Logische Complexiteit

XVI : Cryptografie

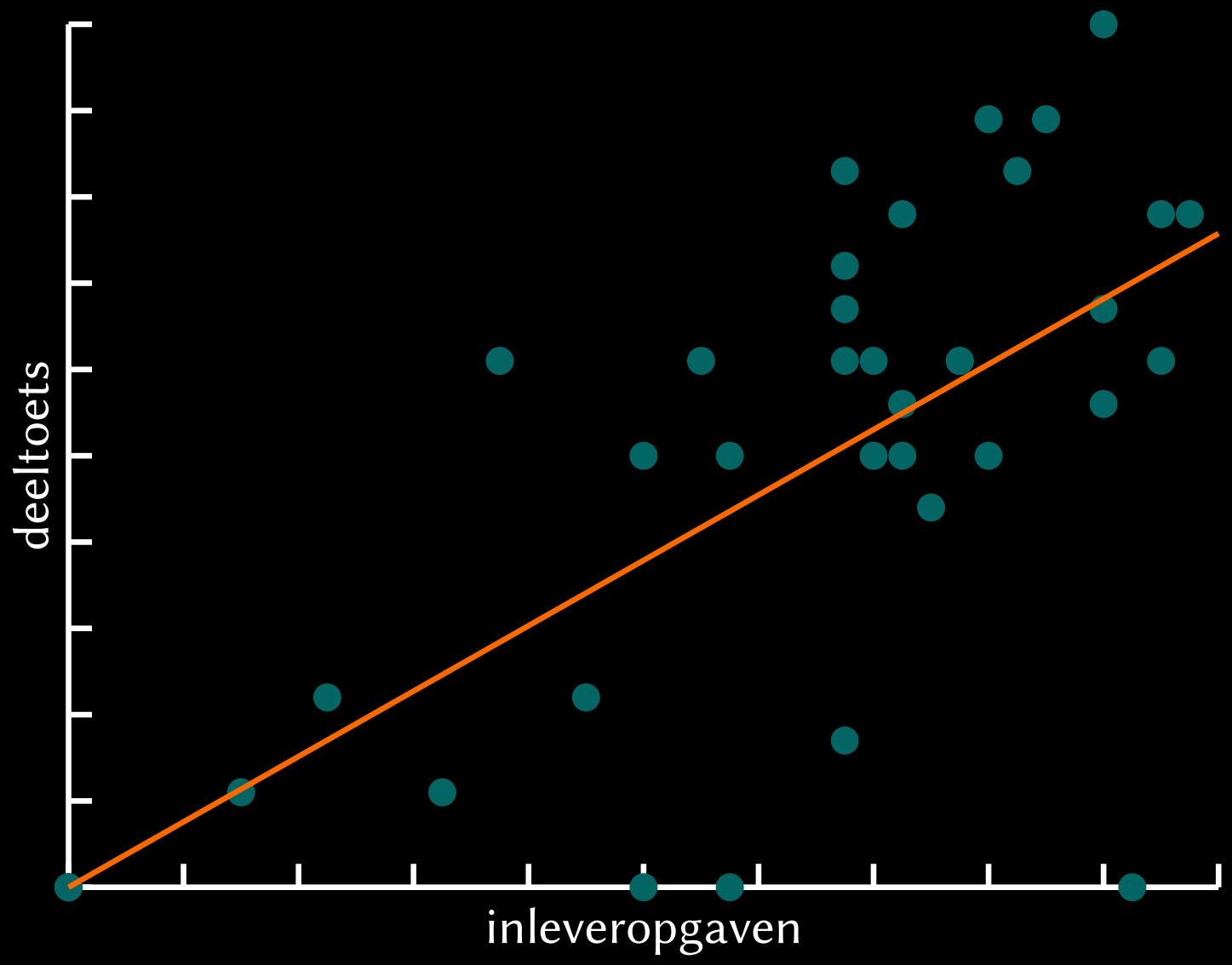
Jeroen Goudsmit
Universiteit Utrecht
dinsdag 3 april 2012

