De kunst en het nut van factoriseren

Ronald van Luijk
(Universiteit Leiden)

1 Februari, 2013
Noordwijkerhout

Vermenigvuldigen

$$\begin{array}{r} 521367 \\ 386139 \quad \times \\ \hline \end{array}$$

Vermenigvuldigen

$$\begin{array}{r} 521367 \\ 386139 \quad \times \\ \hline 4692303 \end{array}$$

Vermenigvuldigen

$$
\begin{array}{rl}
521367 & \\
386139 & \times \\
\hline
4692303 & \\
15641010 &
\end{array}
$$

Vermenigvuldigen

$$
\begin{array}{rl}
521367 & \\
386139 & \times \\
\hline
4692303 & \\
15641010 & \\
52136700 &
\end{array}
$$

Vermenigvuldigen

$$
\begin{array}{rl}
521367 & \\
386139 & \times \\
\hline
4692303 & \\
15641010 & \\
52136700 & \\
3128202000 &
\end{array}
$$

Vermenigvuldigen

$$
\begin{array}{rl}
521367 & \\
386139 & \times \\
\hline
4692303 & \\
15641010 & \\
52136700 & \\
3128202000 & \\
41709360000 &
\end{array}
$$

Vermenigvuldigen

$$
\begin{array}{rl}
521367 & \\
386139 & \times \\
\hline
4692303 & \\
15641010 & \\
52136700 & \\
3128202000 & \\
41709360000 & \\
156410100000 & + \\
\hline
\end{array}
$$

Vermenigvuldigen

$$
\begin{array}{rl}
521367 & \\
386139 & \times \\
\hline
4692303 & \\
15641010 & \\
52136700 & \\
3128202000 & \\
41709360000 & \\
156410100000 & + \\
\hline
201320132013 &
\end{array}
$$

Vermenigvuldigen

$$
\begin{array}{rl}
521367 & \\
386139 & \times \\
\hline
4692303 & \\
15641010 & \\
52136700 & \\
3128202000 & \\
41709360000 & \\
156410100000 & + \\
\hline
201320132013 &
\end{array}
$$

k^2	basisvermenigvuldigingen
$\leq 3k^2$	basisoptellingen
$\leq 4k^2$	basisoperaties.

Twee getallen van rond de k cijfers, samen $2k$ cijfers.

Vermenigvuldigen

$$
\begin{array}{rl}
521367 & \\
386139 & \times \\
\hline
4692303 & \\
15641010 & \\
52136700 & \\
3128202000 & \\
41709360000 & \\
156410100000 & + \\
\hline
201320132013 &
\end{array}
$$

k^2	basisvermenigvuldigingen
$\leq 3k^2$	basisoptellingen
$\leq 4k^2$	basisoperaties.

Twee getallen van rond de k cijfers, samen $2k$ cijfers.

"De tijd die het kost om twee getallen van k cijfers te vermenigvuldigen is kwadratisch in k."

Priemgetallen en de zeef van Eratosthenes

Definities.

1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.

Priemgetallen en de zeef van Eratosthenes

Definities.

1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Priemgetallen en de zeef van Eratosthenes

Definities.

1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Priemgetallen en de zeef van Eratosthenes

Definities.

1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Priemgetallen en de zeef van Eratosthenes

Definities.

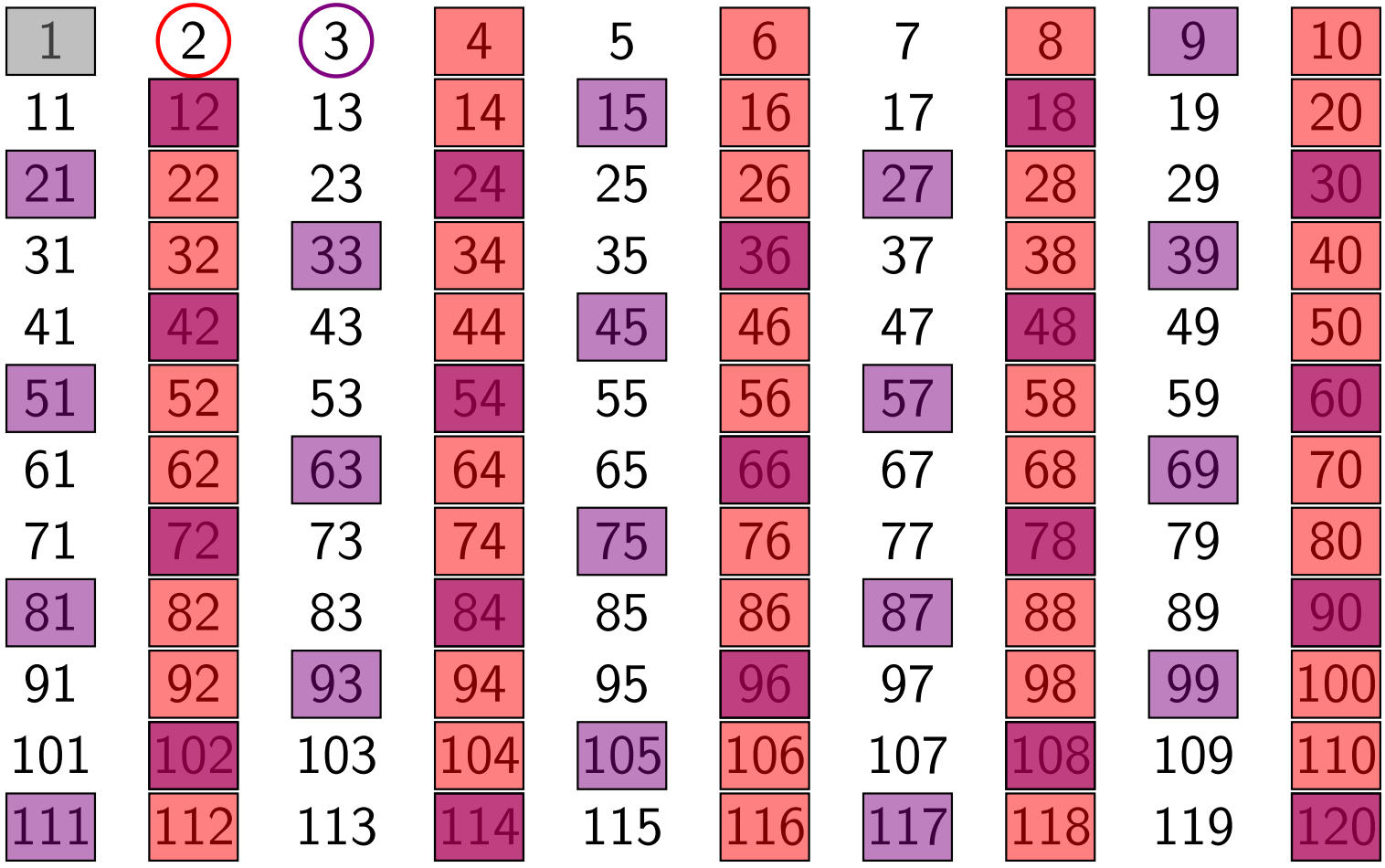
1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Priemgetallen en de zeef van Eratosthenes

Definities.

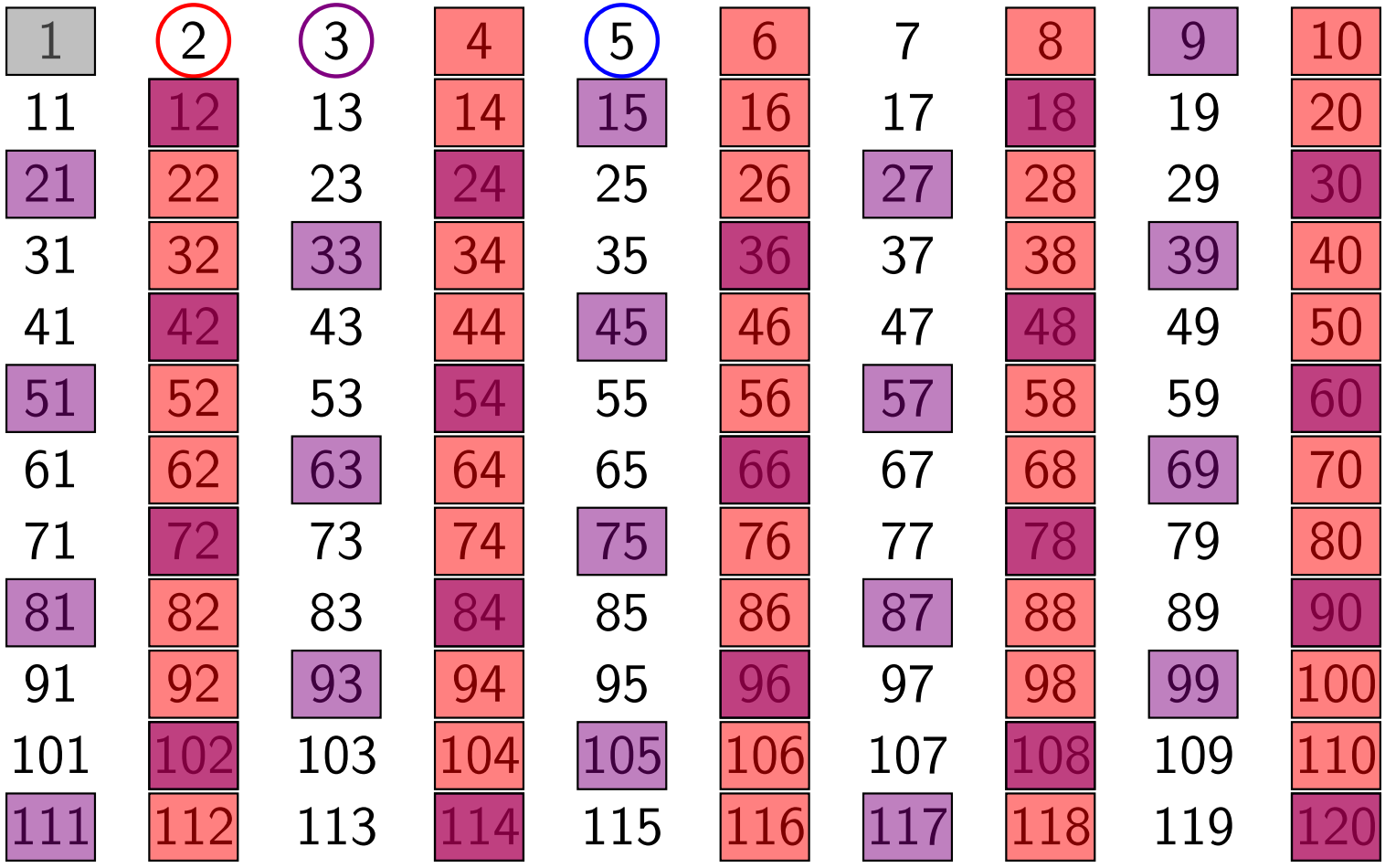
1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.



