Bijlage D · Oplossingen

1. Instapwiskunde

Oefening 1

1) a^{10}
2) $2a^5$
3) 0
4) a^{15}
5) a^7
6) a^6
7) a^8
8) $\frac{1}{4}a^6$

Oefening 2

1) $-a-b$
2) $\frac{a+b}{-c}$ en $\frac{-a-b}{c}$
3) $\frac{4c+3d}{4d}$
4) $\frac{3c}{4d}$
5) -7
6) a^{2+n+m}
7) $-8a^6b^9$
8) c^4d^2
9) $\frac{b^2}{a^{10}}$
10) a^9

Oefening 3

1) -6
2) $\frac{26}{5}$

Oefening 4 De oneven getallen zijn 45, 47 en 49.

Oefening 5

1) a^{-12}
2) $\frac{1}{a}$
3) a^{-20}
4) $\frac{a^6}{b^9}$
5) b^8
6) $16a^{12}b^8$
7) b^{50}
8) a^{23}
9) $-16a^6b$
10) $\frac{16}{9}a^6b^4$

Oefening 6

1) 0
2) $-16x^4y^4$
3) -1
4) $-12x^{12}y^6$
5) $-x^{24}y^6$
6) 0
7) $3x^2-6x-3$
8) $-8x^3+38x^2+6x$
9) $14x^2-21x+8$

Oefening 7

1) $(9x^2+5y)^2$
2) onmogelijk
3) onmogelijk
4) $(5x-6)^2$

Oefening 8

1) $\delta = \frac{-5}{6}$ en $\delta = 0$
2) $x = \frac{-5}{2}$ en $x = \frac{5}{2}$
3) $t = \frac{-3}{2}$ en $t = 2$
4) $x = -1$ en $x = \frac{-1}{4}$
5) $t = -2$
6) $t = -3$ en $t = 2$

Oefening 9 $V(x,y) = -3(a+7b)(x-2y)$

Oefening 10 $K(x) = 9\left(x-\frac{1}{3}\right)^2$

2. Logaritmen

Oefening 11

1) 0
2) 4
3) 2
4) $\frac{4}{3}$
5) $-\frac{3}{2}$
6) -4

Oefening 12 $\log_e(100) > \log_{10}(100)$

Oefening 13 De uitspraak '$\log_3(81)+\log_3(9) = \log_3(729)$' is waar.

Oefening 14

1) 0,778
2) 0,903
3) 0,954
4) 1,255
5) 0,699
6) 1,176
7) 0,176
8) $-0,125$

Oefening 15

1) $\log_{13}(x^2+7) - \log_{13}(x-8)$
2) $\log_{111}P + \log_{111}Q + \log_{111}R - \log_{111}M - \log_{111}V$
3) $2\log_g P + 3\log_g Q + \log_g R - \log_g M$

Oefening 16 Via $\frac{\log_5(8)}{\log_5(4)}$ bekomen we $\frac{3}{2}$ als antwoord.

Oefening 17 De uitspraak '$\frac{1}{\log_a(c)} + \frac{1}{\log_b(c)} = \frac{1}{\log_{(ab)}(c)}$' is waar.

Oefening 18 Een $\log_{10}(x)$ programmeren we als $\frac{\ln(x)}{\ln(10)}$.

Oefening 19

1) $x = \frac{1}{\sqrt{2}}$
2) $x = \frac{1}{3}$
3) $x = \frac{1}{16}$
4) $x = \frac{4}{5}$

Oefening 20

1) $t = \frac{7}{11}$
2) $t = \frac{5}{6}$
3) $t = 1 + \sqrt{10}$

Oefening 21

1) $x \in \{\frac{1}{2},\ 2\}$
2) $x \in \{5,\ 625\}$

Oefening 22 De finale oplossingenverzameling is het singleton $\{2\}$.

Oefening 23 De enige oplossing die voldoet aan de voorwaarden is $t = 4$.

Oefening 24 De unieke oplossing luidt $z = 3$.

Oefening 25 De unieke oplossing is $r = 6$.

Oefening 26

1) We vervangen P_{uit} en P_{in} door de formules $P_{uit} = \dfrac{U_{uit}^2}{R_{uit}}$ en $P_{in} = \dfrac{U_{in}^2}{R_{in}}$, zodat we $A_P = 10 \cdot \log_{10}\left(\dfrac{\frac{U_{uit}^2}{R_{uit}}}{\frac{U_{in}^2}{R_{in}}}\right)$ verkrijgen. Omdat $R_{uit} = R_{in}$ volgt hieruit $A_P = 10 \cdot \log_{10}\left(\dfrac{U_{uit}^2}{U_{in}^2}\right)$. Via de rekenregel 'logaritme van een macht' volgt uit $A_P = 10 \cdot \log_{10}\left(\dfrac{U_{uit}}{U_{in}}\right)^2$ de gevraagde formule.
2) $A_P = 20\ \ dB$
3) $U_{uit} = 2\ \ mV$

3. Functies

Oefening 27

$(-1,-36)$ en $(4,\ 24)$

Oefening 28

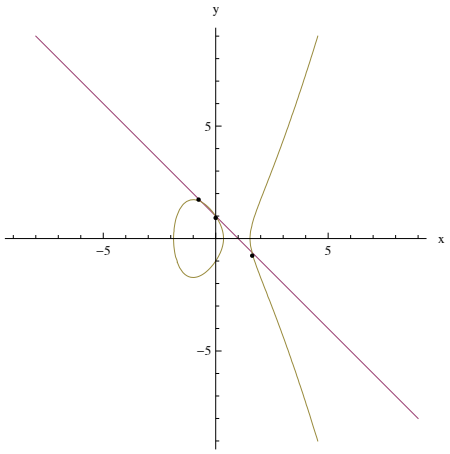
1) $(-\sqrt{5},\ 2)$ en $(\sqrt{5},\ 2)$
2) $(-1,-\sqrt{6})$ en $(-1,\ \sqrt{6})$

Oefening 29

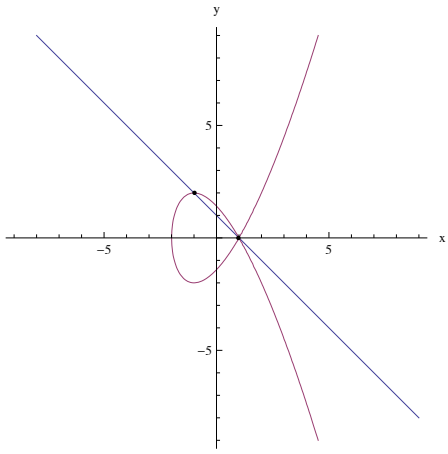
1) $(0,\ 1)$, $(\frac{1+\sqrt{5}}{2},\frac{1-\sqrt{5}}{2})$ en $(\frac{1-\sqrt{5}}{2},\frac{1+\sqrt{5}}{2})$
2) $(0,\ 1)$, $(0,\ 1)$ (tweemaal dus) en $(2,-1)$
3) $(1,\ 1)$, $(\sqrt{3},\sqrt{3})$ en $(-\sqrt{3},-\sqrt{3})$

Oefening 30

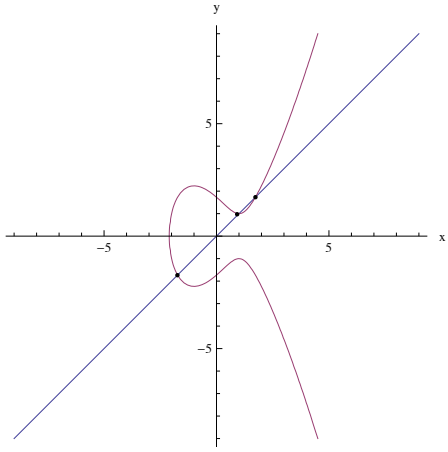
1)



2)

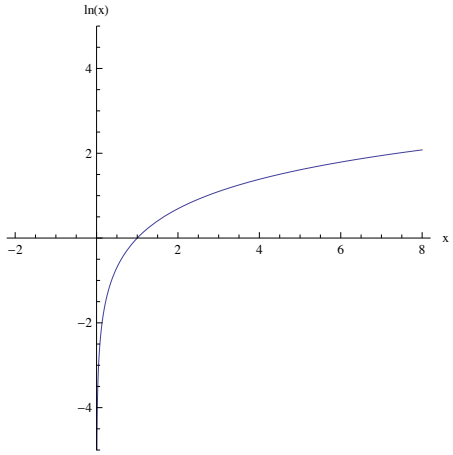


3)



Oefening 31

1)



2) De natuurlijke logaritmische functie $\ln(x)$ heeft als domein $\mathbb{R}^+\backslash\{0\}$ en als beeld $\mathbb{R}$.
3) De functie $\ln(x)$ telt één nulpunt, $x_0 = 1$.
4) De grafiek van $\ln(x)$ neigt naar de y-as als verticale asymptoot zodra x naar 0 nadert.

Oefening 32 Het snijpunt is $(\frac{1}{e}, -1)$.

Oefening 33 De dikte van dit krantenpapier bedraagt minder dan $0,1$ *mm*.

Oefening 34

1) 1024 transistors in 1977
2) vanaf 2008
3) 8 jaren

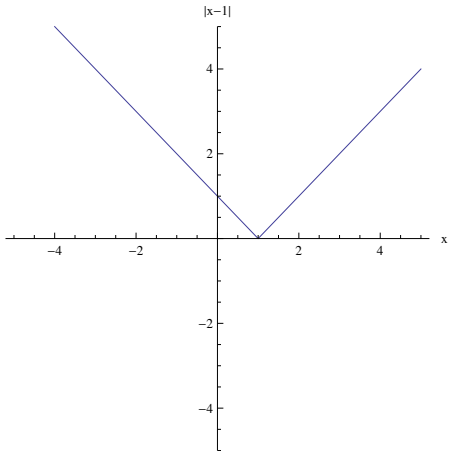
Oefening 35 De functie $f(x)$ heeft als domein $\mathbb{R}$ en $g(x)$ heeft als domein $\mathbb{R}^+\backslash\{0\}$.

Oefening 36

1) De functie $f(x) = |x-1|$ heeft als domein $\mathbb{R}$ en als beeld $\mathbb{R}^+$.
2) De functie heeft één nulpunt, $x_0 = 1$.
3) De functie telt eveneens één singulier punt, $x_s = 1$.

Oefening 37

1) Neen
2) De functie $f(x)$ heeft als domein $\mathbb{R}$ en als beeld $\mathbb{Z}$.
3) De functie telt oneindig veel reële nulpunten $x_0 \in \left]-\frac{1}{2}, \frac{1}{2}\right]$.



4. Getalformaten

Oefening 38

1) DCCCCLXXXXVIIII, of CMXCIX met 'verschil-conventie'
2) ⋂⋂⋂|||
3) 1836_{10}

Oefening 39 De kleinst mogelijke getalbasis is 2, daar getalbasis 1 geen oplopende machten zou hebben.

Oefening 40

1) $a+b=(11\ 0000)_2$
2) $a\cdot b=(10\ 0011\ 1111)_2$
3) $2\cdot a+8\cdot b=(1111\ 0110)_2$

Oefening 41 De getalbasis $8=2^3$ had een handiger conversie toegelaten naar de getalbases 2 en 16. De getalbasis $12=2^2\cdot 3$ bezit met $\{2,3,4,6\}$ meer echte delers dan ons grondtal $10=2\cdot 5$, waardoor meer getallen efficiënt twaalftallig te noteren zijn. *Voorbeeld:* $(0,4)_{12}$ in plaats van $(0,333\ldots)_{10}$ voor de breuk één derde.

Oefening 42 De rest van a modulo 4 is eveneens gelijk aan 2. De rest van a modulo 16 is gelijk aan 2 of gelijk aan 10.

Oefening 43 $(31)_{\text{oct}}=(25)_{\text{dec}}$

Oefening 44 Het getal is $(57)_{10}$.

Oefening 45 Omwille van de eenvoud van het betoog gaan we uit van een geheel getal bestaande uit drie decimalen, $(xyz)_{10}$.
Hieruit volgt dat $(10^2x+10y+z)-(x+y+z)=99x+9y$ waardoor we aantonen dat het geheel getal en zijn cijfersom steevast het negenvoud $9\cdot(11x+y)$ van elkaar

verschillen. Een decimaal getal is dus deelbaar door 9 zodra zijn cijfersom deelbaar is door 9.

Oefening 46 De aankomsttijd van de totale reis: 2 uur (zonder overschrijding van uurgordels).

Oefening 47 De deler 16 kan enkel de natuurlijke getallen van 0 tot 15 als rest geven.

Oefening 48

1) 5 is geen vijftallig cijfer
2) F is geen achttallig cijfer

Oefening 49

$(\ldots)_2$	$(\ldots)_3$	$(\ldots)_5$	$(\ldots)_8$	$(\ldots)_{10}$	$(\ldots)_{16}$	$(\ldots)_{60}$
$(111,111)_2$	$(21,2121\ldots)_3$	$(12,4141\ldots)_5$	$(7,7)_8$	$(7,875)_{10}$	$(7,E)_{16}$	$(7,52'30'')_{60}$
$(1001,10011001\ldots)_2$	$(100,12101210\ldots)_3$	$(14,3)_5$	$(11,46314631\ldots)_8$	$(9,6)_{10}$	$(9,99\ldots)_{16}$	$(9,36')_{60}$
$(1100010,0001)_2$	$(10122,00120012\ldots)_3$	$(343,01240124\ldots)_5$	$(142,04)_8$	$(98,0625)_{10}$	$(62,1)_{16}$	$(1;38,3'45'')_{60}$
$(101011,\overline{000111})_2$	$(1121,01)_3$	$(133,\overline{023421})_5$	$(53,\overline{07})_8$	$(43,\overline{1})_{10}$	$(2B,\overline{1C7})_{16}$	$(43,6'40'')_{60}$
$(100100011,1111)_2$	$(101210,22102210\ldots)_3$	$(2131,43204320\ldots)_5$	$(443,74)_8$	$(291,9375)_{10}$	$(123,F)_{16}$	$(4;51,56'15'')_{60}$
$(100000001000,111)_2$	$(2211011,2121\ldots)_3$	$(31211,4141\ldots)_5$	$(4010,7)_8$	$(2056,875)_{10}$	$(808,E)_{16}$	$(34;16,52'30'')_{60}$
$(0,\overline{0100001010001111010111})_2$	$(0,\overline{0210001121201222110 1})_3$	$(0,11\overline{2})_5$	$(0,\overline{20507534121727024 3656})_8$	$(0,26)_{10}$	$(0,\overline{428F5C})_{16}$	$(0,15'36'')_{60}$

Oefening 50

1) de getalbasis $x = 6$
2) de getalbasis $x = 16$

Oefening 51 Het getal is $(63)_8$.