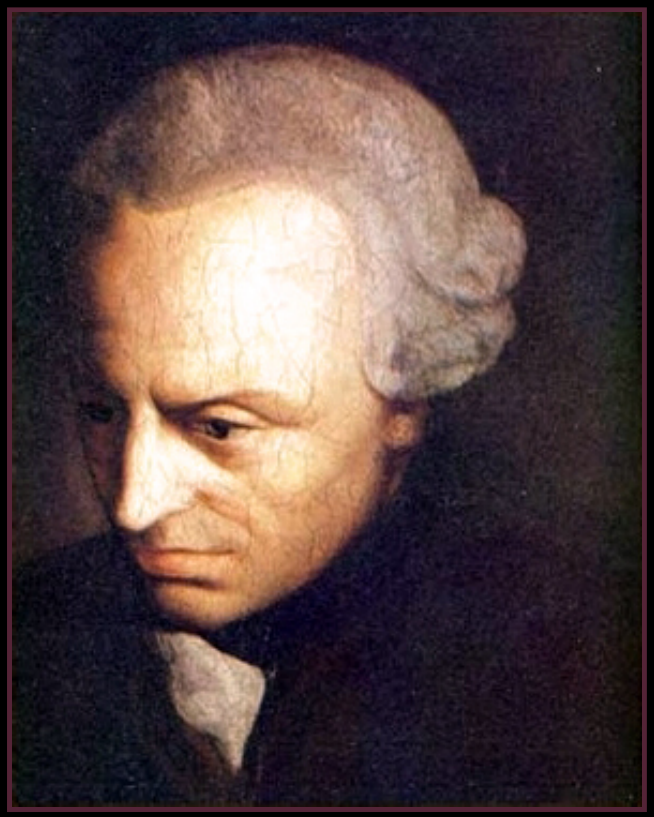
Extra Werkcollege

Drift 21 Sweelinckzaal 9:00 tot 12:45

donderdag aanstaande

Inleveropgaven versus Deeltoets

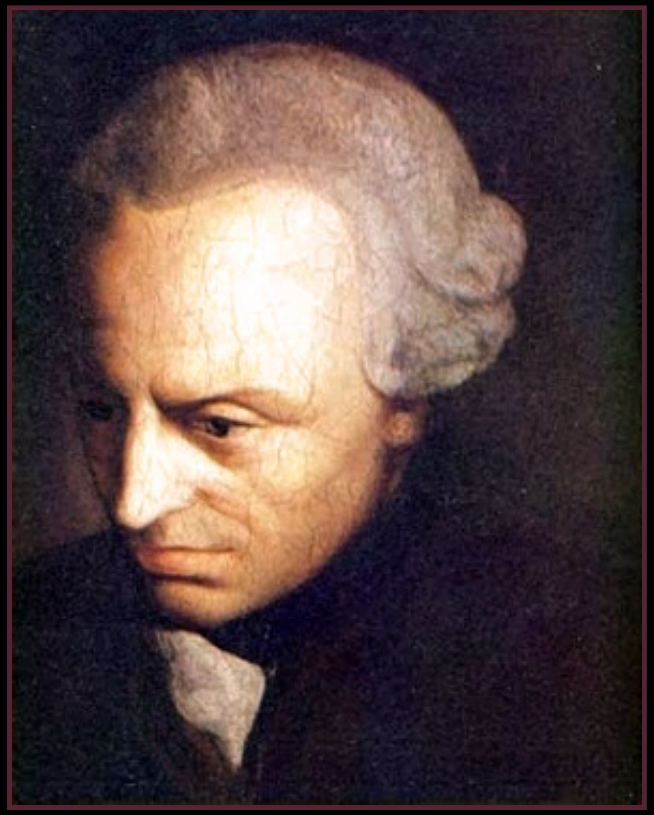