Priemgetallen en de zeef van Eratosthenes

Definities.

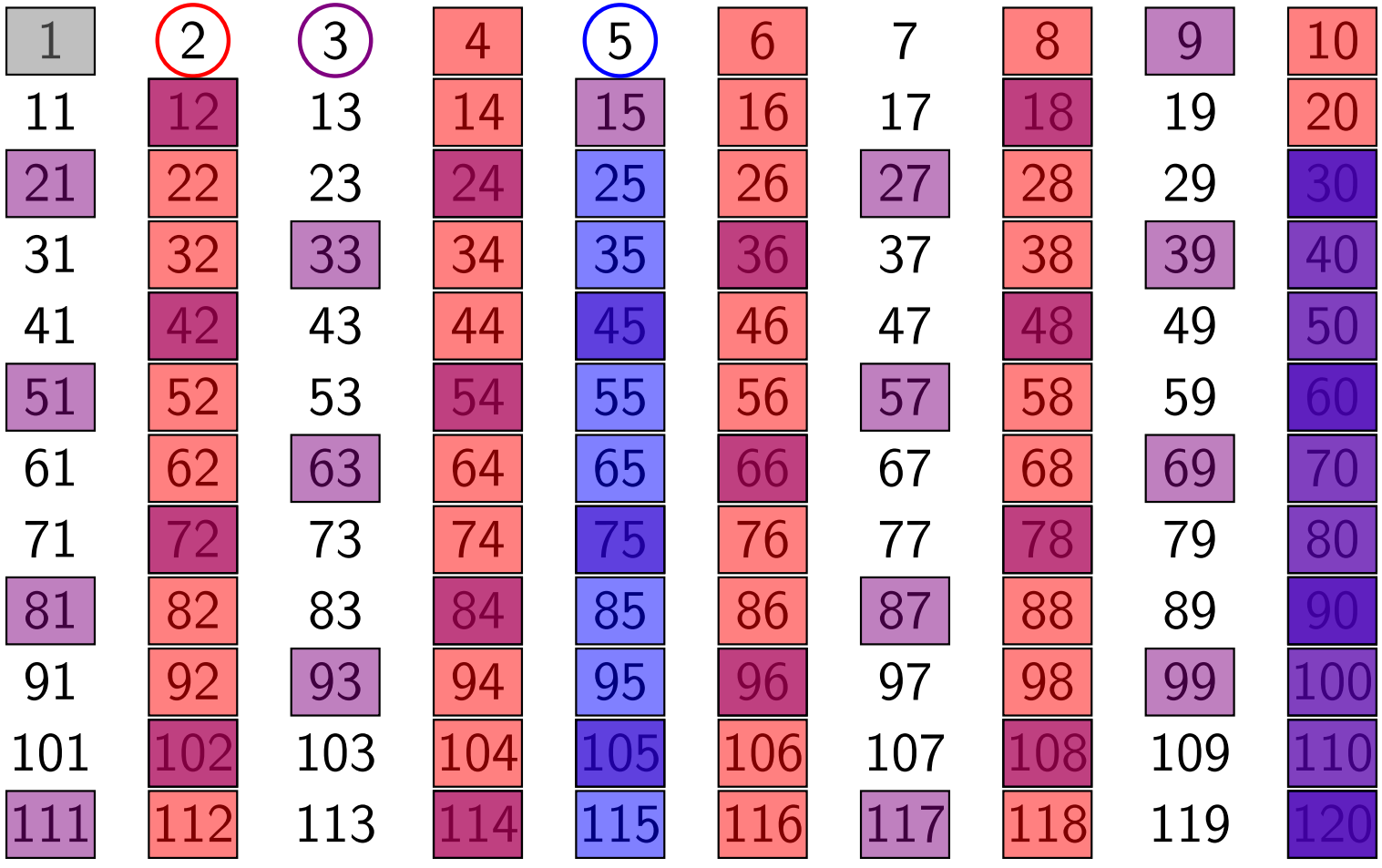
1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.



Priemgetallen en de zeef van Eratosthenes

Definities.

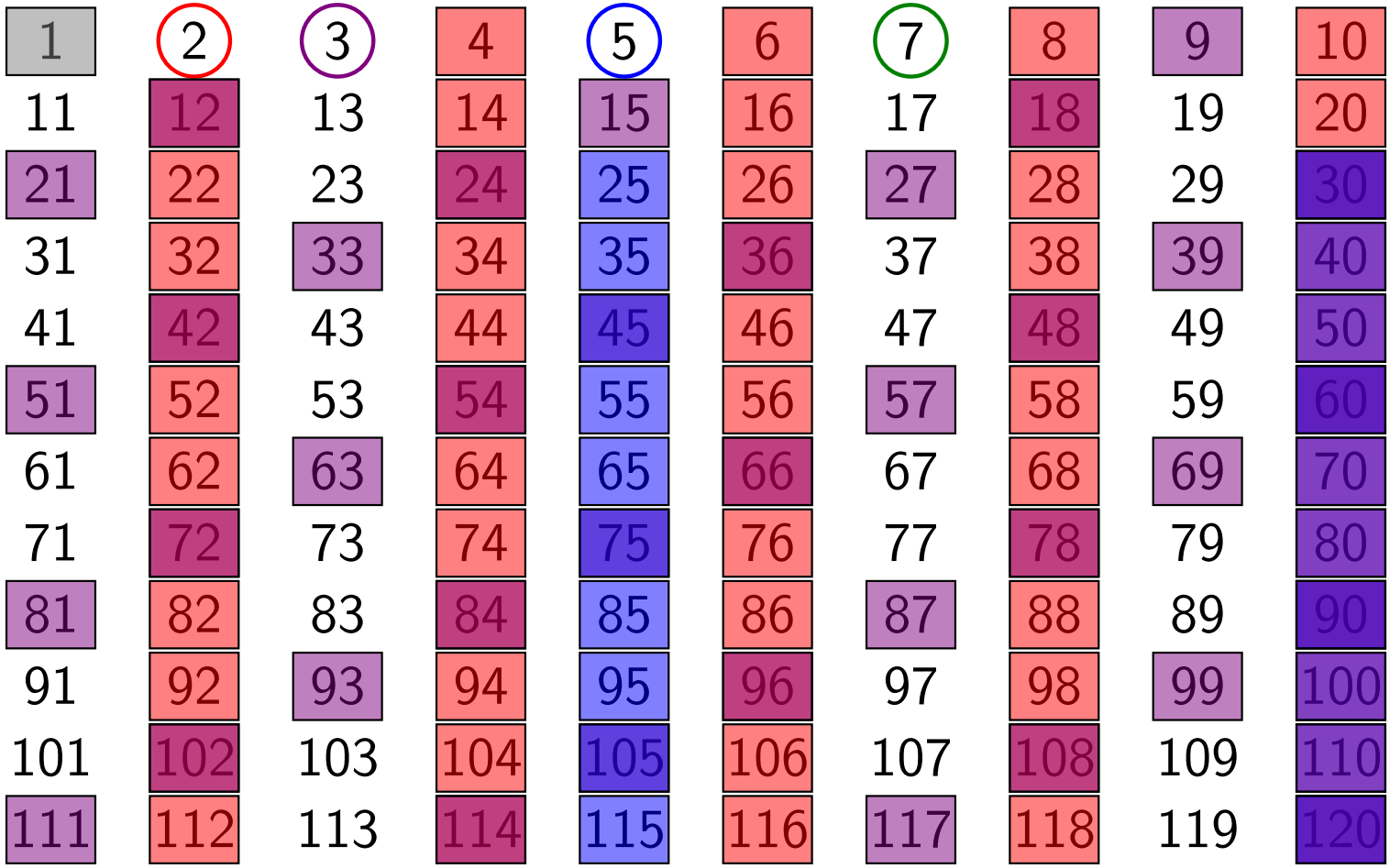
1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.