Oefening 52 De decimale cijfercombinaties die voldoen zijn respectievelijk $(x,y) \in \{(1,2),(1,7),(3,2),(3,7),(5,2),(5,7),(7,2),(7,7),(9,2),(9,7)\}$.

5. Getallen in computers

Oefening 53

#(unsigned long) = 4294967296 (of 18446744073709551616 in de 64-bitarchitectuur)

Oefening 54 Zie de tabel op pagina 96.

Oefening 55 signed long = $\{-2147483648,\ldots,2147483647\}_{\text{dec}} \subset \mathbb{Z}$
(of signed long = $\{-9223372036854775808,\ldots,9223372036854775807\}_{\text{dec}}$)
#(signed long) = 4294967296 (of 18446744073709551616 in de 64-bitarchitectuur)

Oefening 56 Het verschil is $(0000\ 0000\ 0110\ 1011)_{2k/16\text{bit}}$.

Oefening 57 Het getal $-(14377)_{\text{dec}}$.

Oefening 58 De optelling mislukt wegens gehele 'negatieve overflow'.
De verklaring hiervoor op bitniveau luidt: $1\ (0011\ 1100)_{2k/8\text{bit}} = (60)_{\text{dec}}$

Oefening 59

1) $\alpha = 0,0142136\ldots$ en $a_{10} = 1$
2) $\varepsilon_M = 1\%$ en $p_{10} = 2$
3) $\left(\sqrt{2}\right)' = +1,4 \times 10^0$

Oefening 60

1) $\alpha = 0,000033\ldots$ en $a_{10} = 4$
2) $\varepsilon_M = 0,01\%$ en $p_{10} = 4$
3) $\left(\frac{1}{3}\right)' = +3,333 \times 10^{-1}$

Oefening 61 Vervang in het bewijs op pagina 105 het decimaal grondtal 10 overal door het binair grondtal 2.

Oefening 62 $x' = (-1)^0 \times (1,0001)_{\text{bin}} \times 2^{0-4}$

Oefening 63 $x' = (-1)^1 \times (1,1111)_{\text{bin}} \times 2^{6-4}$

Oefening 64

$$\begin{aligned}
1)\ x'_{\text{min}} &= (-1)^0 \times (1,0000\ 0000\ 0000\ 0000\ 0000\ 000)_{\text{bin}} \times 2^{0-127} \\
&= 2^{-127} = 2^{-7} \cdot 2^{-120} = \tfrac{1}{128}\left(2^{10}\right)^{-12} \\
&\approx \tfrac{1}{1000}\left(10^3\right)^{-12} = 10^{-39}
\end{aligned}$$

$$\begin{aligned}
2)\ x'_{\text{max}} &= (-1)^0 \times (1,1111\ 1111\ 1111\ 1111\ 1111\ 111)_{\text{bin}} \times 2^{255-127} \\
&\approx 2 \times 2^{128} \\
&= 2 \times 2^8 \cdot 2^{120} = \tfrac{1}{2}2^{10} \cdot \left(2^{10}\right)^{12} \\
&\approx \tfrac{1}{10}10^3 \cdot \left(10^3\right)^{12} = 10^{38}
\end{aligned}$$

Oefening 65

$x' = 3,141\ 592\ 7_{\text{dec}} \pm 0,000\ 000\ 1_{\text{dec}}$ (waaruit we $x = \pi$ mogen vermoeden).

Oefening 66

De IEEE single precision-bitrij van x' luidt $(\text{C1:AB:00:00})_{\text{h}}$. De relatieve opslagfout $\varepsilon_M = 2^{-24}$ levert een decimale machineprecisie van $p_{10} \approx 8$ opgeslagen beduidende cijfers van elk machinegetal x'.

Oefening 67

$$\begin{aligned} \#(\text{double precision}) &= 2^{64} = 2^4 \cdot 2^{60} = 16 \cdot \left(2^{10}\right)^6 \\ &\approx 16 \cdot \left(10^3\right)^6 = 16 \cdot 10^{18} \end{aligned}$$

$$\begin{aligned} \varepsilon_M &= 2^{-53} = 2^{-3} \cdot 2^{-50} = \tfrac{1}{8}\left(2^{10}\right)^{-5} \\ &\approx \tfrac{1}{10}\left(10^3\right)^{-5} = 10^{-16}, \text{ waaruit } p_{10} = 16 \text{ volgt.} \end{aligned}$$

Oefening 68

We onderzoeken welke fouten kunnen ontstaan uit dergelijke vermenigvuldiging.

$$\begin{aligned} (s' \cdot t')' &= (s' \cdot t')\,[1 \pm \varepsilon] \\ &= \begin{cases} (s\,[1 \pm \varepsilon] \cdot t\,[1 \pm \varepsilon])\,[1 \pm \varepsilon] \\ \text{of} \\ (s\,[1 \mp \varepsilon] \cdot t\,[1 \pm \varepsilon])\,[1 \pm \varepsilon] \\ \text{of} \\ (s\,[1 \mp \varepsilon] \cdot t\,[1 \mp \varepsilon])\,[1 \pm \varepsilon] \end{cases} \\ &= \begin{cases} (s \cdot t)\,[1 \pm \varepsilon]^3 \\ \text{of} \\ (s \cdot t)([1 \mp \varepsilon]\,[1 \pm \varepsilon])\,[1 \pm \varepsilon] \\ \text{of} \\ (s \cdot t)\,[1 \mp \varepsilon]\,([1 \mp \varepsilon]\,[1 \pm \varepsilon]) \end{cases} \end{aligned}$$

$$\begin{aligned} (s' \cdot t')' &= \begin{cases} (s \cdot t)\left[1 \pm 3\varepsilon + 3\varepsilon^2 \pm \varepsilon^3\right] \\ \text{of} \\ (s \cdot t)\left[1 - \varepsilon^2\right][1 \pm \varepsilon] \\ \text{of} \\ (s \cdot t)\,[1 \mp \varepsilon]\left[1 - \varepsilon^2\right] \end{cases} \\ &\approx \begin{cases} (s \cdot t)\,[1 \pm 3\varepsilon] \\ \text{of} \\ (s \cdot t)\,[1 \pm \varepsilon] \end{cases} \end{aligned}$$

We laten de hogere machten van ε die verwaarloosbaar klein worden ten opzichte van 1 en de fractie ε zelf, achterwege en begrijpen dat we nog twee scenario's overhouden. Het eerste ervan vertoont een relatieve foutverhoging.

6. Booleaanse wiskunde

Oefening 69

1) waar
2) onwaar
3) geen booleaanse uitspraak
4) waar
5) onwaar
6) waar

Oefening 70

p	q	$p \to q$	$p \wedge (p \to q)$	$(p \wedge (p \to q)) \to q$
onwaar	onwaar	waar	onwaar	waar
onwaar	waar	waar	onwaar	waar
waar	onwaar	onwaar	onwaar	waar
waar	waar	waar	waar	waar

Oefening 71

1) via het opstellen van de waarheidstabel voor de logische equivalentie

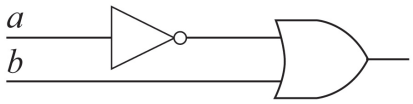
p	q	r	$\neg q$	$\neg r$	$\neg q \wedge \neg r$	$\neg(\neg q \wedge \neg r)$
onwaar	onwaar	onwaar	waar	waar	waar	onwaar
onwaar	onwaar	waar	waar	onwaar	onwaar	waar
onwaar	waar	onwaar	onwaar	waar	onwaar	waar
onwaar	waar	waar	onwaar	onwaar	onwaar	waar
waar	onwaar	onwaar	waar	waar	waar	onwaar
waar	onwaar	waar	waar	onwaar	onwaar	waar
waar	waar	onwaar	onwaar	waar	onwaar	waar
waar	waar	waar	onwaar	onwaar	onwaar	waar

$p \to \neg(\neg q \wedge \neg r)$	$p \wedge \neg q$	$(p \wedge \neg q) \to r$	$(p \to \neg(\neg q \wedge \neg r)) \leftrightarrow ((p \wedge \neg q) \to r)$
waar	onwaar	waar	waar
waar	onwaar	waar	waar
waar	onwaar	waar	waar
waar	onwaar	waar	waar
onwaar	waar	onwaar	waar
waar	waar	waar	waar
waar	onwaar	waar	waar
waar	onwaar	waar	waar

2) via booleaans rekenen

$$\begin{array}{rcl} (p \to \neg(\neg q \wedge \neg r)) & \leftrightarrow & ((p \wedge \neg q) \to r) \\ \neg p \vee \neg(\neg q \wedge \neg r)) = & & \neg(p \wedge \neg q) \vee r = \\ \neg p \vee \neg(\neg q) \vee \neg(\neg r) = & & \neg p \vee \neg(\neg q) \vee r = \\ \neg p \vee q \vee r & & \neg p \vee q \vee r \end{array}$$

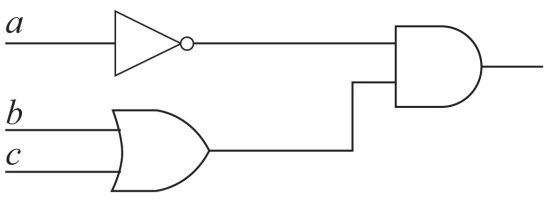
Oefening 72



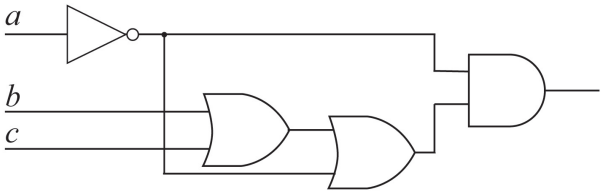
a	b	$\text{imp}(a,b) = \neg a \vee b$
uit	uit	aan
uit	aan	aan
aan	uit	uit
aan	aan	aan

Oefening 73

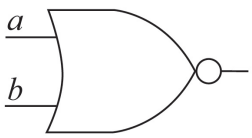
1)

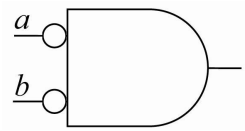


2)



Oefening 74





Oefening 75

$a_1 \wedge a_2 \wedge a_3$, $a_1 \wedge a_2 \wedge \neg a_3$, $a_1 \wedge \neg a_2 \wedge a_3$, $a_1 \wedge \neg a_2 \wedge \neg a_3$,
$\neg a_1 \wedge a_2 \wedge a_3$, $\neg a_1 \wedge a_2 \wedge \neg a_3$, $\neg a_1 \wedge \neg a_2 \wedge a_3$ en $\neg a_1 \wedge \neg a_2 \wedge \neg a_3$.

Oefening 76

$$\begin{aligned}
(a \wedge b) \vee (\neg a \wedge b) \vee (a \wedge \neg b) &= ((a \vee \neg a) \wedge b)) \vee (a \wedge \neg b) \\
&= (1 \wedge b) \vee (a \wedge \neg b) \\
&= b \vee (a \wedge \neg b) \\
&= (b \vee a) \wedge (b \vee \neg b) \\
&= (b \vee a) \wedge 1 \\
&= b \vee a \\
&= a \vee b = f_8(a,b)
\end{aligned}$$

De naamsverklaring van ‘inclusive or’ voor $f_8(a,b)$ lezen we op pagina 159.

$$\begin{aligned}
(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b) &= ((a \vee \neg a) \wedge b) \vee (\neg a \wedge \neg b) \\
&= (1 \wedge b) \vee (\neg a \wedge \neg b) \\
&= b \vee (\neg a \wedge \neg b) \\
&= (b \vee \neg a) \wedge (b \vee \neg b) \\
&= (b \vee \neg a) \wedge 1 \\
&= b \vee \neg a \\
&= \neg a \vee b = f_9(a,b)
\end{aligned}$$

$$\begin{aligned}(a\wedge b)\vee(a\wedge\neg b)\vee(\neg a\wedge\neg b) &= (a\wedge(b\vee\neg b))\vee(\neg a\wedge\neg b)\\ &= (a\wedge 1)\vee(\neg a\wedge\neg b)\\ &= a\vee(\neg a\wedge\neg b)\\ &= (a\vee\neg a)\wedge(a\vee\neg b)\\ &= 1\wedge(a\vee\neg b)\\ &= a\vee\neg b = f_{10}(a,b)\end{aligned}$$

$$\begin{aligned}(\neg a\wedge b)\vee(a\wedge\neg b)\vee(\neg a\wedge\neg b) &= (\neg a\wedge b)\vee((a\vee\neg a)\wedge\neg b)\\ &= (\neg a\wedge b)\vee(1\wedge\neg b)\\ &= (\neg a\wedge b)\vee\neg b\\ &= (\neg a\vee\neg b)\wedge(b\vee\neg b)\\ &= (\neg a\vee\neg b)\wedge 1\\ &= \neg a\vee\neg b = f_7(a,b)\end{aligned}$$

Oefening 77 Zie de benedenhelft van de boekcover.

Oefening 78

1) $\mathrm{dnv}(f(x,y,z,w)) = (\neg x\wedge y\wedge\neg z\wedge w)\vee(\neg x\wedge y\wedge z\wedge w)\vee$
$(x\wedge y\wedge\neg z\wedge\neg w)\vee(x\wedge y\wedge\neg z\wedge w)\vee(x\wedge y\wedge z\wedge w)\vee(x\wedge y\wedge z\wedge\neg w)\vee$
$(x\wedge\neg y\wedge z\wedge w)\vee(x\wedge\neg y\wedge z\wedge\neg w)$

2) $\mathrm{dev}(f(x,y,z,w)) = (x\wedge y)\vee(x\wedge z)\vee(y\wedge w)$

Oefening 79

$\mathrm{dnv}(f(a,b,c,d)) = (\neg a\wedge\neg b\wedge\neg c\wedge d)\vee(\neg a\wedge\neg b\wedge c\wedge d)\vee(a\wedge b\wedge\neg c\wedge\neg d)\vee$
$(a\wedge b\wedge\neg c\wedge d)\vee(a\wedge b\wedge c\wedge d)\vee(a\wedge b\wedge c\wedge\neg d)\vee(a\wedge\neg b\wedge\neg c\wedge\neg d)\vee$
$(a\wedge\neg b\wedge\neg c\wedge d)\vee(a\wedge\neg b\wedge c\wedge d)$

Oefening 80

$\mathrm{dev}(g(a,b,c,d,e)) = (\neg a\wedge d)\vee(a\wedge\neg c\wedge\neg d\wedge e)\vee(a\wedge\neg b\wedge\neg d)$

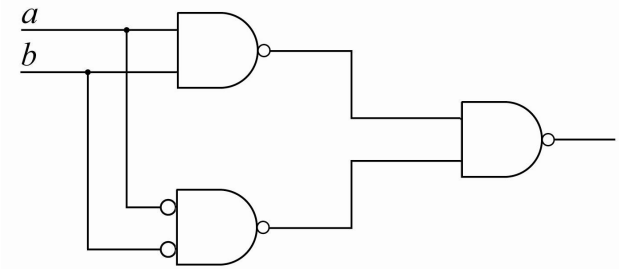
Oefening 81

Het netwerkadres is $(172.23.0.0)_{\mathrm{dec}}$ en het 'broadcast'-adres is $(172.23.255.255)_{\mathrm{dec}}$.