Kant

$\neq$

Pad

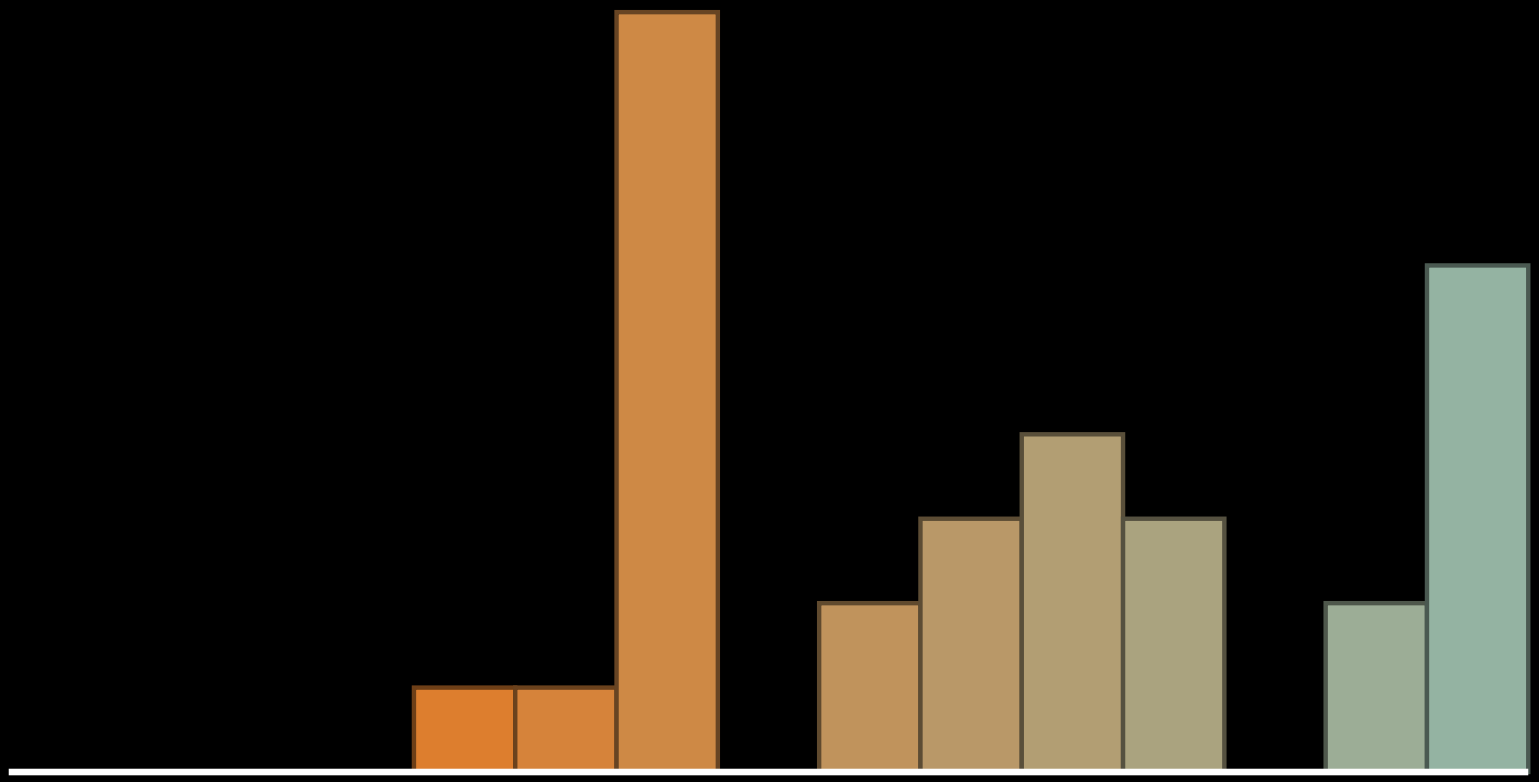


Immanuel Kant
wikimedia

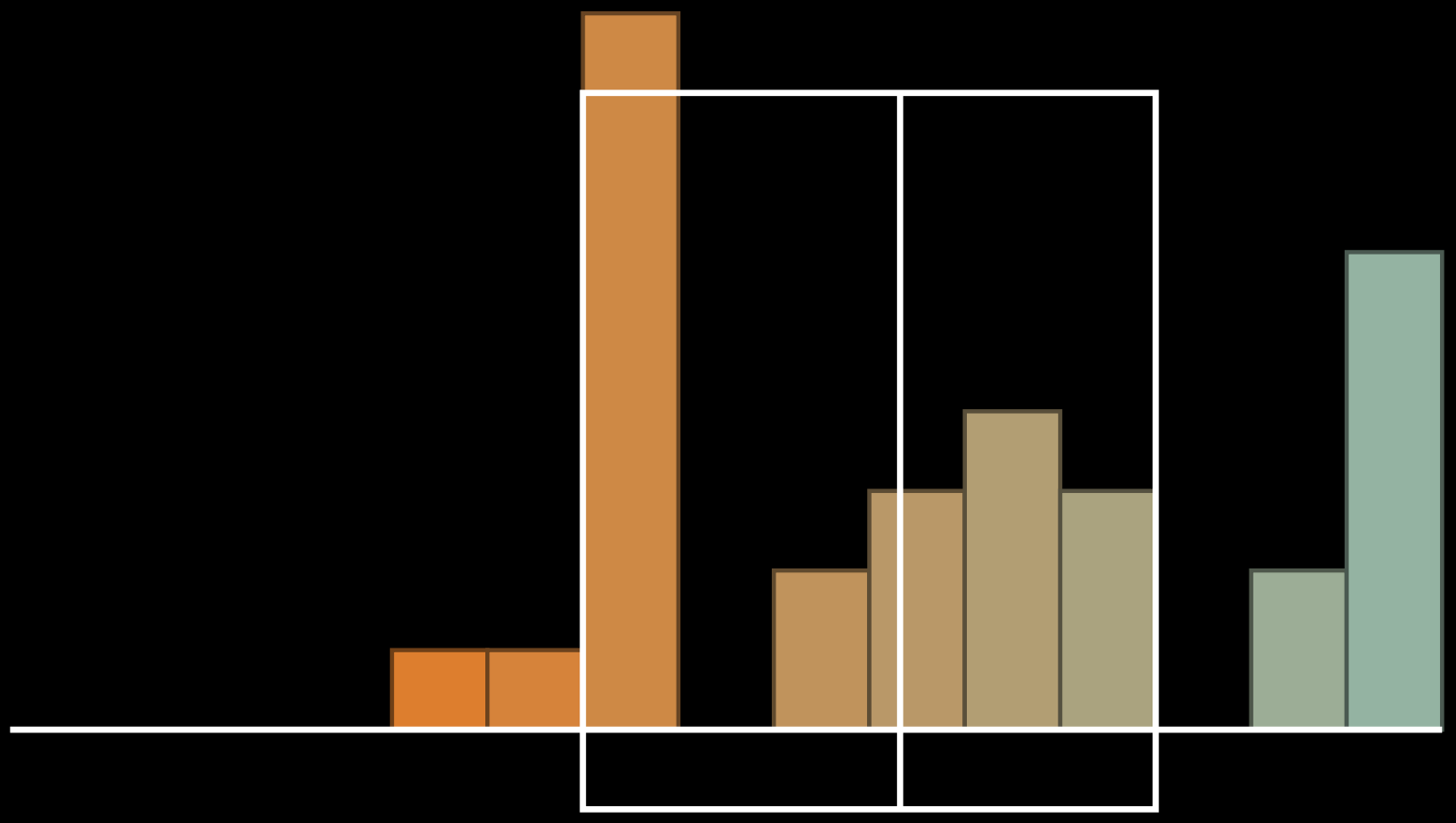
$\neq$

Pad
wikimedia

