3^2 \cdot 5^1$

Gevolg:

Het aantal delers van n is gelijk aan $(n_1 + 1) \cdot (n_2 + 1) \cdot \dots \cdot (n_k + 1)$

Voorbeeld:

Het aantal delers van 360 is $(3 + 1) \cdot (2 + 1) \cdot (1 + 1) = 24$

Grootste gemene deler en kleinste gemene veelvoud

Grootste gemene deler van a en b

= grootste gehele getal d waarvoor $d|a$ en $d|b$

= ggd(a, b)

Kleinste gemene veelvoud van a en b

= kleinste gehele getal d waarvoor $a|d$ en $b|d$

= kgv(a, b)

Er geldt steeds:

$$\mathrm{ggd}(a, b) \cdot \mathrm{kgv}(a, b) = |a \cdot b|$$

Twee getallen a en b zijn **relatief priem** ⇔ ggd(a, b) = 1

Het algoritme van Euclides

= één van de oudste algoritmes (300 v.Chr.)
Wordt gebruikt om de ggd tussen twee gehele getallen a en b te bepalen:

1. Herhaal zolang a verschillend is van b
   1.1. Trek het kleinste getal van het grootste af
2. De gezochte ggd is nu $a = b$

Voorbeeld:

ggd(14,91) = ggd(14,77) = ggd(14,63) = ggd(14,49)
= ggd(14,35) = ggd(14,21) = ggd(14,7) = ggd(7,7) = 7

Belangrijk gevolg!

$\text{ggd}(a, b) = u \cdot a + v \cdot b \;\; (u, v \in \mathbb{Z})$ (niet uniek!)

Het algoritme van Euclides

Een **snellere variant** maakt gebruik van het delingsalgoritme

We weten dat $a = b \cdot q + r$

M.a.w. b past q keer in a

Bijgevolg: ggd(a, b) = ggd($a - \mathrm{b} \cdot q$, b) = ggd(r, b)

Bijvoorbeeld:

ggd(135,36) ?

= ggd(27,36) want $135 = 36 \cdot 3 + 27$

= ggd(9,27) want $36 = 27 \cdot 1 + 9$

= 9 want $27 = 9 \cdot 3 + 0$

Het uitgebreide algoritme van Euclides

Zoek naast de ggd ook naar de getallen u en v in de uitdrukking

$$\text{ggd}(a,\, b) = u \cdot a + v \cdot b \quad (u, v \in \mathbb{Z})$$

Voorbeeld:

Stap 1: zoek de ggd

ggd(336,1768) ?

1768 = 5·336 + 88

336 = 3·88 + 72

88 = 1·72 + 16

72 = 4·16 + 8

16 = 2·8 + 0

Dus: ggd(336,1768) = 8

Stap 2: doe dezelfde stappen in omgekeerde volgorde

8 = 72 − 4·16

= 72 − 4(88 − 1·72)

= −4·88 + 5·72

= −4·88 + 5(336 − 3·88)

= 5·336 − 19·88

= 5·336 − 19(1768 − 5·336)

= −19·1768 + 100·336

Dus: ggd(336,1768) = −19·1768 + 100·336

Het uitgebreide algoritme van Euclides

In tabelvorm (als basis voor een efficiënt computeralgoritme, niet in cursus!):

a	b	u_1	v_1	u_2	v_2
336	1768	1	0	0	1
336	88	1	0	-5	1
72	88	16	-3	-5	1
72	16	16	-3	-21	4
8	16	100	-19	-21	4
8	8	**100**	**-19**	**-121**	**23**

Hieruit lezen we dat:

$$\mathrm{ggd}(336,1768) = 8 = 100 \cdot 336 - 19 \cdot 1768 = -121 \cdot 336 + 23 \cdot 1768$$