Oefening 82

1) We herschrijven de booleaanse functie als
$\mathrm{nxor}(a,b) = \neg\neg((a\wedge b)\vee(\neg a\wedge\neg b)) = \neg(\neg(a\wedge b)\wedge\neg(\neg a\wedge\neg b))$

2) We realiseren het combinatorisch circuit ervoor in nand-technologie.



7. Inleiding tot de cryptografie

Oefening 83

1) 'EBH'
2) 'EBH CPC'
3) 'MFQFM'

Oefening 84

1) 'DAG', 'DGA', 'ADG', 'AGD', 'GDA' en 'GAD'.
2) Aangepaste opgave: 'BOB', 'BBO' en 'OBB'.
3) 'LEPEL', 'LEPLE', 'LEEPL', 'LEELP', 'LELPE', 'LELEP', 'LPEEL', 'LPELE', 'LPLEE', 'LLEPE', 'LLEEP', 'LLPEE', 'ELPEL', 'ELPLE', 'ELEPL', 'ELELP', 'ELLPE', 'ELLEP', 'EPLEL', 'EPLLE', 'EPELL', 'EELPL', 'EELLP', 'EEPLL', 'PLEEL', 'PLELE', 'PLLEE', 'PELEL', 'PELLE' en 'PEELL'

Oefening 85

	$0 \leqslant x < 15$	$-15 < x < 0$
1)	$2,5,8,11,14$	$-13,-10,-7,-4,-1$
2)	$5,14$	$-13,-4$
3)	$0,7,14$	$-14,-7$

Oefening 86

1) $345612 = 3456 \cdot 100 + 12$
2) $345612 = 345 \cdot 1000 + 612$
3) $345612 = 34561 \cdot 10 + 2$

Oefening 87

1) $1,3,5,15$
2) $1,2,3,5,6,10,15,30$
3) $1,2,4,7,14,28$

Oefening 88

$\overline{2}^{-1} \notin \mathbb{Z}_{26}\backslash\{\overline{0}\}$, terwijl $\overline{3}^{-1} = \overline{9}$ en $\overline{5}^{-1} = \overline{21}$. We besluiten hieruit dat $\overline{2} \in \mathbb{Z}_{26}\backslash\{\overline{0}\}$ een nuldeler is.

Oefening 89

$\overline{2}^{-1}$ en $\overline{3}^{-1} \notin \mathbb{Z}_6\backslash\{\overline{0}\}$ terwijl $\overline{5}^{-1} = \overline{5}$. Dit betekent dat $\overline{2}$ en $\overline{3}$ nuldelers zijn in $\mathbb{Z}_6\backslash\{\overline{0}\}$.

Oefening 90

$\overline{2}^{-1} = 4$ en $\overline{3}^{-1} = 5$ (en dus ook $\overline{5}^{-1} = \overline{3}$) in $\mathbb{Z}_7\backslash\{\overline{0}\}$.

Oefening 91

1) $\mathbb{Z}_6^* = \{1,5\}$
2) $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$
3) $\mathbb{Z}_{27}^* = \{1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26\}$
4) $\mathbb{Z}_{34}^* = \{1,3,5,7,9,11,13,15,19,21,23,25,27,29,31,33\}$

Oefening 92 $\overline{x_0} = \overline{21}$ in $\mathbb{Z}_{26}$.

Oefening 93 $\overline{x_0} = \overline{9}$ en $\overline{x_1} = \overline{22}$ in $\mathbb{Z}_{26}$.

Oefening 94

1) de additieve cayleytabel van $(\mathbb{Z}_6, +)$:

$+$ mod 6	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

2) het bewijs dat $(\mathbb{Z}_6, +)$ een commutatieve groep betreft:
Bewijs:

- De verzameling $\mathbb{Z}_6$ blijft gesloten onder de plus-bewerking $(+ \mod 6)$ daar elke som tot $\mathbb{Z}_6$ blijft behoren.
- De associativiteit van de plus-bewerking in $\mathbb{Z}_6$ komt er door overerving van de associativiteit van de gewone optelling in $\mathbb{Z}$.
- We herkennen het cayleytabelelement $\overline{0} \in \mathbb{Z}_6$ onmiddellijk als het nulelement voor de plus-bewerking in $\mathbb{Z}_6$.
- In $\mathbb{Z}_6$ bezit elk element $\overline{a}$ ook zijn tegengestelde $-\overline{a}$ daar elke resultaatrij het neutraal element $\overline{0}$ bevat.

Het is de symmetrie van de cayleytabel ten opzichte van zijn hoofddiagonaal, die de commutativiteit van de plus-bewerking $(+ \mod 6)$ aantoont. We besluiten dat het restsysteem $\mathbb{Z}_6$ uitgerust met de plus-bewerking $(+ \mod 6)$ de commutatieve additieve groep $(\mathbb{Z}_6, +)$ vormt. ■

3) van elk element het tegengesteld element:

$-\overline{0} = \overline{0}, -\overline{1} = \overline{5}, -\overline{2} = \overline{4}, -\overline{3} = \overline{3}, -\overline{4} = \overline{2}$ en $-\overline{5} = \overline{1}$ in $(\mathbb{Z}_6, +)$.

Oefening 95

Bewijs:

- De verzameling $\mathbb{Z}_7 \setminus \{\overline{0}\}$ blijft gesloten onder de maal-bewerking $(\cdot \mod 7)$ daar elk product tot $\mathbb{Z}_7 \setminus \{\overline{0}\}$ blijft behoren.
- De associativiteit van de maal-bewerking in $\mathbb{Z}_7 \setminus \{\overline{0}\}$ komt er door overerving van de associativiteit van de gewone vermenigvuldiging in $\mathbb{Z}$.
- We herkennen het cayleytabelelement $\overline{1} \in \mathbb{Z}_7 \setminus \{\overline{0}\}$ onmiddellijk als het eenheidselement voor de maal-bewerking in $\mathbb{Z}_7 \setminus \{\overline{0}\}$.
- In $\mathbb{Z}_7 \setminus \{\overline{0}\}$ bezit elk element $\overline{a}$ ook zijn invers $\overline{a}^{-1}$ daar elke resultaatrij het neutraal element $\overline{1}$ bevat.

Het is de symmetrie van de cayleytabel ten opzichte van zijn hoofddiagonaal, die de commutativiteit van de maal-bewerking $(\cdot \mod 7)$ aantoont. We besluiten dat het restsysteem zonder nul $\mathbb{Z}_7 \setminus \{\overline{0}\}$, uitgerust met de maal-bewerking $(\cdot \mod 7)$ de commutatieve multiplicatieve groep $(\mathbb{Z}_7 \setminus \{\overline{0}\}, \cdot)$ vormt. ■

Oefening 96

1) de multiplicatieve cayleytabel van $(\mathbb{Z}_6\setminus\{\overline{0}\},\cdot)$:

$\cdot \mod 6$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

2) het bewijs dat $(\mathbb{Z}_6\setminus\{\overline{0}\},\cdot)$ geen groep betreft:

- De verzameling $\mathbb{Z}_6\setminus\{\overline{0}\}$ blijkt niet gesloten onder de maal-bewerking $(\cdot \mod 6)$ daar het product $\overline{0}\notin\mathbb{Z}_6\setminus\{\overline{0}\}$.
- We herkennen het cayleytabelelement $\overline{1}\in\mathbb{Z}_6\setminus\{\overline{0}\}$ als het eenheidselement voor de maal-bewerking.
- De elementen $\overline{2}$, $\overline{3}$ en $\overline{4}$ van $\mathbb{Z}_6\setminus\{\overline{0}\}$ beschikken als nuldelers niet over een invers element; hun resultaatrijen missen het neutraal element $\overline{1}$.

We besluiten uit de eerste en laatste vaststelling dat $\mathbb{Z}_6\setminus\{\overline{0}\}$, uitgerust met de maal-bewerking $(\cdot \mod 6)$ geen groep kan vormen.

3) alle paren aan nuldelers en alle inverteerbare elementen met hun invers element:

De producten $\overline{2}\cdot\overline{3}=\overline{0}$ en $\overline{4}\cdot\overline{3}=\overline{0}$, tonen ons de nuldelers $\overline{2}$, $\overline{3}$ en $\overline{4}$ van $\mathbb{Z}_6\setminus\{\overline{0}\}$. De twee overige elementen van $\mathbb{Z}_6\setminus\{\overline{0}\}$ zijn inverteerbaar als $\overline{1}^{-1}=\overline{1}$ en $\overline{5}^{-1}=\overline{5}$.

8. Lineaire cijfers

Oefening 97

1)
$$\begin{aligned} 3^{300} \mod 25 &\equiv \left(3^3\right)^{100} \mod 25 \\ &\equiv (27 \mod 25)^{100} \\ &\equiv 2^{100} \mod 25 \\ &\equiv \left(2^5\right)^{20} \mod 25 \\ &\equiv (32 \mod 25)^{20} \\ &\equiv 7^{20} \mod 25 \end{aligned}$$

$$\begin{aligned} &\equiv \left(7^2\right)^{10} \mod 25 \\ &\equiv (49 \mod 25)^{10} \\ &\equiv (-1)^{10} \mod 25 \equiv 1 \mod 25 \end{aligned}$$

2) $$\begin{aligned} 213^{22} - 123 \mod 23 &\equiv (213 \mod 23)^{22} - (123 \mod 23) \\ &\equiv 6^{22} - 8 \mod 23 \\ &\equiv 6 \cdot \left(6^3\right)^7 - 8 \mod 23 \\ &\equiv 6 \cdot (216 \mod 23)^7 - 8 \\ &\equiv 6 \cdot 9^7 - 8 \mod 23 \\ &\equiv (6 \cdot 9) \cdot \left(9^2\right)^3 - 8 \mod 23 \\ &\equiv (54 \mod 23) \cdot (81 \mod 23)^3 - 8 \\ &\equiv 8 \cdot 12^3 - 8 \mod 23 \\ &\equiv (8 \cdot 12) \cdot 12^2 - 8 \mod 23 \\ &\equiv (96 \mod 23) \cdot (144 \mod 23) - 8 \\ &\equiv 4 \cdot 6 - 8 \mod 23 \equiv 16 \mod 23 \end{aligned}$$

3) $$\begin{aligned} 17^{25} \mod 26 &\equiv 17^{24} \cdot 17 \mod 26 \\ &\equiv \left(17^2\right)^{12} \cdot 17 \mod 26 \\ &\equiv (289 \mod 26)^{12} \cdot 17 \\ &\equiv 3^{12} \cdot 17 \mod 26 \\ &\equiv \left(3^3\right)^4 \cdot 17 \mod 26 \\ &\equiv (27 \mod 26)^4 \cdot 17 \\ &\equiv 1^4 \cdot 17 \mod 26 \equiv 17 \mod 26 \end{aligned}$$

Oefening 98

De laatste decimaal van 3^{81} is 3, daar

$$\begin{aligned} 3^{81} \mod 10 &\equiv 3 \cdot \left(3^4\right)^{20} \mod 10 \\ &\equiv 3 \cdot (81 \mod 10)^{20} \\ &\equiv 3 \cdot 1^{20} \mod 10 \equiv 3 \mod 10 \end{aligned}$$

Oefening 99 'NCXXYLYL'

Oefening 100 Het tweede invariante ringelement is $16 \in \mathbb{Z}_{26}$ (zie pagina 233), met als 'mini-karakter' de hoofdletter 'Q' (zie pagina 184).

Oefening 101 De wiskundig geldige sleutel $K_1 = (1,0)$ is praktisch onzinnig.

Oefening 102 'HALLOEVE'

Oefening 103 'SUCCES'

Oefening 104 'GEENAPRILVIS'

Oefening 105

Bewijs

$$\begin{aligned} \alpha^{-1}y - \alpha^{-1}\beta \mod 26 &\equiv \alpha^{-1}(\alpha x+\beta) - \alpha^{-1}\beta \mod 26 \\ &\equiv (\alpha^{-1}\cdot\alpha)x + \alpha^{-1}\beta - \alpha^{-1}\beta \mod 26 \\ &\equiv 1x+0 \mod 26 \equiv x \mod 26 \end{aligned}$$ ■

Oefening 106 'METOKZONDERKO'

Oefening 107 'TOBEORNOTTOBE'

Oefening 108

1) 'IBM', vercijferd door	$x+25$
2) 'MDCCCCLXXVIII'	$x+3$
3) 'MDCCCCLXXI'	$x+13$

Oefening 109

Substitueren we de eerste vercijfering $\alpha_1 x+\beta_1 \mod 26 \equiv y$ in de tweede,

$$\begin{aligned} \alpha_2 y+\beta_2 \mod 26 &\equiv \alpha_2(\alpha_1 x+\beta_1)+\beta_2 \mod 26 \\ &\equiv \underbrace{\alpha_2\alpha_1}_{\alpha} x + \underbrace{\alpha_2\beta_1+\beta_2}_{\beta} \mod 26, \end{aligned}$$

dan blijkt dit een eenzelfde vercijfering te geven. Cryptografisch beschouwd is de sleutel $K = (\alpha,\beta)$ ervan sterker noch zwakker.