Priemgetallen en de zeef van Eratosthenes

Definities.

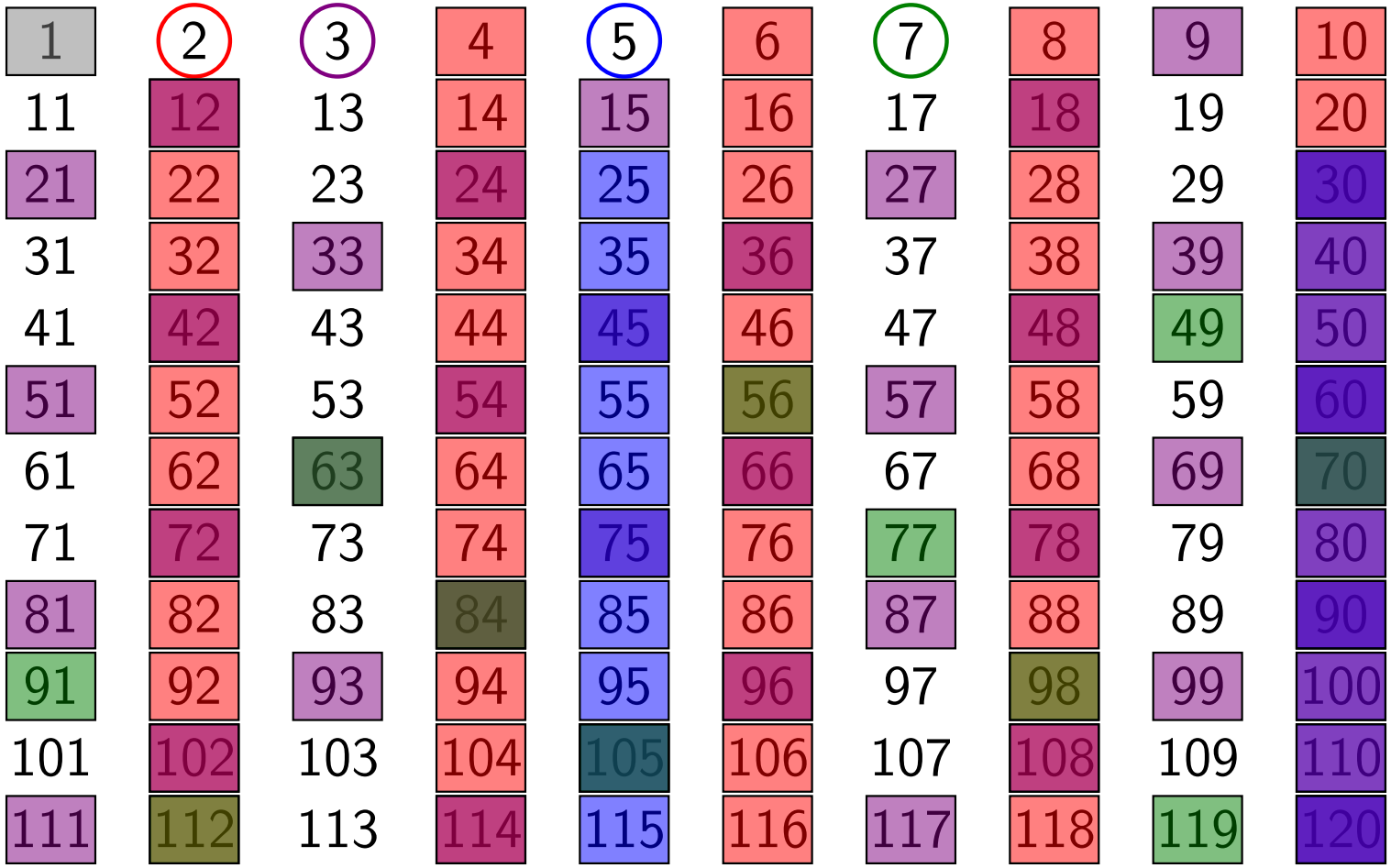
1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.



Priemgetallen en de zeef van Eratosthenes

Definities.

1. Deler: a is een deler van n als n/a geheel is. We schrijven $a|n$.
2. Priemgetal: een positief getal met precies twee positieve delers.



Hoofdstelling van de rekenkunde

Stelling. Elk positief geheel getal is op een unieke manier te ontbinden in priemgetallen.

Voorbeelden.

$$18 = 2 \times 3 \times 3 = 2 \times 3^2$$
$$60 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3 \times 5$$
$$20! = 2^{18} \times 3^8 \times 5^4 \times 7^2 \times 11 \times 13 \times 17 \times 19$$

Hoofdstelling van de rekenkunde

Stelling. Elk positief geheel getal is op een unieke manier te ontbinden in priemgetallen.

Voorbeelden.

$$18 = 2 \times 3 \times 3 = 2 \times 3^2$$

$$60 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3 \times 5$$

$$20! = 2^{18} \times 3^8 \times 5^4 \times 7^2 \times 11 \times 13 \times 17 \times 19$$

$$\underbrace{1111\ldots1}_{67} = 493121 \times 79863595778924342083 \times 28213380943176667001263153660999177245677$$

Hoofdstelling van de rekenkunde

Stelling. Elk positief geheel getal is op een unieke manier te ontbinden in priemgetallen.

Voorbeelden.

$$18 = 2 \times 3 \times 3 = 2 \times 3^2$$
$$60 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3 \times 5$$
$$20! = 2^{18} \times 3^8 \times 5^4 \times 7^2 \times 11 \times 13 \times 17 \times 19$$
$$\underbrace{1111\ldots1}_{67} = 493121 \times 7986359577892434208 3 \times 28213380943176667001263153660999177245677$$

Vragen.

1. Hoe verifiëren we de ontbinding van n? relatief makkelijk
2. Hoe vinden we de ontbinding van n? moeilijk

Modulo-rekenen

Definitie. Gehele getallen a en b zijn congruent modulo n als $a - b$ een veelvoud is van n. We schrijven $a \equiv b \mod n$.

Modulo-rekenen

Definitie. Gehele getallen a en b zijn congruent modulo n als $a - b$ een veelvoud is van n. We schrijven $a \equiv b \mod n$.

Voorbeelden.
Modulo $n = 10$ geldt

$$\begin{aligned} 83 &\equiv 3 \equiv 23 \\ 39 &\equiv 9 \equiv 19 \\ 83 \times 39 &\equiv 3 \times 9 \equiv 23 \times 19 \\ 83 + 39 &\equiv 3 + 9 \equiv 23 + 19 \end{aligned}$$

Modulo-rekenen

Definitie. Gehele getallen a en b zijn congruent modulo n als $a - b$ een veelvoud is van n. We schrijven $a \equiv b \mod n$.

Voorbeelden.
Modulo $n = 10$ geldt

$$\begin{aligned} 83 &\equiv 3 \equiv 23 \\ 39 &\equiv 9 \equiv 19 \\ 83 \times 39 &\equiv 3 \times 9 \equiv 23 \times 19 \\ 83 + 39 &\equiv 3 + 9 \equiv 23 + 19 \end{aligned}$$

Modulo $n = 7$ geldt

$$\begin{aligned} 3^3 &\equiv 27 \equiv -1 \\ 3^6 &\equiv (3^3)^2 \equiv (-1)^2 \equiv 1 \\ 3^{6k} &\equiv (3^6)^k \equiv 1^k \equiv 1 \end{aligned}$$

Priemtesten

Stelling. Zij p priem en a een geheel getal met $\mathrm{ggd}(a, p) = 1$. Dan

$$a^{p-1} \equiv 1 \mod p.$$

Priemtesten

Stelling. Zij p priem en a een geheel getal met $\mathrm{ggd}(a, p) = 1$. Dan

$$a^{p-1} \equiv 1 \mod p.$$

Gevolg. Stel a, n gehele getallen met $\mathrm{ggd}(a, n) = 1$. Als

$$a^{n-1} \not\equiv 1 \mod n,$$

dan is n niet priem.

Priemtesten

Stelling. Zij p priem en a een geheel getal met $\mathrm{ggd}(a,p)=1$. Dan

$$a^{p-1} \equiv 1 \mod p.$$

Gevolg. Stel a, n gehele getallen met $\mathrm{ggd}(a,n)=1$. Als

$$a^{n-1} \not\equiv 1 \mod n,$$

dan is n niet priem.