Inleveropgave 7

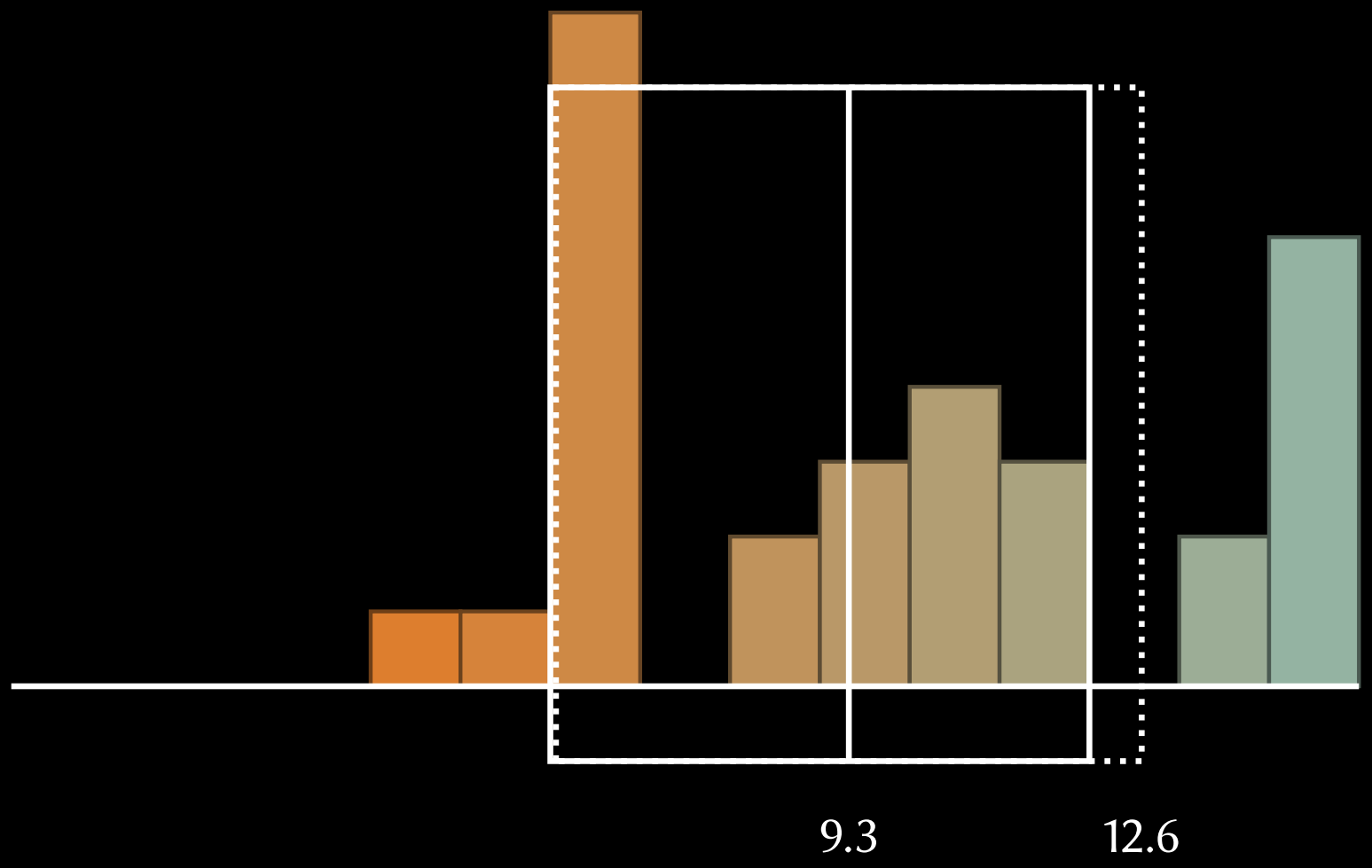


Inleveropgave 7



9.3

Inleveropgave 7



Inleveropgave 8.1.(a)

$$\text{LangPad} := \left\{ \langle G, k \rangle \;\middle|\; \begin{array}{l} G \text{ gerichte graaf} \\ \text{met simpel pad van} \\ \text{lengte minstens } k \end{array} \right\}$$

Inleveropgave 8.1.(a)

Lemma

LangPad *zit in* NP.