Oefening 110 'BINNU-U-TRATTURI'

9. Klutsfuncties

Oefening 111

1) 4 miljard keer
2) $64 \cdot 10^{45}$ keer

Oefening 112

$x \equiv 23 \mod 70$

Oefening 113

1) 2012
2) 1001
3) 1001

Oefening 114

23 of $(128, 233, 338, \ldots)$ dingen

Oefening 115

22 (of $82, 142, 202, \ldots$) soldaten

Oefening 116

1) $1 \cdot 28 + (-3) \cdot 9 = 1$
2) $4 \cdot 200 + (-11) \cdot 72 = 8$
3) $8 \cdot 1245 + (-39) \cdot 255 = 15$

Oefening 117

1) $s \equiv 13 \mod 16$
2) $s \equiv 3 \mod 40$
3) $s \equiv 25 \mod 28$

Oefening 118

1) geen
2) geen
3) zevenenveertig

Oefening 119

1) $\{21\} \subset \mathbb{Z}_{26}$ zie oefening 92
2) $\{9, 22\} \subset \mathbb{Z}_{26}$ zie oefening 93

Oefening 120

1) twee; $\{6,13\} \subset \mathbb{Z}_{14}$
2) één; $\{9\} \subset \mathbb{Z}_{15}$
3) zeven; $\{5,18,31,44,57,70,83\} \subset \mathbb{Z}_{91}$
4) geen
5) vier; $\{22,81,140,199\} \subset \mathbb{Z}_{236}$
6) geen

Oefening 121

Uit de recursieve definitie $f_{n+1} = f_n + f_{n-1}$ halen we de vereiste algoritmestappen.

$$\begin{array}{l|lcl} d & f_{n+1} - f_n & = & f_{n-1} \\ = \text{uggd}(f_{n+1}, f_n) & f_n - f_{n-1} & = & f_{n-2} \\ = \text{uggd}(f_n, f_{n-1}) & \vdots & & \\ \vdots & & \vdots & \\ = \text{uggd}(f_4, f_3) & f_4 - f_3 & = & f_2 \\ = \text{uggd}(f_3, f_2) & f_3 - f_2 & = & f_1 \\ = \text{uggd}(f_2, f_1) & f_2 - f_1 & = & 0 \\ = \text{uggd}(f_1, 0) & & & \\ = 1 & & & \end{array}$$

Door het invullen van $f_1 = f_2 = 1$ als startwaarden, bepalen we de grootste gemene deler als $d = 1$ en dit voor elke twee opeenvolgende fibonaccigetallen.

10. RSA

Oefening 122

Bewijs

$$\begin{aligned} \phi(p) &= \#(\mathbb{Z}_p^*), \text{ zie formule (10.1)} \\ &= \#(\{\overline{a} \in \mathbb{Z}_p \text{ waarvoor } \text{ggd}(a,p) = 1\}), \text{ zie formule (7.18)} \\ &= \#(\{a \in [0, p-1] \subset \mathbb{N} \text{ waarvoor } \text{ggd}(a,p) = 1\}) \\ &= \#([1, p-1] \subset \mathbb{N}), \text{ daar } p \in \mathbb{P} \\ &= p - 1. \end{aligned}$$

■

Oefening 123

Bewijs
Met $p \in \mathbb{P}$ herschrijven we de stelling van Euler:

$$\text{Als } \text{ggd}(a,p) = 1 \text{ dan geldt}$$

$$\begin{aligned} a^{\phi(p)} &\equiv 1 \mod p, \text{ zie formule (10.4)} \\ a^{p-1} &\equiv 1 \mod p, \text{ zie formule (10.2)} \\ a \cdot a^{p-1} &\equiv a \cdot 1 \mod p \\ a^p &\equiv a \mod p. \end{aligned}$$

■

Oefening 124

1)
$$\begin{aligned} 3^{\phi(55)} \mod 55 &\equiv 3^{\phi(5\cdot 11)} \mod 55 \\ &\equiv 3^{\phi(5)\cdot\phi(11)} \mod 55, \text{ daar } \text{ggd}(5,11) = 1 \\ &\equiv 3^{(5-1)\cdot(11-1)} \mod 55, \text{ daar } 5,\ 11 \in \mathbb{P} \\ &\equiv 3^{40} \mod 55 \\ &\equiv \left(3^4\right)^{10} \mod 55 \\ &\equiv (81 \mod 55)^{10} \\ &\equiv 26^{10} \mod 55 \\ &\equiv \left(26^2\right)^5 \mod 55 \\ &\equiv (676 \mod 55)^5 \\ &\equiv 16^5 \mod 55 \\ &\equiv 16^2 \cdot 16^2 \cdot 16 \mod 55 \\ &\equiv (256 \mod 55) \cdot (256 \mod 55) \cdot 16 \\ &\equiv (36 \cdot 36) \cdot 16 \mod 55 \\ &\equiv (1296 \mod 55) \cdot 16 \\ &\equiv 31 \cdot 16 \mod 55 \\ &\equiv 496 \mod 55 \equiv 1 \end{aligned}$$

2)
$$\begin{aligned} 6^{\phi(55)} \mod 55 &\equiv (2\cdot 3)^{\phi(55)} \mod 55 \\ &\equiv 2^{\phi(55)} \cdot 3^{\phi(55)} \mod 55 \\ &\equiv (2^{\phi(55)} \mod 55) \cdot (3^{\phi(55)} \mod 55) \\ &\equiv (2^{40} \mod 55) \cdot 1, \text{ zie oefening 124-1} \end{aligned}$$

$$\begin{aligned}
&\equiv 2^{40} \mod 55\\
&\equiv \left(2^{10}\right)^4 \mod 55\\
&\equiv (1024 \mod 55)^4\\
&\equiv (-21)^4 \mod 55\\
&\equiv \left(-21^2\right)^2 \mod 55\\
&\equiv (441 \mod 55)^2\\
&\equiv 1^2 \mod 55 \equiv 1
\end{aligned}$$

Oefening 125

1) We stellen vooraf vast dat $\phi(101) = 100$ daar $101 \in \mathbb{P}$, waardoor

$$\begin{aligned}
2^{10203} \mod 101 &\equiv 2^{10200} \cdot 2^3 \mod 101\\
&\equiv \left(2^{100}\right)^{102} \cdot 8 \mod 101\\
&\equiv \left(2^{100} \mod 101\right)^{102} \cdot 8, \text{ met ggd}(2,101) = 1\\
&\equiv 1^{102} \cdot 8 \mod 101 \equiv 8.
\end{aligned}$$

2) We stellen vooraf vast dat

$$\begin{aligned}
\phi(100) &= \phi(4 \cdot 25)\\
&= \phi(4) \cdot \phi(25), \text{ daar ggd}(4,25) = 1\\
&= 2 \cdot 20 = 40
\end{aligned}$$

waardoor

$$\begin{aligned}
123^{562} \mod 100 &\equiv (123 \mod 100)^{562}\\
&\equiv 23^{562} \mod 100\\
&\equiv 23^2 \cdot 23^{560} \mod 100\\
&\equiv (529 \mod 100) \cdot \left(23^{40} \mod 100\right)^{14}, \text{ met ggd}(23,100) = 1\\
&\equiv 29 \cdot 1 \mod 100 \equiv 29.
\end{aligned}$$

Oefening 126

$$\begin{aligned}
1) \left(8^5 \mod 34\right)^{27} \mod 55 &\equiv \left(8^2 \cdot 8^2 \cdot 8 \mod 34\right)^{27} \mod 55\\
&\equiv ((64 \mod 34) \cdot (64 \mod 34) \cdot 8)^{27} \mod 55\\
&\equiv ((-4) \cdot (-4) \cdot 8 \mod 34)^{27} \mod 55\\
&\equiv (128 \mod 34)^{27} \mod 55\\
&\equiv 26^{27} \mod 55\\
&\equiv 26 \cdot \left(26^2\right)^{13} \mod 55\\
&\equiv 26 \cdot (676 \mod 55)^{13}
\end{aligned}$$

$$
\begin{aligned}
&\equiv 26\cdot 16^{13} \mod 55\\
&\equiv 26\cdot 16\cdot \left(16^2\right)^6 \mod 55\\
&\equiv 26\cdot 16\cdot (256 \mod 55)^6\\
&\equiv 26\cdot 16\cdot 36^6 \mod 55\\
&\equiv 26\cdot 16\cdot \left(36^2\right)^3 \mod 55\\
&\equiv 26\cdot 16\cdot (1296 \mod 55)^3\\
&\equiv 26\cdot 16\cdot 31^3 \mod 55\\
&\equiv 26\cdot 16\cdot 31\cdot 31^2 \mod 55\\
&\equiv 26\cdot 16\cdot 31\cdot (961 \mod 55)\\
&\equiv 26\cdot 16\cdot 31\cdot 26 \mod 55\\
&\equiv (676 \mod 55)\cdot 16\cdot 31\\
&\equiv 16\cdot 16\cdot 31 \mod 55\\
&\equiv (256 \mod 55)\cdot 31\\
&\equiv 36\cdot 31 \mod 55\\
&\equiv 1116 \mod 55 \equiv 16
\end{aligned}
$$

$$
\begin{aligned}
2)\ \left(8^5 \mod 55\right)^{27} \mod 34 &\equiv \left(8^2\cdot 8^2\cdot 8 \mod 55\right)^{27} \mod 34\\
&\equiv ((64 \mod 55)\cdot(64 \mod 55)\cdot 8)^{27} \mod 34\\
&\equiv (9\cdot 9\cdot 8 \mod 55)^{27} \mod 34\\
&\equiv ((81 \mod 55)\cdot 8)^{27} \mod 34\\
&\equiv (26\cdot 8 \mod 55)^{27} \mod 34\\
&\equiv 43^{27} \mod 34\\
&\equiv (43 \mod 34)^{27}\\
&\equiv 9^{27} \mod 34
\end{aligned}
$$

We stellen hier vast dat

$$
\begin{aligned}
\phi(34) &= \phi(2\cdot 17)\\
&= \phi(2)\cdot\phi(17),\ \text{daar ggd}(2,17)=1\\
&= (2-1)\cdot(17-1)=16,\ \text{daar } 2,\ 17\in\mathbb{P}
\end{aligned}
$$

waardoor

$$
\begin{aligned}
\left(8^5 \mod 55\right)^{27} \mod 34 &\equiv (9^{16} \mod 34)\cdot 9^{11},\ \text{met ggd}(9,34)=1\\
&\equiv 1\cdot 9^{11} \mod 34\\
&\equiv 9\cdot\left(9^2\right)^5 \mod 34\\
&\equiv 9\cdot(81 \mod 34)^5\\
&\equiv 9\cdot 13^5 \mod 34
\end{aligned}
$$

$$\begin{aligned} &\equiv (9\cdot 13)\cdot 13^2\cdot 13^2 \mod 34 \\ &\equiv (117 \mod 34)\cdot(169 \mod 34)\cdot(169 \mod 34) \\ &\equiv 15\cdot(-1)\cdot(-1) \mod 34 \equiv 15 \end{aligned}$$

Oefening 127

We bestuderen beide helften van een willekeurig RSA-sleutelpaar $\{k,K\}$.

- We noemen de privé sleutel k **goed gekozen** als

  $$1 < k < \phi(m) \text{ en } \text{ggd}(k,\phi(m)) = 1.$$

  We begrijpen namelijk dat een $k = 1$ gekozen wiskundig voldoet, maar cryptografisch geen versleuteling biedt. We weten dat voor alle $k \in \mathbb{Z}_{\phi(m)}$ gekozen, geldt dat $k < \phi(m)$. We herinneren eraan dat k^{-1} pas bestaat in $\mathbb{Z}_{\phi(m)}$ als $\text{ggd}(k,\phi(m)) = 1$.
- Daar we de publieke sleutel K berekenen als $K \equiv k^{-1} \mod \phi(m)$, volgt omwille van de beperking op k, voor deze sleutelhelft dezelfde beperking

  $$1 < K < \phi(m) \text{ en } \text{ggd}(K,\phi(m)) = 1.$$

1) $1 < 13 < \phi(2\cdot 17)$ en $\text{ggd}(13,16) = 1$, $\quad 1 < 5 < 16$ en $\text{ggd}(5,16) = 1$.
2) $1 < 27 < \phi(5\cdot 11)$ en $\text{ggd}(27,40) = 1$, $\quad 1 < 3 < 40$ en $\text{ggd}(3,40) = 1$.
3) $1 < 7 < \phi(19\cdot 23)$ en $\text{ggd}(7,396) = 1$, $\quad 1 < 283 < 396$ en $\text{ggd}(283,396) = 1$.

Oefening 128

1) $C \equiv 14 \mod 33$, $\quad M \equiv 14^3 \mod 33 \equiv 5$.
2) $C \equiv 57 \mod 77$, $\quad M \equiv 57^{53} \mod 77 \equiv 8$.

Oefening 129 $M \equiv 5 \mod 35$

Oefening 130

We berekenen $k \equiv 31^{-1} \mod \phi(3599)$ via het uitgebreide grootste gemene deler-algoritme. We stellen vooraf vast dat

$$\begin{aligned} \phi(3599) &= \phi(59\cdot 61) \\ &= \phi(59)\cdot\phi(61), \text{ daar } \text{ggd}(59,61) = 1 \\ &= (59-1)\cdot(61-1) = 3480, \text{ daar } 59,\ 61 \in \mathbb{P} \end{aligned}$$

Uit uggd$(3480,31)$ volgt

$$\begin{aligned} 4\cdot 3480 + (-449)\cdot 31 &= 1, \text{ of dus} \\ 4\cdot 3480 + (-449)\cdot 31 &\equiv 1 \mod 3480 \Leftrightarrow \\ (-449 \mod 3480)\cdot 31 &\equiv 1 \mod 3480 \Leftrightarrow \\ 3031\cdot 31 &\equiv 1 \mod 3480, \end{aligned}$$

waaruit we $k = 3031$ besluiten.

Oefening 131 Een nieuwe keuze van k'_B blijft veilig, tenzij het 'uitlekken' een succesvolle priemontbinding van m_B tot $p_B \cdot q_B$ inhield.

Oefening 132

Bewijs
We tonen het handtekenen aan via substitutie van de handtekening S_A in de machtsverheffing voor de ontsleuteling in de ring $(\mathbb{Z}_{m_A}, +, \cdot)$ en vereenvoudiging tot de vingerafdruk H_A.

$$\begin{aligned}
S_A^{K_A} \mod m_A &\equiv \left(H_A^{k_A} \mod m_A\right)^{K_A} \mod m_A \\
&\equiv H_A^{k_A \cdot K_A} \mod m_A, \text{ waaruit (zie pagina 243)} \\
&\equiv H_A^{1+\phi(m_A)\cdot l} \mod m_A \\
&\equiv H_A^1 \cdot H_A^{\phi(m_A)\cdot l} \mod m_A \\
&\equiv H_A \cdot (H_A^{\phi(m_A)})^l \mod m_A \\
&\equiv H_A \cdot (H_A^{\phi(m_A)} \mod m_A)^l, \text{ met } \gcd(H_A, m_A) = 1 \\
&\equiv H_A \cdot 1^l \equiv H_A
\end{aligned}$$

■

Oefening 133

1) $S_A \equiv 106 \mod 143$, $H_A \equiv 106^{11} \mod 143 \equiv 7$.
2) $S_A \equiv 128 \mod 527$, $H_A \equiv 128^{343} \mod 527 \equiv 2$.

Oefening 134 $H \equiv 1415 \mod 11413$

Oefening 135 We berekenen beide handtekeningen $S_1 \equiv 8^3 \mod 437 \equiv 75$ en $S_2 \equiv 9^3 \mod 437 \equiv 292$ en ontdekken de gevraagde vingerafdruk als $H_1 = 8$.

Oefening 136

1) We berekenen de handtekening machinaal als $S_D \equiv 163 \mod 437$.
2) We parallelliseren deze handtekening tot een pen-en-papier-versie ervan.