Voorbeeld. Is $n=65$ priem? Neem $a=2$. Modulo n geldt

$$\begin{aligned} 2^6 &= 64 \equiv -1, \\ 2^{12} &= (2^6)^2 \equiv (-1)^2 = 1, \\ 2^{64} &= (2^{12})^5 \times 2^4 \equiv 1^5 \times 16 \not\equiv 1, \end{aligned}$$

dus $n=65$ is niet priem!

Priemtesten en factoriseren

Stelling. Er is een priemtest en een constante c, zodanig dat het met die test hooguit ck^6 basisoperaties kost om van een getal van k cijfers te testen of het priem is. $ce^{6 \log k}$ (polynomiaal)

Priemtesten en factoriseren

Stelling. Er is een priemtest en een constante c, zodanig dat het met die test hooguit ck^6 basisoperaties kost om van een getal van k cijfers te testen of het priem is. $ce^{6 \log k}$ (polynomiaal)

Feit. De naïeve "trial and error" factorisatiemethode om een getal n van k cijfers te factoriseren kost in het ergste geval rond de $\sqrt{n} \sim 10^{k/2}$ basisoperaties. e^{ck} (exponentieel)

Priemtesten en factoriseren

Stelling. Er is een priemtest en een constante c, zodanig dat het met die test hooguit ck^6 basisoperaties kost om van een getal van k cijfers te testen of het priem is. $ce^{6 \log k}$ (polynomiaal)

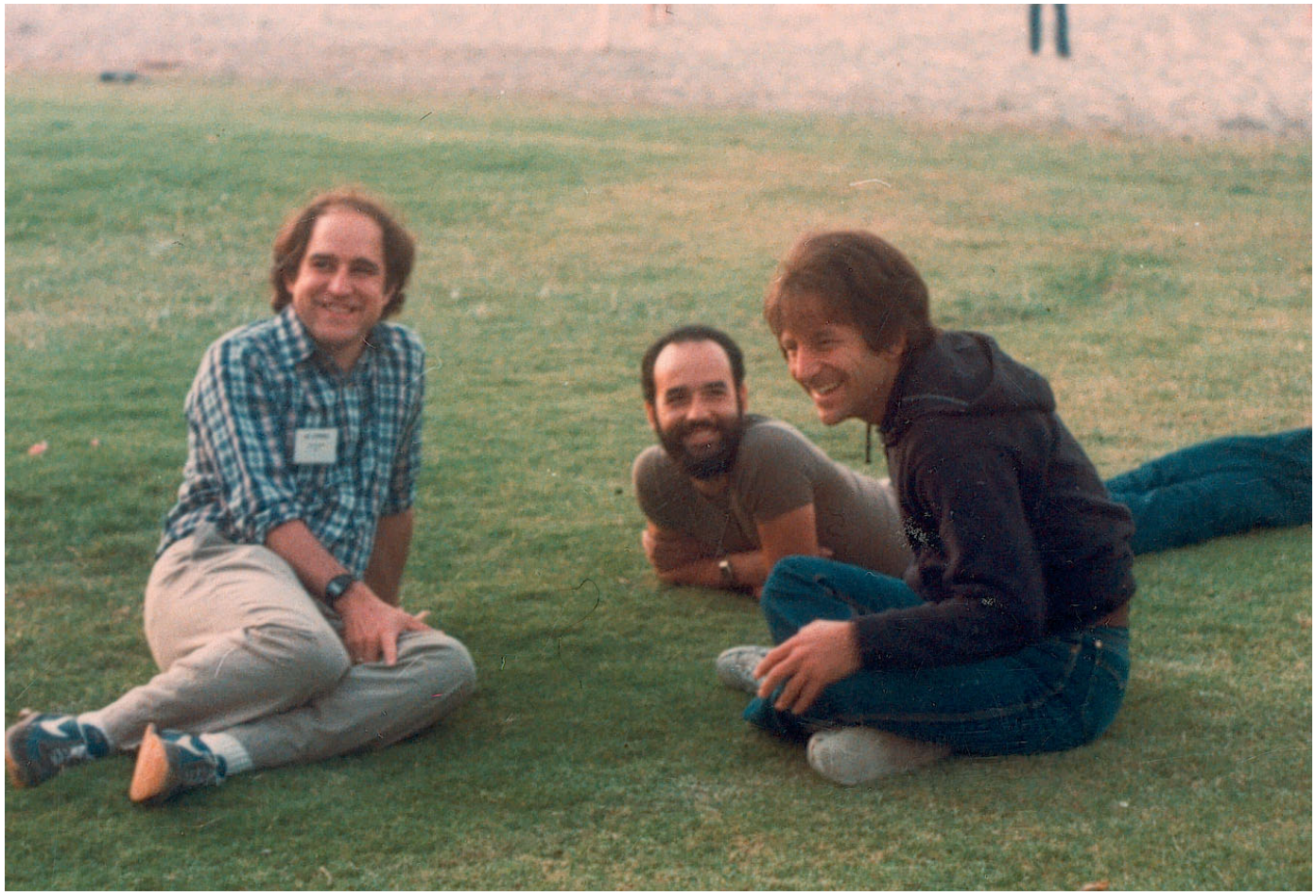
Stelling. Er is een factorisatiealgoritme om een getal van k cijfers te factoriseren dat in het ergste geval rond de $e^{ck^{1/3}(\log k)^{2/3}}$ basisoperaties kost. $e^{ck^{1/3}(\log k)^{2/3}}$ (subexponentieel)

Feit. De naïeve "trial and error" factorisatiemethode om een getal n van k cijfers te factoriseren kost in het ergste geval rond de $\sqrt{n} \sim 10^{k/2}$ basisoperaties. e^{ck} (exponentieel)

RSA (Rivest, Shamir, Adleman)

Cryptosysteem (internetbankieren) dat gebruik maakt van het feit dat factoriseren moeilijk is.

RSA (Rivest, Shamir, Adleman)



Cryptosysteem (internetbankieren) dat gebruik maakt van het feit dat factoriseren moeilijk is.
Record: 232 cijfers (768 bits), dus 'sleutels' $<$ 1024 bits niet veilig!

Alle factorisatiemethoden samengevat

Probleem. Gegeven $n = pq$, vind p en q.

Alle factorisatiemethoden samengevat

Probleem. Gegeven $n = pq$, vind p en q.

Aanpak.

1. Zoek x, y met $p|(x - y)$ **of** $q|(x - y)$.
2. Bereken de grootste gemene deler $\mathrm{ggd}(x - y, n)$.

Alle factorisatiemethoden samengevat

Probleem. Gegeven $n = pq$, vind p en q.

Aanpak.

1. Zoek x, y met $p|(x - y)$ **of** $q|(x - y)$.
2. Bereken de grootste gemene deler $\mathrm{ggd}(x - y, n)$.

Voorbeeld. We berekenen $\mathrm{ggd}(1148, 539)$.

$$\boxed{1148} = 2 \times \boxed{539} + \boxed{70}$$

Alle factorisatiemethoden samengevat

Probleem. Gegeven $n = pq$, vind p en q.

Aanpak.

1. Zoek x, y met $p|(x - y)$ **of** $q|(x - y)$.
2. Bereken de grootste gemene deler $\mathrm{ggd}(x - y, n)$.

Voorbeeld. We berekenen $\mathrm{ggd}(1148, 539)$.

$$\boxed{1148} = 2 \times \boxed{539} + \boxed{70}$$
$$\boxed{539} = 7 \times \boxed{70} + \boxed{49}$$

Alle factorisatiemethoden samengevat

Probleem. Gegeven $n = pq$, vind p en q.

Aanpak.

1. Zoek x, y met $p|(x - y)$ **of** $q|(x - y)$.
2. Bereken de grootste gemene deler $\mathrm{ggd}(x - y, n)$.

Voorbeeld. We berekenen $\mathrm{ggd}(1148, 539)$.

$$\begin{aligned} 1148 &= 2 \times 539 + 70 \\ 539 &= 7 \times 70 + 49 \\ 70 &= 1 \times 49 + 21 \end{aligned}$$

Alle factorisatiemethoden samengevat

Probleem. Gegeven $n = pq$, vind p en q.

Aanpak.

1. Zoek x, y met $p|(x - y)$ **of** $q|(x - y)$.
2. Bereken de grootste gemene deler $\mathrm{ggd}(x - y, n)$.

Voorbeeld. We berekenen $\mathrm{ggd}(1148, 539)$.

$$\begin{aligned} 1148 &= 2 \times 539 + 70 \\ 539 &= 7 \times 70 + 49 \\ 70 &= 1 \times 49 + 21 \\ 49 &= 2 \times 21 + 7 \end{aligned}$$

Alle factorisatiemethoden samengevat

Probleem. Gegeven $n = pq$, vind p en q.

Aanpak.

1. Zoek x, y met $p|(x - y)$ **of** $q|(x - y)$.
2. Bereken de grootste gemene deler $\mathrm{ggd}(x - y, n)$.

Voorbeeld. We berekenen $\mathrm{ggd}(1148, 539)$.

$$\begin{aligned}
1148 &= 2 \times 539 + 70 \\
539 &= 7 \times 70 + 49 \\
70 &= 1 \times 49 + 21 \\
49 &= 2 \times 21 + 7 \\
21 &= 3 \times 7
\end{aligned}$$

Alle factorisatiemethoden samengevat

Probleem. Gegeven $n = pq$, vind p en q.