Inleveropgave 8.1.(a)

Lemma

LangPad *zit in* NP.

Bewijs.

We maken een controleur M van LangPad.

Inleveropgave 8.1.(a)

Lemma

LangPad *zit in* NP.

Bewijs.

We maken een controleur M van LangPad.

$M :=$ "Op invoer $\langle \langle G, k \rangle, c \rangle$

1. Test of $c = \langle c_1, \ldots, c_l \rangle$ een rijtje van l knopen uit G is.
2. Test of opeenvolgende knopen in c verbonden zijn.
3. Test of $l \geq k$.
4. Test of er dubbele knopen in G zitten.
5. Als (1), (2) en (3) slagen en (4) faalt, accepteer. Zo niet, verwerp."

Inleveropgave 8.1.(a)

Lemma

LangPad *zit in* NP.

Bewijs.

We maken een controleur M van LangPad.

$M :=$ "Op invoer $\langle \langle G, k \rangle, c \rangle$

1. Test of $c = \langle c_1, \ldots, c_l \rangle$ een rijtje van l knopen uit G is.
2. Test of opeenvolgende knopen in c verbonden zijn.
3. Test of $l \geq k$.
4. Test of er dubbele knopen in G zitten.
5. Als (1), (2) en (3) slagen en (4) faalt, accepteer. Zo niet, verwerp."

$$\langle G, k \rangle \in \text{LangPad} \quad \text{precies als} \quad \exists c.\ \langle \langle G, k \rangle, c \rangle \in \mathcal{L}(M) \qquad \blacksquare$$

Inleveropgave 8.1.(a)

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Inleveropgave 8.1.(a)

Lemma

$\mathrm{HamPath} \leq_{\mathrm{p}} \mathrm{LangPad}$

Bewijs.

Per $\langle \mathrm{G}, s, t \rangle$ maken we $\langle G, k \rangle$.

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\mathrm{HamPath} \leq_{\mathrm{p}} \mathrm{LangPad}$

Bewijs.

Per $\langle \mathrm{G}, s, t \rangle$ maken we $\langle G, k \rangle$.

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \end{aligned}$$

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

HamPath $\leq_{\mathrm{p}}$ LangPad

Bewijs.

Per $\langle \mathrm{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Stel $\langle G, s, t \rangle \in$ HamPath.

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t.

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

HamPath $\leq_{\mathrm{p}}$ LangPad

Bewijs.

Per $\langle \mathrm{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Stel $\langle G, s, t \rangle \in$ HamPath. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$.

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad van s naar t.

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad van s naar t. Dus $\langle G, k \rangle \in \text{LangPad}$

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad van s naar t. Dus $\langle G, k \rangle \in \text{LangPad}$

Stel $\langle G, k \rangle \in \text{LangPad}$.

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad van s naar t. Dus $\langle G, k \rangle \in \text{LangPad}$

Stel $\langle G, k \rangle \in \text{LangPad}$. Nu moet er een simpel pad zijn tussen s en t.

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad van s naar t. Dus $\langle G, k \rangle \in \text{LangPad}$

Stel $\langle G, k \rangle \in \text{LangPad}$. Nu moet er een simpel pad zijn tussen s en t. Dit geeft een Hamiltoniaans pad in G tussen s en t.

Inleveropgave 8.1.(a)

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{LangPad}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{s, t\} \\ E &:= E \cup \{\langle s, s \rangle, \langle t, t \rangle\} \\ k &:= |V| + 2 = |V| \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad van s naar t. Dus $\langle G, k \rangle \in \text{LangPad}$

Stel $\langle G, k \rangle \in \text{LangPad}$. Nu moet er een simpel pad zijn tussen s en t. Dit geeft een Hamiltoniaans pad in G tussen s en t. Dus $\langle G, s, t \rangle \in \text{HamPath}$. ■

Inleveropgave 8.2

$$\mathrm{HamLus} := \left\{ \langle G \rangle \;\middle|\; \begin{array}{l} G \text{ gerichte graaf} \\ \text{met lus die elke} \\ \text{knoop precies één} \\ \text{keer raakt} \end{array} \right\}$$

Inleveropgave 8.2

Lemma

HamLus *zit in* NP.