- We parallelliseren het machtsverheffen eerst naar twee kleinere grondtallen.

$$\begin{aligned}
220^{283} \mod 19 \cdot 23 &\Leftrightarrow (11^{283},\ 13^{283})_{\mathrm{r}} \mod (19, 23) \\
&\quad \downarrow \\
&\Leftrightarrow (11^{\ 13},\ 13^{\ 19})_{\mathrm{r}} \mod (19, 23) \\
&\Leftrightarrow (11, 2)_{\mathrm{r}} \mod (19, 23)
\end{aligned}$$

- Via de cryptografenmethode vinden we de macht $S_D \equiv 220^{283} \mod 19 \cdot 23$ van het grote getal 220, zonder omwegen als:

$$\begin{aligned} S_D &\equiv 11 \cdot 115 + 2 \cdot 323 \mod 19 \cdot 23 \\ &\equiv 1265 + 646 \mod 437 \equiv 1911 \mod 437 \equiv 163. \end{aligned}$$

11. DSA

Oefening 137

Bewijs

- De verzameling $\mathbb{Z}_{11}$ vormt de additieve commutatieve groep $(\mathbb{Z}_{11}, +)$ onder zijn plus-bewerking $(+ \mod 11)$, zie pagina 196.
- De verzameling $\mathbb{Z}_{11} \setminus \{0\}$ vormt de multiplicatieve commutatieve groep $(\mathbb{Z}_{11} \setminus \{0\}, \cdot)$ onder de maal-bewerking $(\cdot \mod 11)$:
  - De verzameling $\mathbb{Z}_{11} \setminus \{0\}$ is gesloten onder de maal-bewerking $(\cdot \mod 11)$, eventueel op te merken aan de resultaatzone van de cayleytabel. Dit wordt ons verzekerd door de afwezigheid van nuldelers in $\mathbb{Z}_{11} \setminus \{0\}$. Er bestaan geen $a,\ b \in \mathbb{Z}_{11} \setminus \{0\}$ waarvoor $a \cdot b \equiv 0 \mod 11$, daar hieruit zou volgen dat $a \cdot b \equiv 11 \mod 11$, wat in strijd is met de eigenschap van het priemgetal $11 \in \mathbb{P}$.
  - De maal-bewerking $(\cdot \mod 11)$ is associatief. Deze eigenschap is verzekerd door overerving via de gewone vermenigvuldiging uit $(\mathbb{Z}, \cdot)$.
  - De verzameling $\mathbb{Z}_{11} \setminus \{0\}$ bevat het neutraal element voor de maal-bewerking, eventueel te ontdekken in de cayleytabel $(\mathbb{Z}_{11} \setminus \{0\}, \cdot)$. De restklasse $1 \in \mathbb{Z}_{11} \setminus \{0\}$ wordt verzekerd door alle getallen in $\mathbb{Z}$ die rest 1 opleveren na deling door 11. De eigenschappen van de restklasse $1 \in \mathbb{Z}_{11} \setminus \{0\}$ worden doorgegeven door het neutraal element $1 \in (\mathbb{Z}, \cdot)$.
  - De verzameling $\mathbb{Z}_{11} \setminus \{0\}$ bevat van elk element ook invers element, eventueel op te baseren op het voorkomen van 1 in elke resultaatrij van de cayleytabel $(\mathbb{Z}_{11} \setminus \{0\}, \cdot)$. Voor elke restklasse $a \in \mathbb{Z}_{11} \setminus \{0\}$ zijn we verzekerd van zijn inverse restklasse $a^{-1} \in \mathbb{Z}_{11} \setminus \{0\}$, daar de bestaansvoorwaarde $\text{ggd}(a, 11) = 1$ is verzekerd. Doordat enerzijds uit $a \in \mathbb{Z}_{11} \setminus \{0\} = \{1, 2, 3, \ldots, 10\}$ volgt dat $1 \leqslant a < 11$ en de eigenschap van het priemgetal $11 \in \mathbb{P}$ anderzijds, is de onderlinge ondeelbaarheid van a en 11 verzekerd.
  - De commutativiteit van de maal-bewerking $(\cdot \mod 11)$ verkrijgen we door overerving vanuit $(\mathbb{Z}, \cdot)$.

- Dat er distributiviteit geldt van de maal-bewerking ten opzichte van de plus-bewerking in $(\mathbb{Z}_{11},+,\cdot)$, verkrijgen we ten slotte door overerving vanuit de commutatieve ring $(\mathbb{Z},+,\cdot)$.

We besluiten uit dit alles dat $(\mathbb{Z}_{11},+,\cdot)$ een eindig priemveld vormt. ■

Oefening 138

macht	0	1	2	3	4
1	0	1	2	3	4
2	0	1	4	4	1
3	0	1	3	2	4
4	0	1	1	1	1
$\in \mathbb{N}$	*orde*	*1*	*4*	*4*	*2*

Oefening 139

1) *Bewijs*
Uit

$$a^u \equiv 1 \mod p, \text{ voor de kleinste } u \in \mathbb{N}\backslash\{0\}, \text{ zie definitie (11.2)}$$

en

$$a^{\phi(p)} \equiv 1 \mod p, \text{ met } \text{ggd}(a,p) = 1, \text{ zie de stelling van Euler (10.4)}$$

volgt $u \leqslant \phi(p)$, waaruit $u \leqslant p-1$ volgt, daar $p \in \mathbb{P}$. ■

2) *Bewijs*
Uit de definitie van de rekenkundige orde $u \in \mathbb{N}\backslash\{0\}$ halen we achtereenvolgens

$$\begin{aligned}
a^u \equiv 1 \mod p &\Leftrightarrow a^u \cdot 1^k \equiv 1 \mod p, \text{ met } k < u \\
&\Leftrightarrow a^u \cdot (a^{\phi(p)})^k \equiv 1 \mod p, \text{ via de stelling van Euler (10.4)} \\
&\Leftrightarrow a^u \cdot (a^{p-1})^k \equiv 1 \mod p, \text{ daar } p \in \mathbb{P} \\
&\Leftrightarrow a^{u+k\cdot(p-1)} \equiv 1 \mod p \\
&\Leftrightarrow u + k\cdot(p-1) = 0 \\
&\Leftrightarrow u + k\cdot(p-1) \equiv 0 \mod u \\
&\Leftrightarrow k\cdot(p-1) \equiv 0 \mod u \\
&\Leftrightarrow p-1 \equiv 0 \mod u, \text{ daar } k < u \in \mathbb{N}\backslash\{0\} \\
&\Leftrightarrow p-1 \text{ is deelbaar door } u.
\end{aligned}$$

■

Oefening 140

Het priemveld $(\mathbb{Z}_{11},+,\cdot)$ telt

$$\phi(11-1) = \phi(10) = \phi(2\cdot 5) = \phi(2)\cdot\phi(5) = (2-1)\cdot(5-1) = 4$$

generatoren, daar $\text{ggd}(2,5) = 1$ en $2,\ 5 \in \mathbb{P}$. De tabel van de natuurlijke machten (zie pagina 259) in $\mathbb{Z}_{11}$ leert ons $\text{gen}(\mathbb{Z}_{11}) = \{2,6,7,8\}$.

Oefening 141 Zie pagina 258.

Oefening 142

1) 8

2) 4

3) 6

Oefening 143

1) *Bewijs:* zie pagina 42 bij wijze van hint.
Stellen we $x \equiv \text{dlog}_g(a) \mod (p-1)$ dan geldt $g^x \equiv a \mod p$, en analoog stemt $y \equiv \text{dlog}_g(b) \mod (p-1)$ overeen met $g^y \equiv b \mod p$. Substitueren we nu deze a en b in het gevraagde product, dan komt er

$$\text{dlog}_g(a \cdot b) \mod (p-1) \equiv \text{dlog}_g(g^x \cdot g^y) \equiv \text{dlog}_g(g^{x+y}).$$

Gebaseerd op de vuistregel 'logaritme is een exponent' besluiten we:
$\text{dlog}_g(g^{x+y}) \equiv x+y \mod (p-1)$. Met een terugsubstitutie verkrijgen we ten slotte

$$\text{dlog}_g(a \cdot b) \equiv x+y \equiv \text{dlog}_g(a) + \text{dlog}_g(b) \mod (p-1). \qquad \blacksquare$$

2) *Bewijs:* zie pagina 44 als hint.
Stellen we $x \equiv \text{dlog}_g(a^n) \mod (p-1)$ dan geldt $g^x \equiv a^n \mod p$, en op analoge manier volgt uit $y \equiv \text{dlog}_g(a) \mod (p-1)$ dat $g^y \equiv a \mod p$. Willen we nu a elimineren uit bovenstaande identiteiten, dan kunnen we bijvoorbeeld de tweede in de eerste substitueren zodat $g^x \equiv a^n \mod p \Rightarrow g^x \equiv (g^y)^n \Rightarrow g^x \equiv g^{y \cdot n}$ of $x \equiv n \cdot y \mod (p-1)$. Terugsubstitutie van x en y besluit het bewijs met

$$\text{dlog}_g(a^n) \equiv n \cdot \text{dlog}_g(a) \mod (p-1). \qquad \blacksquare$$

We gebruiken de rekenregels $\mod (p-1)$ voor discreet logaritmerekenen in $\mathbb{Z}_{11}$.

1) discrete logaritme versus product:

$$\begin{aligned} \text{dlog}_2(3 \cdot 5) \mod 11 &\equiv \text{dlog}_2(3) + \text{dlog}_2(5) \mod 10 \\ &\equiv 8+4 \mod 10, \text{ zie oefening 142} \\ &\equiv 12 \mod 10 \equiv 2. \end{aligned}$$

$$\begin{aligned} \text{We maken ook de proef als } 2^2 \mod 11 &\equiv 3 \cdot 5 \mod 11 \Leftrightarrow \\ 4 \mod 11 &\equiv 4 \mod 11. \end{aligned}$$

2) discrete logaritme van een macht:

$$\begin{aligned} \operatorname{dlog}_2(3^2) \mod 11 &\equiv 2 \cdot \operatorname{dlog}_2(3) \mod 10 \\ &\equiv 2 \cdot 8 \mod 10, \text{ zie oefening 142} \\ &\equiv 16 \mod 10 \equiv 6. \end{aligned}$$

$$\begin{aligned} \text{We maken ook de proef als } 2^6 \mod 11 &\equiv 3^2 \mod 11 \Leftrightarrow \\ 64 \mod 11 &\equiv 9 \mod 11 \Leftrightarrow \\ 9 \mod 11 &\equiv 9 \mod 11. \end{aligned}$$

Oefening 144

Alice berekent met haar privé sleutel $k_A = 6$ haar publieke $K_A \equiv 5^6 \mod 23 \equiv 8$, als macht van de generator. Alice beschikt hierdoor over haar sleutelpaar $\{k_A = 6,\ K_A = 8\}$.

Bob berekent met zijn privé sleutel $k_B = 15$ zijn publieke $K_B \equiv 5^{15} \mod 23 \equiv 19$. Bob beschikt hierdoor over zijn sleutelpaar $\{k_B = 15,\ K_B = 19\}$.

$$\begin{aligned} \text{Alice berekent } K &\equiv 19^6 \mod 23 \equiv 2 \quad \text{en} \\ \text{Bob berekent } K' &\equiv 8^{15} \mod 23 \equiv 2. \end{aligned}$$

De gelijkheid van beide machten $K \equiv K' \equiv 2 \mod 23$ bezorgt beide correspondenten hun veilig uitgewisselde symmetrische sleutel.

Oefening 145

Als kraker beschikken we over:

het priemveld	$(\mathbb{Z}_{11}, +, \cdot)$	met generator $2 \in \text{gen}(\mathbb{Z}_{11})$,
de publieke sleutels	$K_A = 9$ en $K_B = 3$	van Alice en Bob en
de werkwijze	$K \equiv 3^{k_A} \mod 11$	zonder k_A; enkel $9 \equiv 2^{k_A} \mod 11$.

Om de uitgewisselde sleutel K te achterhalen, moeten we ons toeleggen op het achterhalen van een privé sleutel zoals k_A. Zodra we hiertoe $9 \equiv 2^x \mod 11$ willen oplossen naar x, lopen we tegen de eenrichtingsfunctie $\text{dexp}_2 \mod 11$ aan. Een exponentiële vergelijking zoals $2^x \mod 11 \equiv 9$ oplossen naar x, komt overeen met de brute kracht aanval waarbij we alle mogelijke waarden voor $x \in \mathbb{Z}_{10}$ uitproberen.

$$\begin{aligned} 2^0 \mod 11 &\equiv 1 \\ 2^1 \mod 11 &\equiv 2 \\ 2^2 \mod 11 &\equiv 4 \end{aligned}$$

$$
\begin{array}{lll}
2^3 \mod 11 & \equiv & 8 \\
2^4 \mod 11 & \equiv & 5 \\
2^5 \mod 11 & \equiv & 10 \\
2^6 \mod 11 & \equiv & 9 \Rightarrow k_A = 6 \text{ en zo } K \equiv 3^6 \equiv 3 \mod 11 \\
\vdots & & \text{als het eindpunt van deze brute kracht aanval.} \\
2^9 \mod 11 & \equiv & 6, \text{ als theoretisch eindpunt.}
\end{array}
$$

Oefening 146

1) $K_A \mod 11 \equiv 8$ en $m_A \mod 10 \equiv 7$
2) $s_A \mod 10 \equiv 9$
3) $m_B \mod 10 \equiv 7$ bij de lokale vingerafdruk $H_B = 2$, impliceert zowel de authenticiteit als de integriteit van de zending.
4) $m_B \mod 10 \equiv 8$ bij de lokale vingerafdruk $H_B = 6$, waardoor noch authenticiteit noch integriteit zijn gewaarborgd.

Oefening 147

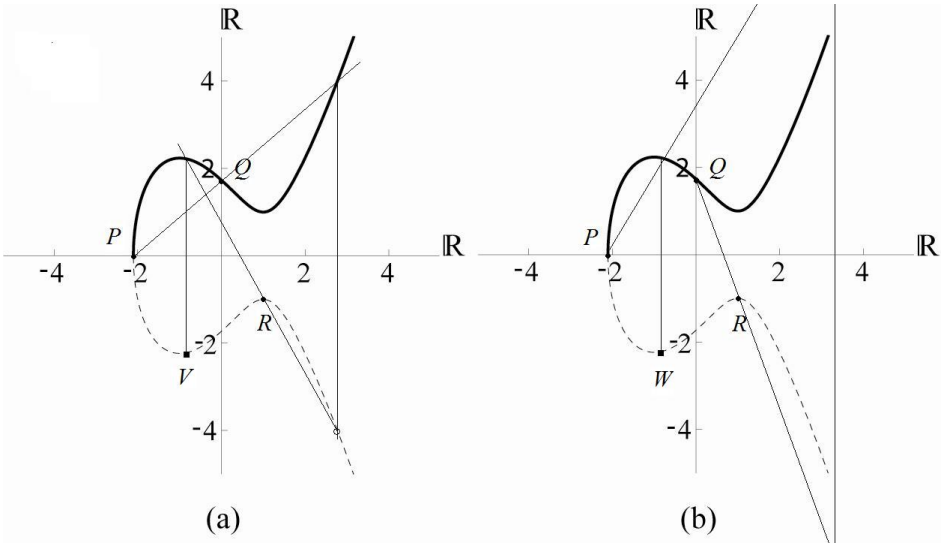
In tegenstelling tot de RSA-handtekening (zie formule (10.11)) bevat de DSA-handtekening (zie formule (11.11)) een random wegwerpsleutelpaar $\{k_O, m\}$.