Aanpak.

1. Zoek x, y met $p|(x - y)$ **of** $q|(x - y)$.
2. Bereken de grootste gemene deler $\mathrm{ggd}(x - y, n)$.

Voorbeeld. We berekenen $\mathrm{ggd}(1148, 539)$.

$$
\begin{aligned}
1148 &= 2 \times 539 + 70 \\
539 &= 7 \times 70 + 49 \\
70 &= 1 \times 49 + 21 \\
49 &= 2 \times 21 + 7 \\
21 &= 3 \times 7
\end{aligned}
$$

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Birthday paradox.
Trekken we $\sqrt{2p \log 2}$ getallen uit $\{0, 1, 2, \ldots, p-1\}$,
dan is de kans 50% dat er een dubbele tussen zit.

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Birthday paradox.
Trekken we $\sqrt{2p \log 2}$ getallen uit $\{0, 1, 2, \ldots, p-1\}$,
dan is de kans 50% dat er een dubbele tussen zit.

Gevolg. Gegeven $\sqrt{2p \log 2} \sim \sqrt{p}$ getallen is de
kans 50% dat er twee congruent zijn modulo p.

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Birthday paradox.
Trekken we $\sqrt{2p \log 2}$ getallen uit $\{0, 1, 2, \ldots, p-1\}$,
dan is de kans 50% dat er een dubbele tussen zit.

Gevolg. Gegeven $\sqrt{2p \log 2} \sim \sqrt{p}$ getallen is de
kans 50% dat er twee congruent zijn modulo p.

Aanpak. Gegeven $n = pq$ met p, q onbekend en $p < \sqrt{n} < q$.
1. Selecteer $\sqrt[4]{n} > \sqrt{p}$ getallen modulo n.
2. Zoek x, y met $x \equiv y \mod p$, dus met $\mathrm{ggd}(x - y, n) > 1$.

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Birthday paradox.
Trekken we $\sqrt{2p \log 2}$ getallen uit $\{0, 1, 2, \ldots, p-1\}$,
dan is de kans 50% dat er een dubbele tussen zit.

Gevolg. Gegeven $\sqrt{2p \log 2} \sim \sqrt{p}$ getallen is de
kans 50% dat er twee congruent zijn modulo p.

Aanpak. Gegeven $n = pq$ met p, q onbekend en $p < \sqrt{n} < q$.
1. Selecteer $\sqrt[4]{n} > \sqrt{p}$ getallen modulo n.
2. Zoek x, y met $x \equiv y \mod p$, dus met $\mathrm{ggd}(x - y, n) > 1$.

Probleem. Er zijn $\sqrt[4]{n} \times \sqrt[4]{n} = \sqrt{n}$ paren te testen...

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Birthday paradox.
Trekken we $\sqrt{2p \log 2}$ getallen uit $\{0, 1, 2, \ldots, p-1\}$,
dan is de kans 50% dat er een dubbele tussen zit.

Gevolg. Gegeven $\sqrt{2p \log 2} \sim \sqrt{p}$ getallen is de
kans 50% dat er twee congruent zijn modulo p.

Aanpak. Gegeven $n = pq$ met p, q onbekend en $p < \sqrt{n} < q$.
1. Selecteer $\sqrt[4]{n} > \sqrt{p}$ getallen modulo n.
2. Zoek x, y met $x \equiv y \mod p$, dus met $\mathrm{ggd}(x - y, n) > 1$.

Probleem. Er zijn $\sqrt[4]{n} \times \sqrt[4]{n} = \sqrt{n}$ paren te testen...

Oplossing. Kies de $\sqrt[4]{n}$ getallen niet volledig willekeurig!

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

$x_j \mod n$

$x_0 = 2$
$x_1 = 8$
$x_2 = 68$
$x_3 = 104$
$x_4 = 264$
$x_5 = 332$
$x_6 = 144$
$x_7 = 5$
$x_8 = 29$
$x_9 = 91$
$x_{10} = 368$
$x_{11} = 85$
$x_{12} = 66$

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

$x_j \mod n$	$x_j \mod 13$
$x_0 = 2$	
$x_1 = 8$	
$x_2 = 68$	
$x_3 = 104$	
$x_4 = 264$	
$x_5 = 332$	
$x_6 = 144$	8
$x_7 = 5$	$\uparrow$
$x_8 = 29$	
$x_9 = 91$	2
$x_{10} = 368$	
$x_{11} = 85$	
$x_{12} = 66$	

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

$x_j \mod n$	$x_j \mod 13$
$x_0 = 2$	
$x_1 = 8$	
$x_2 = 68$	
$x_3 = 104$	
$x_4 = 264$	3
$x_5 = 332$	$\uparrow$
$x_6 = 144$	8
$x_7 = 5$	$\uparrow$
$x_8 = 29$	
$x_9 = 91$	2
$x_{10} = 368$	
$x_{11} = 85$	
$x_{12} = 66$	

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

$x_j \mod n$	$x_j \mod 13$
$x_0 = 2$	
$x_1 = 8$	0
$x_2 = 68$	$\uparrow$
$x_3 = 104$	
$x_4 = 264$	3
$x_5 = 332$	$\uparrow$
$x_6 = 144$	
$x_7 = 5$	8
$x_8 = 29$	$\uparrow$
$x_9 = 91$	
$x_{10} = 368$	2
$x_{11} = 85$	
$x_{12} = 66$	

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

$x_j \mod n$	$x_j \mod 13$
$x_0 = 2$	4
$x_1 = 8$	0 ↗
$x_2 = 68$	↑
$x_3 = 104$	3
$x_4 = 264$	↑
$x_5 = 332$	8
$x_6 = 144$	↑
$x_7 = 5$	2
$x_8 = 29$	
$x_9 = 91$	
$x_{10} = 368$	
$x_{11} = 85$	
$x_{12} = 66$	

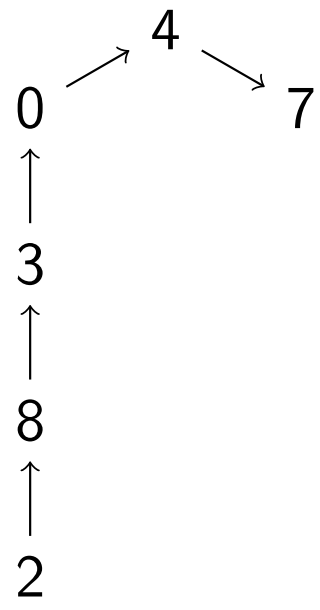
Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

$x_j \mod n$	$x_j \mod 13$
$x_0 = 2$	
$x_1 = 8$	
$x_2 = 68$	
$x_3 = 104$	
$x_4 = 264$	
$x_5 = 332$	
$x_6 = 144$	
$x_7 = 5$	
$x_8 = 29$	
$x_9 = 91$	
$x_{10} = 368$	
$x_{11} = 85$	
$x_{12} = 66$	

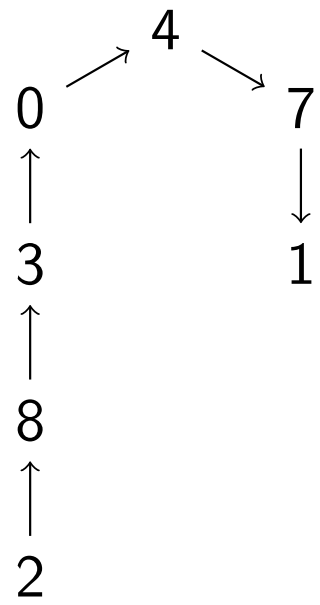


Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

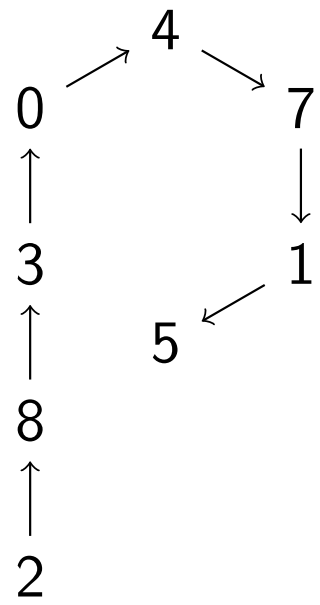
$x_j \mod n$	$x_j \mod 13$
$x_0 = 2$	
$x_1 = 8$	
$x_2 = 68$	
$x_3 = 104$	
$x_4 = 264$	
$x_5 = 332$	
$x_6 = 144$	
$x_7 = 5$	
$x_8 = 29$	
$x_9 = 91$	
$x_{10} = 368$	
$x_{11} = 85$	
$x_{12} = 66$	