Oefening 148

1) Alice's privé sleutel $k_A = 3$.
2) De gebruikte wegwerpsleutel $k_O = 7$.
3) Opnieuw vinden we $k_O = 7$.
4) Opnieuw vinden we $k_A = 3$.
5) Beide benaderingen blijken consistent.

12. Elliptische krommenversleuteling

Oefening 149



Oefening 150

Starten we van de definitie (12.3),

$$S = P \oplus Q \;\Leftrightarrow\; S = \text{ spiegelbeeld tegenover de } x\text{-as van } PQ \cap \mathbb{E},$$

dan volgt hieruit dat het spiegelbeeld tegenover de x-as van het sompunt $P \oplus Q$ gelijk is aan $PQ \cap \mathbb{E}$, wat als snijpunt uiteraard op de rechte PQ ligt. ■

Oefening 151

We beseffen dat een punt $P(r,0) \in x$-as op de symmetrie-as van de kromme $\mathbb{E}$ ligt. Het meetkundig tweevoud ervan vinden we via de definitie (12.3).

$$\begin{aligned} T &= 2 \odot P(r,0) \\ &= P(r,0) \oplus P(r,0) \Leftrightarrow T = \text{ spiegelbeeld tegenover de } x\text{-as van raaklijn } PP \cap \mathbb{E}, \\ &\qquad \text{en daar de raaklijn aan } \mathbb{E} \text{ door } P \text{ vertikaal is,} \\ &\qquad \text{is zijn snijpunt met } \mathbb{E} \cup \{\text{Zero}\} \text{ het punt Zero (zie pagina 278).} \\ &\Leftrightarrow T = \text{ spiegelbeeld tegenover } x\text{-as van Zero } = \text{ Zero} \quad \blacksquare \end{aligned}$$

Het meetkundig drievoud vinden we makkelijker als

$$\begin{aligned} 3 \odot P(r,0) &= 2 \odot P(r,0) \oplus P(r,0) \\ &= \text{Zero} \oplus P(r,0) = P(r,0). \end{aligned}$$

De meetkundige orde van een punt $P(r,0) \in x$-as is $u = 2$, volgens definitie (12.10).

Oefening 152

De kwadratische residu's staan telkens uitgerekend in de rechterkolom; de linkerkolom bevat de kleinste vierkantswortel ervan.

1) alle kwadratische residu's in $\mathbb{Z}_5$

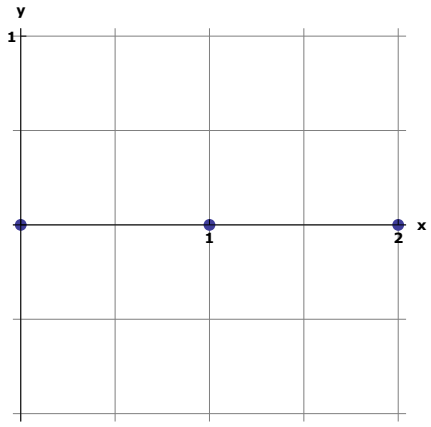
w	$w^2 \equiv r \mod 5$
0	$0^2 \equiv 0$
1	$1^2 \equiv 1$
2	$2^2 \equiv 4$

2) alle kwadratische residu's in $\mathbb{Z}_{11}$

w	$w^2 \equiv r \mod 11$
0	$0^2 \equiv 0$
1	$1^2 \equiv 1$
2	$2^2 \equiv 4$
3	$3^2 \equiv 9$
4	$4^2 \equiv 5$
5	$5^2 \equiv 3$

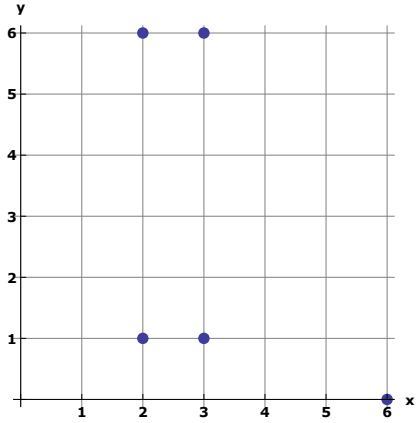
Oefening 153

1) PKD $\equiv 2 \mod 3$
$\#(\mathbb{E}_3(2,0)) = 3$



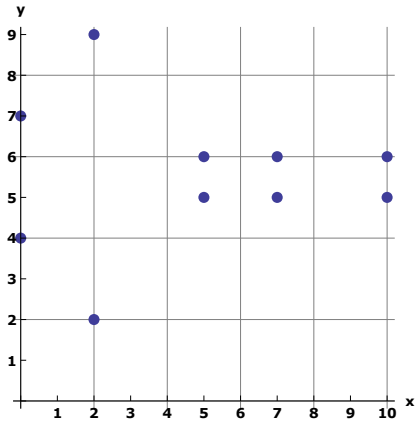
$\mathbb{E}_3(2,0) = \{(0,0),(0,1),(0,2)\}$

2) PKD $\equiv 2 \mod 7$
$\#(\mathbb{E}_7(2,3)) = 5 \approx 7$



$\mathbb{E}_7(2,3) = \{(2,1),(2,6),(3,1),(3,6),(6,0)\}$

3) PKD $\equiv 8 \mod 11$
$\#(\mathbb{E}_{11}(1,5)) = 10 \approx 11$



$\mathbb{E}_{11}(1,5) = \{(0,4),(0,7),(2,2),(2,9),(5,5),(5,6),(7,5),(7,6),(10,5),(10,6)\}$

Oefening 154

1) De priemkromme $E_2(1,0)$ met $2 \not\equiv 3 \mod 4$, en $\#(E_2(1,0)) = 2$.

x	$x^3+1x+0 \equiv y^2 \mod 2$	vierkantswortels $y \in \mathbb{Z}_2$	punten $P(x,y)$
0	$0^3+1\cdot 0+0 \equiv 0$	0	$(0,0)$
1	$1^3+1\cdot 1+0 \equiv 0$	0	$(1,0)$

2) De priemkromme $E_3(1,0)$ met $3 \equiv 3 \mod 4$, en (dus) $\#(E_3(1,0)) = 3$.

x	$x^3+1x+0 \equiv y^2 \mod 3$	vierkantswortels $y \in \mathbb{Z}_3$	punten $P(x,y)$
0	$0^3+1\cdot 0+0 \equiv 0$	0	$(0,0)$
1	$1^3+1\cdot 1+0 \equiv 2$		
2	$2^3+1\cdot 2+0 \equiv 1$	1 en $-1 \equiv 2$	$(2,1),(2,2)$

3) De priemkromme $E_5(1,0)$ met $5 \not\equiv 3 \mod 4$, en $\#(E_5(1,0)) \neq 5$.

x	$x^3+1x+0 \equiv y^2 \mod 5$	vierkantswortels $y \in \mathbb{Z}_5$	punten $P(x,y)$
0	$0^3+1\cdot 0+0 \equiv 0$	0	$(0,0)$
1	$1^3+1\cdot 1+0 \equiv 2$		
2	$2^3+1\cdot 2+0 \equiv 0$	0	$(2,0)$
3	$(-2)^3+1\cdot(-2)+0 \equiv 0$	0	$(3,0)$
4	$(-1)^3+1\cdot(-1)+0 \equiv 3$		

4) De priemkromme $E_7(1,0)$ met $7 \equiv 3 \mod 4$, en (dus) $\#(E_7(1,0)) = 7$.

x	$x^3+1x+0 \equiv y^2 \mod 7$	vierkantswortels $y \in \mathbb{Z}_7$	punten $P(x,y)$
0	$0^3+1\cdot 0+0 \equiv 0$	0	$(0,0)$
1	$1^3+1\cdot 1+0 \equiv 2$	3 en $-3 \equiv 4$	$(1,3),(1,4)$
2	$2^3+1\cdot 2+0 \equiv 3$		
3	$3^3+1\cdot 3+0 \equiv 2$	3 en $-3 \equiv 4$	$(3,3),(3,4)$
4	$(-3)^3+1\cdot(-3)+0 \equiv 5$		
5	$(-2)^3+1\cdot(-2)+0 \equiv 4$	2 en $-2 \equiv 5$	$(5,2),(5,5)$
6	$(-1)^3+1\cdot(-1)+0 \equiv 5$		

5) De priemkromme $E_{11}(1,0)$ met $11 \equiv 3 \mod 4$, en (dus) $\#(E_{11}(1,0)) = 11$.

x	$x^3+1x+0 \equiv y^2 \mod 11$	vierkantswortels $y \in \mathbb{Z}_{11}$	punten $P(x,y)$
0	$0^3+1\cdot 0+0 \equiv 0$	0	$(0,0)$
1	$1^3+1\cdot 1+0 \equiv 2$		
2	$2^3+1\cdot 2+0 \equiv 10$		
3	$3^3+1\cdot 3+0 \equiv 8$		
4	$4^3+1\cdot 4+0 \equiv 2$		
5	$5^3+1\cdot 5+0 \equiv 9$	3 en $-3 \equiv 8$	$(5,3),(5,8)$
6	$(-5)^3+1\cdot(-5)+0 \equiv 2$		
7	$(-4)^3+1\cdot(-4)+0 \equiv 9$	3 en $-3 \equiv 8$	$(7,3),(7,8)$
8	$(-3)^3+1\cdot(-3)+0 \equiv 3$	5 en $-5 \equiv 6$	$(8,5),(8,6)$
9	$(-2)^3+1\cdot(-2)+0 \equiv 1$	1 en $-1 \equiv 10$	$(9,1),(9,10)$
10	$(-1)^3+1\cdot(-1)+0 \equiv 9$	3 en $-3 \equiv 8$	$(10,3),(10,8)$

Oefening 155

Neen, daar de PKD $\equiv 4\cdot 10^3+27\cdot 5^2 \mod 17 \equiv 0$, is de priemkromme singulier.

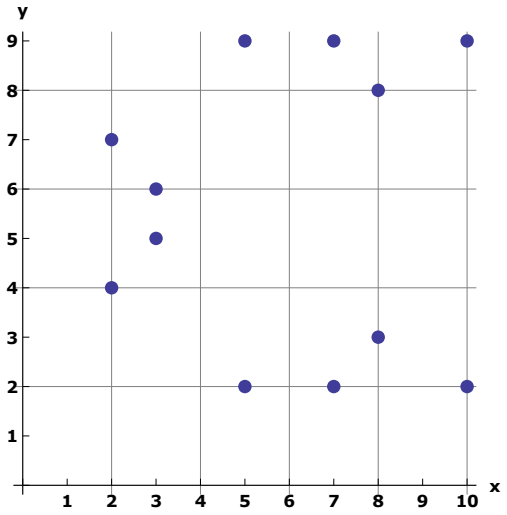
Oefening 156

De punten van de priemkromme $E_{11}(1,6)$.

x	$x^3+1x+6 \equiv y^2 \mod 11$	vierkantswortels $y \in \mathbb{Z}_{11}$	punten $P(x,y)$
0	$0^3+1\cdot 0+6 \equiv 6$		
1	$1^3+1\cdot 1+6 \equiv 8$		
2	$2^3+1\cdot 2+6 \equiv 5$	4 en $-4 \equiv 7$	$(2,4),(2,7)$
3	$3^3+1\cdot 3+6 \equiv 3$	5 en $-5 \equiv 6$	$(3,5),(3,6)$
4	$4^3+1\cdot 4+6 \equiv 8$		
5	$5^3+1\cdot 5+6 \equiv 4$	2 en $-2 \equiv 9$	$(5,2),(5,9)$
6	$(-5)^3+1\cdot(-5)+6 \equiv 8$		
7	$(-4)^3+1\cdot(-4)+6 \equiv 4$	2 en $-2 \equiv 9$	$(7,2),(7,9)$
8	$(-3)^3+1\cdot(-3)+6 \equiv 9$	3 en $-3 \equiv 8$	$(8,3),(8,8)$
9	$(-2)^3+1\cdot(-2)+6 \equiv 7$		
10	$(-1)^3+1\cdot(-1)+6 \equiv 4$	2 en $-2 \equiv 9$	$(10,2),(10,9)$

$(12+1)\odot G(2,7) = \text{Zero}$,
daar $\#(\mathbb{E}_{11}(1,6)) = 12$.