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

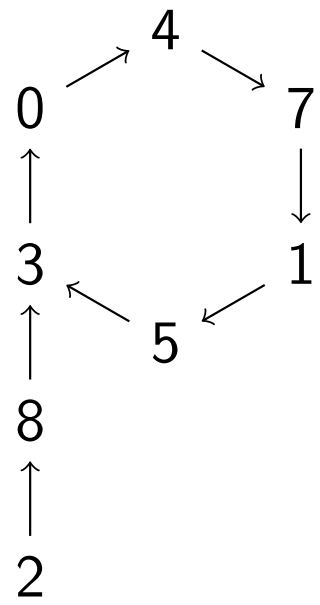
$x_j \mod n$	$x_j \mod 13$
$x_0 = 2$	
$x_1 = 8$	
$x_2 = 68$	
$x_3 = 104$	
$x_4 = 264$	
$x_5 = 332$	
$x_6 = 144$	
$x_7 = 5$	
$x_8 = 29$	
$x_9 = 91$	
$x_{10} = 368$	
$x_{11} = 85$	
$x_{12} = 66$	

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

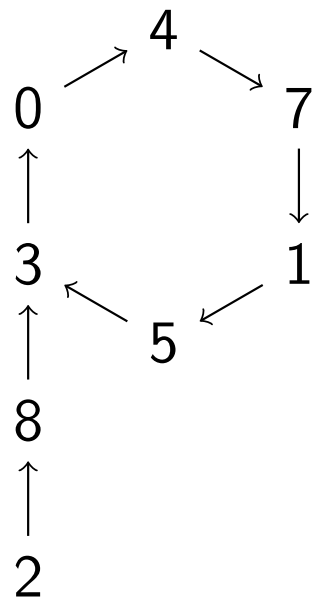
$x_j \mod n$	$x_j \mod 13$
$x_0 = 2$	
$x_1 = 8$	
$x_2 = 68$	
$x_3 = 104$	
$x_4 = 264$	
$x_5 = 332$	
$x_6 = 144$	
$x_7 = 5$	
$x_8 = 29$	
$x_9 = 91$	
$x_{10} = 368$	
$x_{11} = 85$	
$x_{12} = 66$	

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

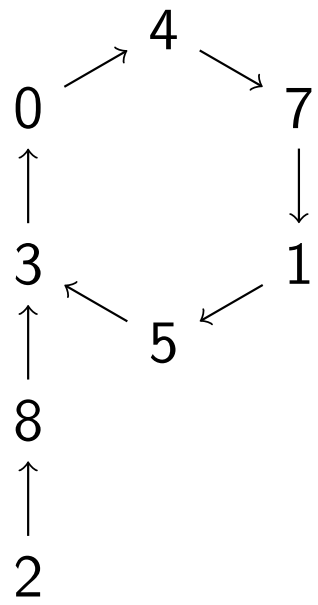
$x_j \mod n$	$x_j \mod 13$	mod 13
$x_0 = 2$ $x_1 = 8$ $x_2 = 68$ $x_3 = 104$ $x_4 = 264$ $x_5 = 332$ $x_6 = 144$ $x_7 = 5$ $x_8 = 29$ $x_9 = 91$ $x_{10} = 368$ $x_{11} = 85$ $x_{12} = 66$		$x_2 \equiv x_8$

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

$x_j \mod n$	$x_j \mod 13$	mod 13
$x_0 = 2$		$x_2 \equiv x_8$
$x_1 = 8$		$x_3 \equiv x_9$
$x_2 = 68$		$x_4 \equiv x_{10}$
$x_3 = 104$		$x_5 \equiv x_{11}$
$x_4 = 264$		$x_6 \equiv x_{12}$
$x_5 = 332$		$x_7 \equiv x_{13}$
$x_6 = 144$		
$x_7 = 5$		
$x_8 = 29$		
$x_9 = 91$		
$x_{10} = 368$		
$x_{11} = 85$		
$x_{12} = 66$		

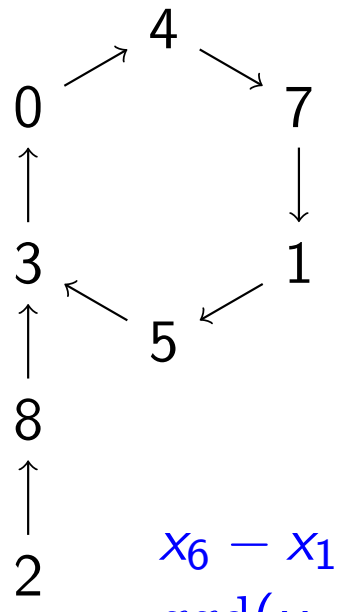
$x_j \equiv x_{2j}$

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Voorbeeld. $n = 377 \ (= 13 \times 29)$.

$x_0 = 2$

$x_{j+1} = x_j^2 + 4 \mod n$

$x_j \mod n$	$x_j \mod 13$	mod 13
$x_0 = 2$		$x_2 \equiv x_8$
$x_1 = 8$		$x_3 \equiv x_9$
$x_2 = 68$		$x_4 \equiv x_{10}$
$x_3 = 104$		$x_5 \equiv x_{11}$
$x_4 = 264$		$x_6 \equiv x_{12}$
$x_5 = 332$		$x_7 \equiv x_{13}$
$x_6 = 144$		
$x_7 = 5$		
$x_8 = 29$		
$x_9 = 91$		
$x_{10} = 368$		
$x_{11} = 85$		
$x_{12} = 66$		

$x_j \equiv x_{2j}$

$x_6 - x_{12} = 144 - 66 = 78$

$\gcd(x_6 - x_{12}, n) = \gcd(78, 377) = 13$

Pollard rho $\sqrt[4]{n} \sim 10^{k/4}$ (exponentieel)

Uiteindelijke algoritme.

Input: n.

Kies x_0, c.

$f(a) := a^2 + c$.

$x := x_0$.

$y := x_0$.

Repeat

$x := f(x)$.

$y := f(f(y))$.

$d := \mathrm{ggd}(x - y, n)$.

until $d > 1$.

Return d.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 1. Factoriseer $n = 247$.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 1. Factoriseer $n = 247$.

$247 = 256 - 9 = 16^2 - 3^2 = (16 - 3) \times (16 + 3) = 13 \times 19.$

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 1. Factoriseer $n = 247$.
$247 = 256 - 9 = 16^2 - 3^2 = (16 - 3) \times (16 + 3) = 13 \times 19$.

Les. Als $n = pq$ een deler is van $x^2 - y^2 = (x - y)(x + y)$, dan zijn de priemen p en q een deler van $x - y$ of $x + y$.
Met 50% kans is $\mathrm{ggd}(x - y, n)$ een priemdeler van n.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 1. Factoriseer $n = 247$.
$247 = 256 - 9 = 16^2 - 3^2 = (16 - 3) \times (16 + 3) = 13 \times 19$.

Les. Als $n = pq$ een deler is van $x^2 - y^2 = (x - y)(x + y)$, dan zijn de priemen p en q een deler van $x - y$ of $x + y$.
Met 50% kans is $\mathrm{ggd}(x - y, n)$ een priemdeler van n.

Voorbeeld 2. Factoriseer $n = 133$.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 1. Factoriseer $n = 247$.
$247 = 256 - 9 = 16^2 - 3^2 = (16 - 3) \times (16 + 3) = 13 \times 19$.

Les. Als $n = pq$ een deler is van $x^2 - y^2 = (x - y)(x + y)$, dan zijn de priemen p en q een deler van $x - y$ of $x + y$.
Met 50% kans is $\mathrm{ggd}(x - y, n)$ een priemdeler van n.

Voorbeeld 2. Factoriseer $n = 133$.
Er geldt $2^7 + 5 = 133 = 5^3 + 2^3$, dus modulo 133 geldt

$$2^7 \equiv -5,$$
$$5^3 \equiv -2^3,$$
$$2 \times 5 \equiv 2 \times 5,$$

dus ook $2^8 \times 5^4 \equiv 2^4 \times 5^2$, dus $400^2 \equiv 20^2$.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 1. Factoriseer $n = 247$.
$247 = 256 - 9 = 16^2 - 3^2 = (16 - 3) \times (16 + 3) = 13 \times 19$.

Les. Als $n = pq$ een deler is van $x^2 - y^2 = (x - y)(x + y)$, dan zijn de priemen p en q een deler van $x - y$ of $x + y$.
Met 50% kans is $\mathrm{ggd}(x - y, n)$ een priemdeler van n.

Voorbeeld 2. Factoriseer $n = 133$.
Er geldt $2^7 + 5 = 133 = 5^3 + 2^3$, dus modulo 133 geldt

$$2^7 \equiv -5,$$
$$5^3 \equiv -2^3,$$
$$2 \times 5 \equiv 2 \times 5,$$

dus ook $2^8 \times 5^4 \equiv 2^4 \times 5^2$, dus $400^2 \equiv 20^2$.
We vinden $\mathrm{ggd}(400 - 20, 133) = 19$ en $133 = 7 \times 19$.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 3. Factoriseer $n = 119$.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 3. Factoriseer $n = 119$.

1. Kies een priemgrens: $P = 5$.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 3. Factoriseer $n = 119$.

1. Kies een priemgrens: $P = 5$.
2. Zeef priemfactoren $\leq P$ uit getallen in interval rond n.

$$2^3 \times 3 \times 5 = 120$$
$$? = 121$$
$$2 \times ? = 122$$
$$3 \times ? = 123$$
$$2^2 \times ? = 124$$
$$5^3 = 125$$
$$2 \times 3^3 \times ? = 126$$
$$? = 127$$
$$2^7 = 128$$
$$\vdots$$
$$3^3 \times 5 = 135$$

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 3. Factoriseer $n = 119$.

1. Kies een priemgrens: $P = 5$.
2. Zeef priemfactoren $\leq P$ uit getallen in interval rond n.

$$\begin{aligned} 2^3 \times 3 \times 5 &= 120 \equiv 1 \\ 5^3 &= 125 \equiv 2 \times 3 \\ 2^7 &= 128 \equiv 3^2 \\ 3^3 \times 5 &= 135 \equiv 2^4 \\ 2 \times 3 &= \quad 6 \equiv 2 \times 3 \end{aligned}$$

3. Voeg triviale relaties toe en factoriseer de resten van de volledig gefactoriseerde getallen.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 3. Factoriseer $n = 119$.

1. Kies een priemgrens: $P = 5$.
2. Zeef priemfactoren $\leq P$ uit getallen in interval rond n.

$$\begin{aligned} 2^3 \times 3 \times 5 &= 120 \equiv 1 \\ 5^3 &= 125 \equiv 2 \times 3 \\ 2^7 &= 128 \equiv 3^2 \\ 3^3 \times 5 &= 135 \equiv 2^4 \\ 2 \times 3 &= \quad 6 \equiv 2 \times 3 \end{aligned}$$

3. Voeg triviale relaties toe en factoriseer de resten van de volledig gefactoriseerde getallen.
4. Selecteer relaties die vermenigvuldigen tot $\square \equiv \square$.
   Rijen 1,2 en 5 geven $2^4 \times 3^2 \times 5^4 \equiv 2^2 \times 3^2$, dus $300^2 \equiv 6^2$.

Kwadratische zeef $e^{c\sqrt{k \log k}}$ (subexponentieel)

Voorbeeld 3. Factoriseer $n = 119$.

1. Kies een priemgrens: $P = 5$.
2. Zeef priemfactoren $\leq P$ uit getallen in interval rond n.

$$\begin{aligned} 2^3 \times 3 \times 5 &= 120 \equiv 1 \\ 5^3 &= 125 \equiv 2 \times 3 \\ 2^7 &= 128 \equiv 3^2 \\ 3^3 \times 5 &= 135 \equiv 2^4 \\ 2 \times 3 &= \quad 6 \equiv 2 \times 3 \end{aligned}$$

3. Voeg triviale relaties toe en factoriseer de resten van de volledig gefactoriseerde getallen.
4. Selecteer relaties die vermenigvuldigen tot $\square \equiv \square$. Rijen 1,2 en 5 geven $2^4 \times 3^2 \times 5^4 \equiv 2^2 \times 3^2$, dus $300^2 \equiv 6^2$.
5. Bereken grootste gemene deler $\mathrm{ggd}(300 - 6, n) = 7$ en concludeer $n = 7 \times 17$.

Kwadratische zeef (selectie van de relaties)

$$2^3 \times 3 \times 5 = 120 \equiv 1$$

$$5^3 = 125 \equiv 2 \times 3$$

$$2^7 = 128 \equiv 3^2$$

$$3^3 \times 5 = 135 \equiv 2^4$$

$$2 \times 3 = \quad 6 \equiv 2 \times 3$$

Kwadratische zeef (selectie van de relaties)

$$2^3 \times 3 \times 5 = 120 \equiv 1$$
$$5^3 = 125 \equiv 2 \times 3$$
$$2^7 = 128 \equiv 3^2$$
$$3^3 \times 5 = 135 \equiv 2^4$$
$$2 \times 3 = \quad 6 \equiv 2 \times 3$$

$$\left(\begin{array}{ccc|c|cc} 3 & 1 & 1 & & 0 & 0 \\ 0 & 0 & 3 & & 1 & 1 \\ 7 & 0 & 0 & & 0 & 2 \\ 0 & 3 & 1 & & 4 & 0 \\ 1 & 1 & 0 & & 1 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c|cc} 1 & 1 & 1 & & 0 & 0 \\ 0 & 0 & 1 & & 1 & 1 \\ 1 & 0 & 0 & & 0 & 0 \\ 0 & 1 & 1 & & 0 & 0 \\ 1 & 1 & 0 & & 1 & 1 \end{array}\right) = M$$

Met de regel $1 + 1 = 0$ zoeken we naar rijen met som 0.

Kwadratische zeef (selectie van de relaties)

$$2^3 \times 3 \times 5 = 120 \equiv 1$$
$$5^3 = 125 \equiv 2 \times 3$$
$$2^7 = 128 \equiv 3^2$$
$$3^3 \times 5 = 135 \equiv 2^4$$
$$2 \times 3 = \quad 6 \equiv 2 \times 3$$

$$\left(\begin{array}{ccc|c|cc} 3 & 1 & 1 & & 0 & 0 \\ 0 & 0 & 3 & & 1 & 1 \\ 7 & 0 & 0 & & 0 & 2 \\ 0 & 3 & 1 & & 4 & 0 \\ 1 & 1 & 0 & & 1 & 1 \end{array}\right) \quad \rightsquigarrow \quad \left(\begin{array}{ccc|c|cc} 1 & 1 & 1 & & 0 & 0 \\ 0 & 0 & 1 & & 1 & 1 \\ 1 & 0 & 0 & & 0 & 0 \\ 0 & 1 & 1 & & 0 & 0 \\ 1 & 1 & 0 & & 1 & 1 \end{array}\right) = M$$

Met de regel $1 + 1 = 0$ zoeken we naar rijen met som 0.
De oplossingen corresponderen met elementen van de kern van M^{t}!

Kwadratische zeef (selectie van de relaties)

Niet in voordracht. Je kunt modulo n ook delen door kleine priemen. Delen door rechterkant geeft kleinere matrices. Triviale relaties niet meer nodig.

$$2^3 \times 3 \times 5 = 120 \equiv 1$$
$$5^3 = 125 \equiv 2 \times 3$$
$$2^7 = 128 \equiv 3^2$$
$$3^3 \times 5 = 135 \equiv 2^4$$
$$2 \times 3 = 6 \equiv 2 \times 3$$

$$\begin{pmatrix} 3 & 1 & 1 \\ -1 & -1 & 3 \\ 7 & -2 & 0 \\ -4 & 3 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\left(\begin{array}{ccc|cc} 3 & 1 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 & 1 \\ 7 & 0 & 0 & 0 & 2 \\ 0 & 3 & 1 & 4 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|cc} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{array}\right) = M$$

Met de regel $1 + 1 = 0$ zoeken we naar rijen met som 0.
De oplossingen corresponderen met elementen van de kern van M^{t}!

Kwadratische zeef (selectie van de relaties)

$$2^3 \times 3 \times 5 = 120 \equiv 1$$
$$5^3 = 125 \equiv 2 \times 3$$
$$2^7 = 128 \equiv 3^2$$
$$3^3 \times 5 = 135 \equiv 2^4$$
$$2 \times 3 = 6 \equiv 2 \times 3$$

Niet in voordracht. Je kunt modulo n ook delen door kleine priemen. Delen door rechterkant geeft kleinere matrices. Triviale relaties niet meer nodig.

$$\begin{pmatrix} 3 & 1 & 1 \\ -1 & -1 & 3 \\ 7 & -2 & 0 \\ -4 & 3 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\left(\begin{array}{ccc|cc} 3 & 1 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 & 1 \\ 7 & 0 & 0 & 0 & 2 \\ 0 & 3 & 1 & 4 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|cc} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{array}\right) = M$$

Met de regel $1 + 1 = 0$ zoeken we naar rijen met som 0.
De oplossingen corresponderen met elementen van de kern van M^{t}!

Record: 135 cijfers (meer dan half miljoen “kleine” priemen.)

Andere sterke algoritmes

- De elliptische krommen methode.
- De getallenlichamenzeef (number field seive). Recordhouder

RSA

1. Bob kiest geheime priemen p en q.
2. Bob berekent publieke $n{=}pq$.

RSA

1. Bob kiest geheime priemen p en q.
2. Bob berekent publieke $n{=}pq$.
3. Bob kiest publieke exponent d.
4. Bob berekent geheime e zodat $de \equiv 1 \mod (p-1)(q-1)$.

RSA

1. Bob kiest geheime priemen p en q.
2. Bob berekent publieke $n{=}pq$.
3. Bob kiest publieke exponent d.
4. Bob berekent geheime e zodat $de \equiv 1 \mod (p-1)(q-1)$.

Nu geldt voor elke M met $\mathrm{ggd}(M, n) = 1$:

$$M^{p-1} \equiv 1 \mod p$$
$$M^{q-1} \equiv 1 \mod q$$

RSA

1. Bob kiest geheime priemen p en q.
2. Bob berekent publieke $n{=}pq$.
3. Bob kiest publieke exponent d.
4. Bob berekent geheime e zodat $de \equiv 1 \mod (p-1)(q-1)$.