(zie pagina 286)



Oefening 157

1) We illustreren de eigenschap voor $k=2$ en $l=3$.

$$\begin{aligned} 2\odot(3\odot P) &= (3\odot P)\oplus(3\odot P) \\ &= (P\oplus P\oplus P)\oplus(P\oplus P\oplus P) \\ &= 6\odot P = (2\cdot 3)\odot P \end{aligned}$$

2) We illustreren de eigenschap voor $k = 3$ en $l = 2$.

$$\begin{aligned} 3 \odot (2 \odot P) &= (2 \odot P) \oplus (2 \odot P) \oplus (2 \odot P) \\ &= (P \oplus P) \oplus (P \oplus P) \oplus (P \oplus P) \\ &= 6 \odot P = (3 \cdot 2) \odot P \end{aligned}$$

Op grond van deze illustratie vermoeden we de commutativiteit

$$k \odot (l \odot P) = l \odot (k \odot P)$$

3) We bewijzen zowel de eigenschap als de commutativiteit ervan.

$$\begin{aligned} k \odot (l \odot P) &= \underbrace{(l \odot P) \oplus (l \odot P) \oplus \ldots \oplus (l \odot P)}_{k \text{ termen}} \\ &= \underbrace{\underbrace{(P \oplus P \oplus \ldots \oplus P)}_{l \text{ termen}} \oplus \underbrace{(P \oplus P \oplus \ldots \oplus P)}_{l \text{ termen}} \oplus \ldots \oplus \underbrace{(P \oplus P \oplus \ldots \oplus P)}_{l \text{ termen}}}_{k \text{ termen}} \\ &= \underbrace{(P \oplus P \oplus \ldots \oplus P) \oplus (P \oplus P \oplus \ldots \oplus P) \oplus \ldots \oplus (P \oplus P \oplus \ldots \oplus P)}_{k \cdot l \text{ termen}} \\ &= (k \cdot l) \odot P \\ &= (l \cdot k) \odot P, \text{ wegens de commutativiteit in } (\mathbb{N}, \cdot) \end{aligned}$$

■

Oefening 158

1) We gaan alle validatiestappen na voor $K_A(17,4)$ op $\mathbb{E}_{31}(3,12) \cup \{\text{Zero}\}$.

$$\begin{aligned} K_A(17,4) &\neq \text{Zero} \\ 17^3 + 3 \cdot 17 + 12 &\equiv 4^2 \mod 31 \Leftrightarrow \\ 16 &\equiv 16 \mod 31 \Leftrightarrow \\ 30 \odot K_A(17,4) &= \text{Zero}, \text{ zie pagina 287.} \end{aligned}$$

2) We gaan alle validatiestappen na voor $K_B(16,23)$ op $\mathbb{E}_{31}(3,12) \cup \{\text{Zero}\}$.

$$\begin{aligned} K_B(16,23) &\neq \text{Zero} \\ 16^3 + 3 \cdot 16 + 12 &\equiv 23^2 \mod 31 \Leftrightarrow \\ 2 &\equiv 2 \mod 31 \Leftrightarrow \\ 30 \odot K_B(16,23) &= 30 \odot (6 \odot G(13,4)), \text{ zie pagina 292} \\ &= 6 \odot (30 \odot G(13,4)), \text{ zie oefening 157} \\ &= 6 \odot \text{Zero}, \text{ zie pagina 288} \\ &= \text{Zero}. \end{aligned}$$

3) We gaan alle validatiestappen na voor $K(1,4)$ op $\mathbb{E}_{31}(3,12) \cup \{\text{Zero}\}$.

$$\begin{aligned} K(1,4) &\neq \text{Zero} \\ 1^3+3\cdot 1+12 &\equiv 4^2 \mod 31 \Leftrightarrow \\ 16 &\equiv 16 \mod 31 \Leftrightarrow \\ 30 \odot K(1,4) &= 30 \odot (17 \odot K_B(16,23)), \text{ zie pagina 295} \\ &= 17 \odot (30 \odot K_B(16,23)), \text{ zie oefening 157} \\ &= 17 \odot \text{Zero}, \text{ zie oefening 158-2} \\ &= \text{Zero}. \end{aligned}$$

4) We bewijzen de derde validatiestap voor elk sleutelpunt $K = k \odot G$.

$$\begin{aligned} u \odot K &= u \odot (k \odot G) \\ &= k \odot (u \odot G), \text{ zie oefening 157} \\ &= k \odot \text{Zero}, \text{ daar } u \text{ de orde is van } G \\ &= \text{Zero} \end{aligned}$$

■

13. AES

Oefening 159

1) We gaan de kardinaliteit $\#(\mathbb{F}_{2^3}) = 2^3 = 8$ na door opsomming:

$$\mathbb{F}_{2^3} = \{0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1\}$$

2) We gaan de kardinaliteit $\#(\mathbb{F}_{3^2}) = 3^2 = 9$ na door opsomming:

$$\mathbb{F}_{3^2} = \{0,\ 1,\ 2,\ x,\ x+1,\ x+2,\ 2x,\ 2x+1,\ 2x+2\}$$

3) We gaan de kardinaliteit $\#(\mathbb{F}_{5^2}) = 5^2 = 25$ na door opsomming:

$$\begin{aligned} \mathbb{F}_{5^2} = \{&0,\ 1,\ 2,\ 3,\ 4,\ x,\ x+1,\ x+2,\ x+3,\ x+4,\ 2x,\ 2x+1,\ 2x+2,\ 2x+3,\ 2x+4, \\ &3x,\ 3x+1,\ 3x+2,\ 3x+3,\ 3x+4,\ 4x,\ 4x+1,\ 4x+2,\ 4x+3,\ 4x+4\} \end{aligned}$$

4) We gaan de kardinaliteit $\#(\mathbb{F}_{3^3}) = 3^3 = 27$ na door opsomming:

$$\begin{aligned} \mathbb{F}_{3^3} = \{&0,\ 1,\ 2,\ x,\ x+1,\ x+2,\ 2x,\ 2x+1,\ 2x+2,\ x^2,\ x^2+1,\ x^2+2, \\ &x^2+x,\ x^2+x+1,\ x^2+x+2,\ x^2+2x,\ x^2+2x+1,\ x^2+2x+2, \\ &2x^2,\ 2x^2+1,\ 2x^2+2,\ 2x^2+x,\ 2x^2+x+1,\ 2x^2+x+2, \\ &2x^2+2x,\ 2x^2+2x+1,\ 2x^2+2x+2\} \end{aligned}$$

Oefening 160

Voor $\mathbb{F}_{2^2}$ met $P(x) = x^2 + x + 1 \mod 2$ komt er:

element	tegengesteld	invers
0	0	geen
1	1	1
x	x	$x+1$
$x+1$	$x+1$	x

Oefening 161

In $\mathbb{F}_{2^4}$ met $P(x) = x^4 + x + 1 \mod 2$ komt er:

1) x^3
2) $x^3 + 1$
3) $x^3 + x^2 + x$

In $\mathbb{F}_{2^4}$ met $P(x) = x^4 + x^3 + 1 \mod 2$ komt er:

1) x^3
2) $x^3 + x$
3) x^2

Oefening 162

In $\mathbb{F}_{2^8}$ van AES met $P(x) = x^8 + x^4 + x^3 + x + 1 \mod 2$ komt er:

1) $x^7 + x^6 + x^5 + x$
2) $x^7 + x^6 + x^5 + x^3 + x^2 + x$
3) $x^5 + x^4 + x^3 + x^2$

Oefening 163

In $\mathbb{F}_{2^8}$ van AES met $P(x) = x^8 + x^4 + x^3 + x + 1 \mod 2$ komt er:

1) $(x^6 + x^4 + x^3 + x + 1) \cdot (x^7 + x^6 + x^5 + x^4) \equiv 1$, en AES-substituent $s(x) = (39)_{\text{h}}$
2) $(x^6 + x^3 + x + 1) \cdot (x^4 + x + 1) \equiv 1$, en AES-substituent $s(x) = (\text{B3})_{\text{h}}$
3) $(x^7 + x^4 + x^2 + 1) \cdot (x^7 + x^3 + x) \equiv 1$, en AES-substituent $s(x) = (2\text{A})_{\text{h}}$

Oefening 164 We berekenen de derde kolom van de AES-toestand $M^{(i)}$ als:

$$M^{(i)} \overset{\text{mod } P(x)}{\equiv} \begin{pmatrix} \ddots & & 48 & \\ & \dots & \text{F8} & \\ & & \text{D3} & \\ & & \text{7A} & \dots \end{pmatrix}_{\text{h}}.$$

Oefening 165 We berekenen de uitgaande AES-toestand $A^{(i)}$ als:

$$A^{(i)} \overset{\text{mod } 2}{\equiv} \begin{pmatrix} \text{6C} & \text{3C} & \text{E7} & \text{0C} \\ \text{7C} & \text{EC} & \text{01} & \text{01} \\ \text{05} & \text{9A} & \text{1B} & \text{0F} \\ \text{EA} & \text{43} & \text{94} & \text{15} \end{pmatrix}_{\text{h}}.$$

Oefening 166

We berekenen de tien rondenveeltermen $r(x)$ in $\mathbb{F}_{2^8}$ van AES met $P(x) = x^8 + x^4 + x^3 + x + 1 \mod 2$ als:

ronde	$j \equiv 1 \mod 4$	rondeveelterm $r(x)$
1	5	$x^{\frac{5-5}{4}} \equiv x^0 \equiv 1$
2	9	$x^{\frac{9-5}{4}} \equiv x^1 \equiv x$
3	13	$x^{\frac{13-5}{4}} \equiv x^2$
4	17	$x^{\frac{17-5}{4}} \equiv x^3$
5	21	$x^{\frac{21-5}{4}} \equiv x^4$
6	25	$x^{\frac{25-5}{4}} \equiv x^5$
7	29	$x^{\frac{29-5}{4}} \equiv x^6$
8	33	$x^{\frac{33-5}{4}} \equiv x^7$
9	37	$x^{\frac{37-5}{4}} \equiv x^8 \overset{\text{mod } P(x)}{\equiv} x^8 - (x^8 + x^4 + x^3 + x + 1) \equiv x^4 + x^3 + x + 1$
10	41	$x^{\frac{41-5}{4}} \equiv x^9 \overset{\text{mod } P(x)}{\equiv} x^9 - x \cdot (x^8 + x^4 + x^3 + x + 1) \equiv x^5 + x^4 + x^2 + x$

Oefening 167

In $\mathbb{F}_{2^8}$ van AES met $P(x) = x^8 + x^4 + x^3 + x + 1 \mod 2$ komt er:

1) $g(x) = (\text{F0})_{\text{h}}$, met $g(x) \cdot s(x) \equiv (x^7 + x^6 + x^5 + x^4) \cdot (x^6 + x^4 + x^3 + x + 1) \equiv 1$
2) $g(x) = (13)_{\text{h}}$, met $g(x) \cdot s(x) \equiv (x^4 + x + 1) \cdot (x^6 + x^3 + x + 1) \equiv 1$
3) $g(x) = (\text{8A})_{\text{h}}$, met $g(x) \cdot s(x) \equiv (x^7 + x^3 + x) \cdot (x^7 + x^4 + x^2 + 1) \equiv 1$

Oefening 168

Bewijs
Het vereenvoudigen (mod 2) van de coëfficiëntentransformatie na de omgekeerde coëfficiëntentransformatie, toont:

$$\begin{pmatrix} 0&0&1&0&0&1&0&1\\ 1&0&0&1&0&0&1&0\\ 0&1&0&0&1&0&0&1\\ 1&0&1&0&0&1&0&0\\ 0&1&0&1&0&0&1&0\\ 0&0&1&0&1&0&0&1\\ 1&0&0&1&0&1&0&0\\ 0&1&0&0&1&0&1&0 \end{pmatrix} \cdot \left(\begin{pmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{pmatrix} \cdot \begin{pmatrix} \beta_0\\ \beta_1\\ \beta_2\\ \beta_3\\ \beta_4\\ \beta_5\\ \beta_6\\ \beta_7 \end{pmatrix} + \begin{pmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{pmatrix} \right) + \begin{pmatrix} 1\\0\\1\\0\\0\\0\\0\\0 \end{pmatrix} \overset{\text{mod } 2}{\equiv} \begin{pmatrix} \beta_0\\ \beta_1\\ \beta_2\\ \beta_3\\ \beta_4\\ \beta_5\\ \beta_6\\ \beta_7 \end{pmatrix}$$

■

Oefening 169

Bewijs
Het matrixvermenigvuldigen van M_{AES} met $M_{\text{AES}^{-1}}$ in $\mathbb{F}_{2^8}^{4\times 4}$,
met $P(x) = x^8 + x^4 + x^3 + x + 1 \mod 2$ toont:

$$\begin{pmatrix} x & x+1 & 1 & 1\\ 1 & x & x+1 & 1\\ 1 & 1 & x & x+1\\ x+1 & 1 & 1 & x \end{pmatrix} \cdot \begin{pmatrix} x^3+x^2+x & x^3+x+1 & x^3+x^2+1 & x^3+1\\ x^3+1 & x^3+x^2+x & x^3+x+1 & x^3+x^2+1\\ x^3+x^2+1 & x^3+1 & x^3+x^2+x & x^3+x+1\\ x^3+x+1 & x^3+x^2+1 & x^3+1 & x^3+x^2+x \end{pmatrix}$$

$$\overset{\text{mod } P(x)}{\equiv} \begin{pmatrix} 1&0&0&0\\ 0&1&0&1\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}$$

■

14. Inleiding tot codes

Oefening 170

Daar per cijferrij slechts één van de elf mogelijke resten (namelijk 0) na deling door 11 wordt aanvaard voor een geldig rekeningnummer, kan slechts 1 op de 11 cijferrijen een Nederlands rekeningnummer vormen, met name $\frac{1}{11} \approx 9\%$.

Oefening 171

1) ongeldig 2) geldig 3) geldig

Oefening 172

1) $x \equiv 8 \mod 11$ 2) $x \equiv 3 \mod 11$ 3) $x \equiv 9 \mod 11$

Oefening 173

Voor $P14351501539$ geldt $16+1+4+3+5+1+5+0+1+5+3+9 \equiv 8 \mod 9$ wat het tot een geldig serienummer voor een eurobiljet maakt.

Oefening 174

1) zie pagina 345
2) $w = 11\ 011$

Oefening 175

Daar $d = 2$ is de code 1-bitfoutdetecterend en zonder correctievermogen.

Oefening 176

1) $C(5,2,5) = \{00\ 000, 11\ 111\}$ met $E = 20\%$
2) $d = 5$, dus een 4-bitfoutdetecterende en 2-bitfoutcorrigerende code
3) $w = 00\ 000$
4) $w = 11\ 111$
5) $F = \{10\ 000, 01\ 000, 00\ 100, 00\ 010, 00\ 001, 11\ 000, 01\ 100, 00\ 110, 00\ 011,$
$10\ 100, 01\ 010, 00\ 101, 10\ 010, 01\ 001, 10\ 001\}$

Oefening 177

1) $E = 33\%$
2) $d = 3$, dus een 2-bitfoutdetecterende en 1-bitfoutcorrigerende code
3) $w = 10\ 1010$
4) $F = \{10\ 0000, 01\ 0000, 00\ 1000, 00\ 0100, 00\ 0010, 00\ 0001\}$

Oefening 178

1) $C(6,8,2) = \{000\ 000, 001\ 001, 010\ 010, 011\ 011, 100\ 100, 101\ 101, 110\ 110, 111\ 111\}$ met $E = 50\%$
2) $d = 2$, dus een 1-bitfoutdetecterende en niet-corrigerende code
3) $F = \{\ \}$

15. Lineaire codes

Oefening 179

C is geen lineaire code daar het nulcodewoord $\vec{o} \notin C$

Oefening 180

$$\begin{array}{lcl} \vec{w}_0 & \equiv & 1\cdot\vec{w}_1 + 1\cdot\vec{w}_1 \\ \vec{w}_0 & \equiv & 0\cdot\vec{w}_1 + 0\cdot\vec{w}_2 \\ \vec{w}_0 & \equiv & 1\cdot\vec{w}_1 + 1\cdot\vec{w}_2 + 1\cdot\vec{w}_3 \end{array}$$

Oefening 181

1) We gaan na dat $C = \{(0,0,0,0),\ (0,1,0,1),\ (1,0,1,0),\ (1,1,1,1)\}$ lineair is:

$$\begin{array}{lcl} (0,0,0,0)+\vec{w}_i & \equiv & \vec{w}_i \in C, \\ (0,1,0,1)+(1,0,1,0) & \equiv & (1,1,1,1) \in C, \\ (0,1,0,1)+(1,1,1,1) & \equiv & (1,0,1,0) \in C, \\ (1,0,1,0)+(1,1,1,1) & \equiv & (0,1,0,1) \in C. \end{array}$$

2) We vinden $d = 2$ via de hamming gewichten van de codewoorden.

codewoord	hamming gewicht
$\vec{w}_0$	$\text{hwt}(\vec{w}_0) = \text{hwt}(0,0,0,0) = 0$
$\vec{w}_1$	$\text{hwt}(\vec{w}_1) = \text{hwt}(0,1,0,1) = 2$
$\vec{w}_2$	$\text{hwt}(\vec{w}_2) = \text{hwt}(1,0,1,0) = 2$
$\vec{w}_3$	$\text{hwt}(\vec{w}_3) = \text{hwt}(1,1,1,1) = 4$
	$d = \min_{i\neq 0}(\text{hwt}(\vec{w}_i)) = 2$

3) $C(6,4,2)$ blijkt dus een 1-bitfoutdetecterende en niet-corrigerende code.