Nu geldt voor elke M met $\mathrm{ggd}(M, n) = 1$:

$$M^{p-1} \equiv 1 \mod p$$
$$M^{q-1} \equiv 1 \mod q$$
$$M^{(p-1)(q-1)} \equiv 1 \mod p$$

RSA

1. Bob kiest geheime priemen p en q.
2. Bob berekent publieke $n{=}pq$.
3. Bob kiest publieke exponent d.
4. Bob berekent geheime e zodat $de \equiv 1 \mod (p-1)(q-1)$.

Nu geldt voor elke M met $\mathrm{ggd}(M, n) = 1$:

$$\begin{aligned} M^{p-1} &\equiv 1 \mod p \\ M^{q-1} &\equiv 1 \mod q \\ M^{(p-1)(q-1)} &\equiv 1 \mod p \\ M^{(p-1)(q-1)} &\equiv 1 \mod q \end{aligned}$$

RSA

1. Bob kiest geheime priemen p en q.
2. Bob berekent publieke $n{=}pq$.
3. Bob kiest publieke exponent d.
4. Bob berekent geheime e zodat $de \equiv 1 \mod (p-1)(q-1)$.

Nu geldt voor elke M met $\mathrm{ggd}(M, n) = 1$:

$$
\begin{aligned}
M^{p-1} &\equiv 1 \mod p \\
M^{q-1} &\equiv 1 \mod q \\
M^{(p-1)(q-1)} &\equiv 1 \mod p \\
M^{(p-1)(q-1)} &\equiv 1 \mod q \\
M^{(p-1)(q-1)} &\equiv 1 \mod n
\end{aligned}
$$

RSA

1. Bob kiest geheime priemen p en q.
2. Bob berekent publieke $n{=}pq$.
3. Bob kiest publieke exponent d.
4. Bob berekent geheime e zodat $de \equiv 1 \mod (p-1)(q-1)$.

Nu geldt voor elke M met $\mathrm{ggd}(M, n) = 1$:

$$
\begin{aligned}
M^{p-1} &\equiv 1 \mod p \\
M^{q-1} &\equiv 1 \mod q \\
M^{(p-1)(q-1)} &\equiv 1 \mod p \\
M^{(p-1)(q-1)} &\equiv 1 \mod q \\
M^{(p-1)(q-1)} &\equiv 1 \mod n \\
M^{de-1} &\equiv 1 \mod n
\end{aligned}
$$

RSA

1. Bob kiest geheime priemen p en q.
2. Bob berekent publieke $n{=}pq$.
3. Bob kiest publieke exponent d.
4. Bob berekent geheime e zodat $de \equiv 1 \mod (p-1)(q-1)$.

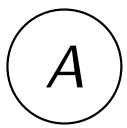
Nu geldt voor elke M met $\mathrm{ggd}(M, n) = 1$:

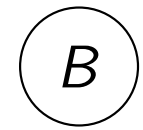
$$
\begin{aligned}
M^{p-1} &\equiv 1 \mod p \\
M^{q-1} &\equiv 1 \mod q \\
M^{(p-1)(q-1)} &\equiv 1 \mod p \\
M^{(p-1)(q-1)} &\equiv 1 \mod q \\
M^{(p-1)(q-1)} &\equiv 1 \mod n \\
M^{de-1} &\equiv 1 \mod n \\
(M^d)^e = M^{de} &\equiv M \mod n.
\end{aligned}
$$

RSA

$n = pq$

$de \equiv 1 \mod (p-1)(q-1)$





M

RSA

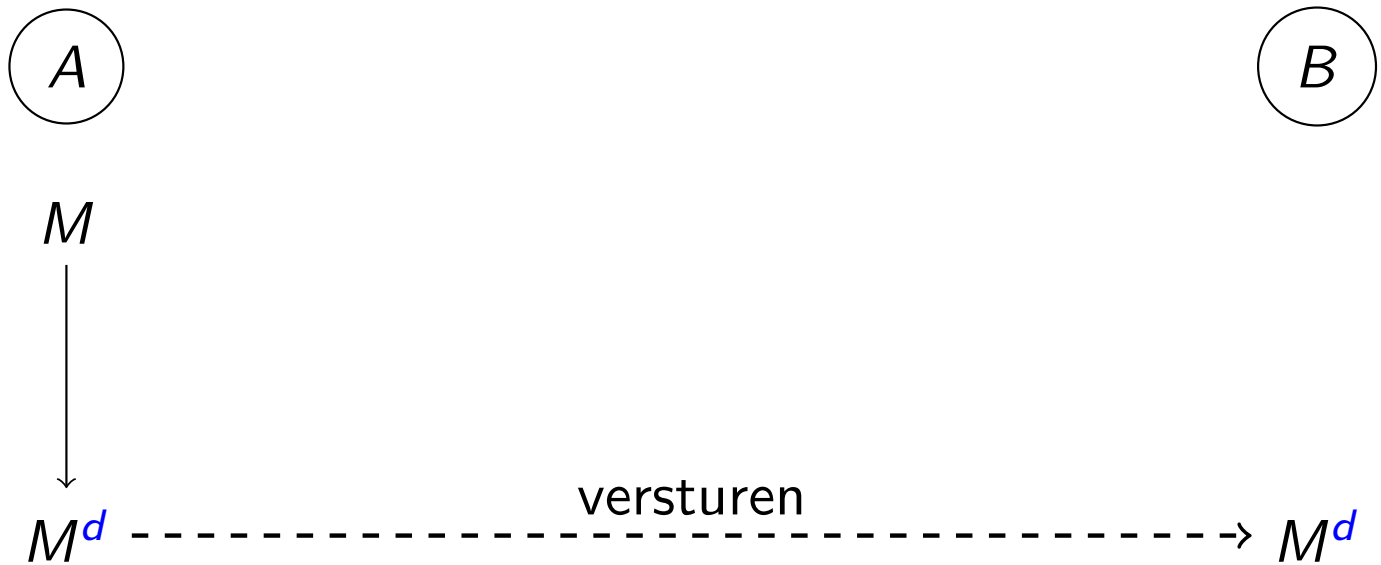
$n = pq$

$de \equiv 1 \mod (p-1)(q-1)$

RSA

$n = pq$

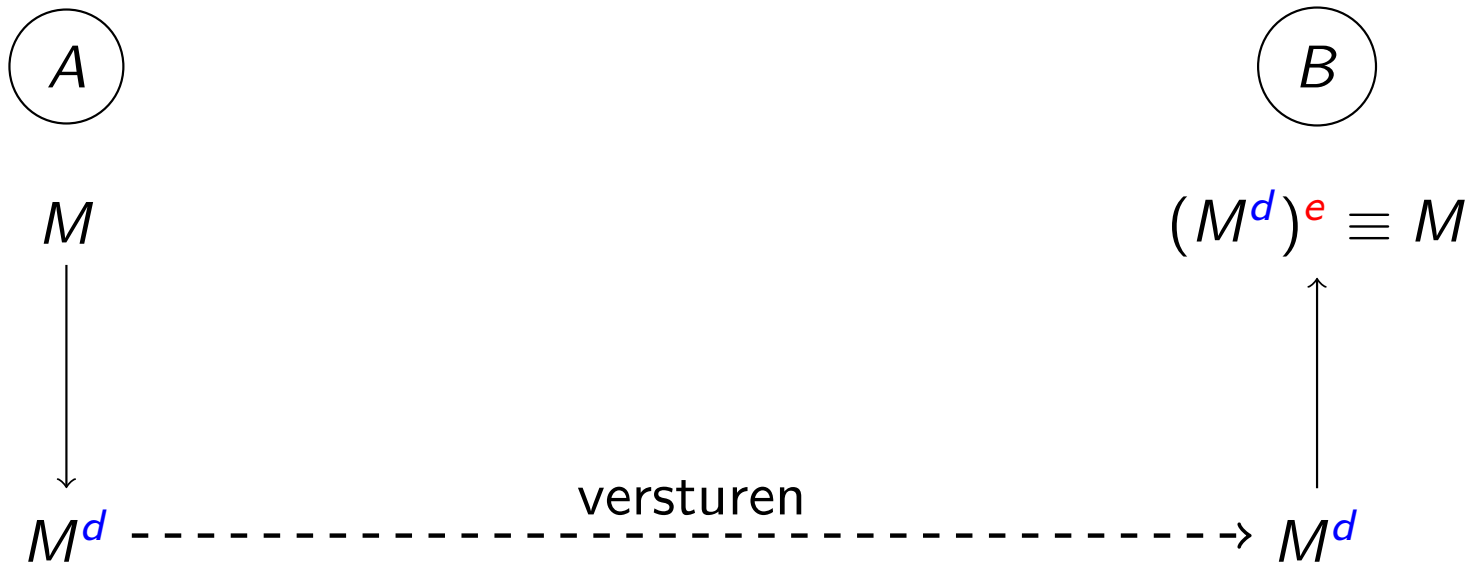
$de \equiv 1 \mod (p-1)(q-1)$



RSA

$n = pq$

$de \equiv 1 \mod (p-1)(q-1)$



Veel plezier verder op de Nationale Wiskunde Dagen!