4) $F = \{\ \}$

Oefening 182

1) We bepalen de canonieke generatormatrix als

$$G_{can} \equiv \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

2) We vinden $d = 2$ via de hamming gewichten van de codewoorden.

codewoord	hamming gewicht
$\vec{w}_0$	$\text{hwt}(\vec{w}_0) = \text{hwt}(0,0,0,0,0,0) = 0$
$\vec{w}_1$	$\text{hwt}(\vec{w}_1) = \text{hwt}(0,0,1,0,0,1) = 2$
$\vec{w}_2$	$\text{hwt}(\vec{w}_2) = \text{hwt}(0,1,0,0,1,0) = 2$
$\vec{w}_3$	$\text{hwt}(\vec{w}_3) = \text{hwt}(0,1,1,0,1,1) = 4$
$\vec{w}_4$	$\text{hwt}(\vec{w}_4) = \text{hwt}(1,0,0,1,0,0) = 2$
$\vec{w}_5$	$\text{hwt}(\vec{w}_5) = \text{hwt}(1,0,1,1,0,1) = 4$
$\vec{w}_6$	$\text{hwt}(\vec{w}_6) = \text{hwt}(1,1,0,1,1,0) = 4$
$\vec{w}_7$	$\text{hwt}(\vec{w}_7) = \text{hwt}(1,1,1,1,1,1) = 6$
	$d = \min_{i \neq 0}(\text{hwt}(\vec{w}_i)) = 2$

3) $C[6,3,2]$ blijkt dus een 1-bitfoutdetecterende en niet-corrigerende code.

4) We vinden de canonieke pariteittester als

$$H_{can} \equiv \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

5) We detecteren de fout bij ontvangst van $\vec{r} \equiv (1,0,1,1,0,0)$ via een van de nulvector verschillend syndroom als

$$S(\vec{r}) \equiv S((1,0,1,1,0,0)) \overset{\text{mod } 2}{\equiv} (1\ 0\ 1\ 1\ 0\ 0) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{\text{mod } 2}{\equiv} (0\ 0\ 1) \not\equiv \vec{o}.$$

De vermeende foutcorrectie steunt theoretisch op de hamming afstanden van de ontvangen $\vec{r} \equiv (1,0,1,1,0,0)$ *ten opzichte van* de codewoorden uit $C[6,3,2]$. Met $\text{hmd}((1,0,1,1,0,0),(1,0,1,1,0,1)) = 1$, $\text{hmd}((1,0,1,1,0,0),(1,0,0,1,0,0)) = 1$, blijkt 'de' dichtste buur van $\vec{r}$ in $C[6,3,2]$ echter onbeslist.

Oefening 183

1) zie pagina 367

2) $(1\ 0\ 0)$

Oefening 184

1) $E = 50\%$, kardinaliteit $\#C = 2^3 = 8$ en

$$\begin{aligned} C &= \{(0,0,0,0,0,0),(0,0,1,0,1,1),(0,1,0,1,0,1),(0,1,1,1,1,0),\\ &\quad (1,0,0,1,1,0),(1,0,1,1,0,1),(1,1,0,0,1,1),(1,1,1,0,0,0)\} \end{aligned}$$

2) We vinden $d = 3$ via de hamming gewichten van de codewoorden.

codewoord	hamming gewicht
$\vec{w}_0$	$\text{hwt}(\vec{w}_0) = \text{hwt}(0,0,0,0,0,0) = 0$
$\vec{w}_1$	$\text{hwt}(\vec{w}_1) = \text{hwt}(0,0,1,0,1,1) = 3$
$\vec{w}_2$	$\text{hwt}(\vec{w}_2) = \text{hwt}(0,1,0,1,0,1) = 3$
$\vec{w}_3$	$\text{hwt}(\vec{w}_3) = \text{hwt}(0,1,1,1,1,0) = 4$
$\vec{w}_4$	$\text{hwt}(\vec{w}_4) = \text{hwt}(1,0,0,1,1,0) = 3$
$\vec{w}_5$	$\text{hwt}(\vec{w}_5) = \text{hwt}(1,0,1,1,0,1) = 4$
$\vec{w}_6$	$\text{hwt}(\vec{w}_6) = \text{hwt}(1,1,0,0,1,1) = 4$
$\vec{w}_7$	$\text{hwt}(\vec{w}_7) = \text{hwt}(1,1,1,0,0,0) = 3$
	$d = \min_{i\neq 0}(\text{hwt}(\vec{w}_i)) = 3$

Als corrigeerbaar ruistype vinden we hierdoor

$$\begin{aligned} F &= \{(1,0,0,0,0,0),(0,1,0,0,0,0),(0,0,1,0,0,0),(0,0,0,1,0,0),\\ &\quad (0,0,0,0,1,0),(0,0,0,0,0,1)\}. \end{aligned}$$

3) We vinden de canonieke pariteittester als

$$H_{can} \equiv \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

4) We corrigeren de fout bij ontvangst van $\vec{r} \equiv (1,0,1,1,0,0)$ waarbij

$$S(\vec{r}) \equiv S((1,0,1,1,0,0)) \overset{\text{mod } 2}{\equiv} (1\ 0\ 1\ 1\ 0\ 0) \cdot \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{\text{mod } 2}{\equiv} (0\ 0\ 1),$$

betekent, daar ook voor $\vec{f} = (0,0,0,0,0,1)$ geldt dat

$$S(\vec{f}) \equiv S((0,0,0,0,0,1)) \overset{\text{mod } 2}{\equiv} (0\ 0\ 1),$$

we hieruit $S(\vec{r}) \equiv S(\vec{f})$ besluiten. Hierdoor corrigeren we de ontvangen $\vec{r}$ als

$$\vec{r} - \vec{f} \equiv (1,0,1,1,0,0) - (0,0,0,0,0,1) \overset{\text{mod } 2}{\equiv} (1,0,1,1,0,1).$$

We decoderen ten slotte codewoord $(1,0,1,1,0,1) \in C$ tot bericht $(1,0,1) \in M$ via een met de generatormatrix G voorberekende (de)codeertabel, volgens

$$\vec{w}_i \overset{\text{mod } 2}{\equiv} \vec{m}_i \cdot G_{can}.$$

Oefening 185

1) $(0,0,0,0,0,0,0,0)$
2) $(1,0,0,0,1,0,1,0)$

Oefening 186

$\#(H(1)) = 1$, $E = 0\%$
$\#(H(2)) = 2$, $E = 33\%$
$\#(H(3)) = 16$, $E = 57\%$
$\#(H(4)) = 2048$, $E = 73\%$
$\#(H(5)) = 67108864$, $E = 84\%$

Oefening 187

1) $(0,1,0)$
2) $(0,0,1)$

16. Cyclische tests

Oefening 188

1) ongeldig
2) geldig
3) ongeldig

Oefening 189

De gestructureerde mededeling bevat een fout.

Oefening 190

We noteren alle Belgische (geldige) bankrekeningnummers zoals op pagina 381.

$$(x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10})_{\text{dec}} \overset{\text{mod } 97}{\equiv} (x_{11}x_{12})_{\text{dec}} \iff$$

$$10^9x_1+10^8x_2+10^7x_3+10^6x_4+10^5x_5+10^4x_6+10^3x_7+10^2x_8+10x_9+x_{10} \overset{\text{mod } 97}{\equiv} 10x_{11}+x_{12}$$

1) We tonen aan dat er geen twee Belgische (geldige) bankrekeningnummers zijn die op precies één positie van elkaar verschillen.
Bewijs:
We veronderstellen dat we naast het voorgaande toch een nummer vinden zoals

$$(x_1x_2x_3x_4y_5x_6x_7x_8x_9x_{10})_{\text{dec}} \overset{\text{mod } 97}{\equiv} (x_{11}x_{12})_{\text{dec}}.$$

Dan vinden we het verschil tussen hun beide congruenties (zie formule (7.4)) als

$$\begin{aligned}
(10^5 \mod 97)(x_5-y_5) &\equiv 0 \Leftrightarrow \\
90(x_5-y_5) &\equiv 0 \mod 97 \Leftrightarrow \\
90^{-1}\cdot 90(x_5-y_5) &\equiv 90^{-1}\cdot 0 \mod 97, \text{ daar ggd}(90,97)=1 \Leftrightarrow \\
1\cdot(x_5-y_5) &\equiv 0 \mod 97 \Leftrightarrow \\
x_5 &\equiv y_5 \mod 97.
\end{aligned}$$

Bovenstaande redenering blijft als bewijs gelden voor elke positie. ■

2) We bewijzen dat er Belgische (geldige) bankrekeningnummers bestaan die op precies twee posities van elkaar verschillen.
Bewijs:
We veronderstellen dat we naast het voorgaande toch een nummer vinden zoals

$$(x_1x_2x_3x_4y_5x_6x_7x_8x_9x_{10})_{\text{dec}} \overset{\text{mod } 97}{\equiv} (y_{11}x_{12})_{\text{dec}}.$$

Dan vinden we het verschil tussen hun beide congruenties (zie formule (7.4)) als

$$\begin{aligned}
10^5(x_5-y_5) &\equiv 10(x_{11}-y_{11}) \mod 97 \Leftrightarrow \\
90(x_5-y_5) &\equiv 10(x_{11}-y_{11}) \mod 97 \Leftrightarrow \\
10^{-1}\cdot 90(x_5-y_5) &\equiv 10^{-1}\cdot 10(x_{11}-y_{11}) \mod 97, \text{ daar ggd}(10,97)=1 \Leftrightarrow \\
9\cdot(x_5-y_5) &\equiv 1\cdot(x_{11}-y_{11}) \mod 97 \Leftrightarrow \\
9(x_5-y_5) &= x_{11}-y_{11}, \text{ met } x_i,y_i \in \{0,1,\ldots,9\} \Leftrightarrow \\
x_5-y_5=1 &\text{ als } x_{11}=9, y_{11}=0 \text{ en} \\
x_5=9, y_5=8 &\text{ of } x_5=8, y_5=7 \text{ of } \ldots \text{ of } x_5=1, y_5=0.
\end{aligned}$$

Bovenstaande redenering blijft succesvol uitwerkbaar voor andere posities. ■

Oefening 191

1) $T(x)=x^7+x^6+x^5+x^4+x^2+1=(\text{F5})_{\text{h}}$
2) $W(x)=x^{13}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^2+1$

Oefening 192

1) $T(x) = x^3 + x^2 + x = (0\text{E})_\text{h}$
2) $W(x) = x^{23} + x^{17} + x^{15} + x^{10} + x^8 + x^3 + x^2 + x$
   $V(x) = x^{23} + x^{17} + x^{15} + x^{13} + x^{10} + x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$
3) $R(x) = x^4 + x = (12)_\text{h}$

Oefening 193

1) $T(x) = x^4 + x + 1 = (13)_\text{h}$
2) $W(x) = x^8 + x^7 + x^6 + x^4 + x + 1$
   $V(x) = x^8 + x^4 + x^3 + x^2 + x + 1$
3) $R(x) = x^4 + x = (12)_\text{h}$

Oefening 194

1) $M_1(x) = (x^9 + x^7 + x^6 + x^5 + x^4) + (x^6 + x + 1)$,
   $M_2(x) = (x^9 + x^7 + x^6 + x^5 + x^4) + x \cdot (x^6 + x + 1)$,
   $M_3(x) = (x^9 + x^7 + x^6 + x^5 + x^4) + (x^2 + 1) \cdot (x^6 + x + 1)$.
2) $W_1(x) = (x^{15} + x^{13} + x^{12} + x^{11} + x^{10} + x^5 + x^4 + x^2) + (x^6 + x + 1)^2$,
   $W_2(x) = (x^{15} + x^{13} + x^{12} + x^{11} + x^{10} + x^5 + x^4 + x^2) + (x + 1) \cdot (x^6 + x + 1)$,
   $W_3(x) = (x^{15} + x^{13} + x^{12} + x^{11} + x^{10} + x^5 + x^4 + x^2) + (x^2 + 1) \cdot (x^6 + x + 1)$.

Oefening 195

1) $G(x) \equiv x^8 + x^7 + x^3 + x^2 + 1 \mod 2$, is irreducibel (zie pagina 308)
   wiskundig: de 8-bit checksums vormen een galoisveld $(\mathbb{F}_{2^8}, +, \cdot)$
   pragmatisch: detectie van 1-bitfouten, bitfoutgroepen van maximum lengte 8

2) $G(x) \equiv (1 + x)(1 + x + x^2 + x^3 + x^5 + x^6 + x^7) \mod 2$
   wiskundig: de 8-bit checksums vormen een binaire ring $(\mathbb{Z}_2[x] \mod G(x), +, \cdot)$
   pragmatisch: detectie van 1-bitfouten, *elk* oneven aantal bitfouten,
   bitfoutgroepen van maximum lengte 8

3) $G(x) \equiv (1 + x)(1 + x + x^2)(1 + x^2 + x^3 + x^4 + x^5) \mod 2$
   wiskundig: de 8-bit checksums vormen een binaire ring $(\mathbb{Z}_2[x] \mod G(x), +, \cdot)$
   pragmatisch: detectie van 1-bitfouten, bitfoutgroepen van maximum lengte 8

4) $G(x) \equiv x^8 + x^4 + x^3 + x^2 + 1 \mod 2$, is irreducibel
   wiskundig: de 8-bit checksums vormen een galoisveld $(\mathbb{F}_{2^8}, +, \cdot)$
   pragmatisch: detectie van 1-bitfouten, bitfoutgroepen van maximum lengte 8