Inleveropgave 8.2

Lemma

HamLus *zit in* NP.

Bewijs.

We maken een controleur M van HamLus.

Inleveropgave 8.2

Lemma

HamLus *zit in* NP.

Bewijs.

We maken een controleur M van HamLus.

$M :=$ "Op invoer $\langle \langle G \rangle, c \rangle$

1. Test of $c = \langle c_1, \ldots, c_n \rangle$ een rijtje van $n = |G|$ knopen uit G is.
2. Test of opeenvolgende knopen in c verbonden zijn.
3. Test of c_n en c_1 verbonden zijn.
4. Test of er dubbele knopen in G zitten.
5. Als (1), (2) en (3) slagen en (4) faalt, accepteer. Zo niet, verwerp."

Inleveropgave 8.2

Lemma

HamLus *zit in* NP.

Bewijs.

We maken een controleur M van HamLus.

$M :=$ "Op invoer $\langle \langle G \rangle, c \rangle$

1. Test of $c = \langle c_1, \ldots, c_n \rangle$ een rijtje van $n = |G|$ knopen uit G is.
2. Test of opeenvolgende knopen in c verbonden zijn.
3. Test of c_n en c_1 verbonden zijn.
4. Test of er dubbele knopen in G zitten.
5. Als (1), (2) en (3) slagen en (4) faalt, accepteer. Zo niet, verwerp."

$$\langle G, k \rangle \in \text{HamLus} \quad \text{precies als} \quad \exists c.\ \langle \langle G, k \rangle, c \rangle \in \mathcal{L}(M) \qquad \blacksquare$$

Inleveropgave 8.2

Lemma

$\text{HamPath} \leq_p \text{HamLus}$

Inleveropgave 8.2

Lemma

$\text{HamPath} \leq_{\text{p}} \text{HamLus}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$.

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

HamPath $\leq_{\mathrm{p}}$ HamLus

Bewijs.

Per $\langle \mathrm{G}, s, t \rangle$ maken we $\langle G, k \rangle$.

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\mathrm{HamPath} \leq_{\mathrm{p}} \mathrm{HamLus}$

Bewijs.

Per $\langle \mathrm{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{HamLus}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$.

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{HamLus}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t.

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\mathrm{HamPath} \leq_{\mathrm{p}} \mathrm{HamLus}$

Bewijs.

Per $\langle \mathrm{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

Stel $\langle G, s, t \rangle \in \mathrm{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$.

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{HamLus}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad wat begint in $*$.

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{HamLus}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad wat begint in $*$. Dus $\langle G \rangle \in \text{HamLus}$

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{HamLus}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad wat begint in $*$. Dus $\langle G \rangle \in \text{HamLus}$

Stel $\langle G \rangle \in \text{HamLus}$.

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{HamLus}$

Bewijs.

Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad wat begint in $*$. Dus $\langle G \rangle \in \text{HamLus}$

Stel $\langle G \rangle \in \text{HamLus}$. Nu is er een lus .

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

HamPath $\leq_{\mathrm{p}}$ HamLus

Bewijs.

Per $\langle \mathrm{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

Stel $\langle G, s, t \rangle \in$ HamPath. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad wat begint in $*$. Dus $\langle G \rangle \in$ HamLus

Stel $\langle G \rangle \in$ HamLus. Nu is er een lus . Dit geeft een Hamiltoniaans pad in G tussen s en t.

Inleveropgave 8.2

$\langle V, E \rangle$

$\langle V, E \rangle$

Lemma

$\text{HamPath} \leq_{\text{p}} \text{HamLus}$

Bewijs.

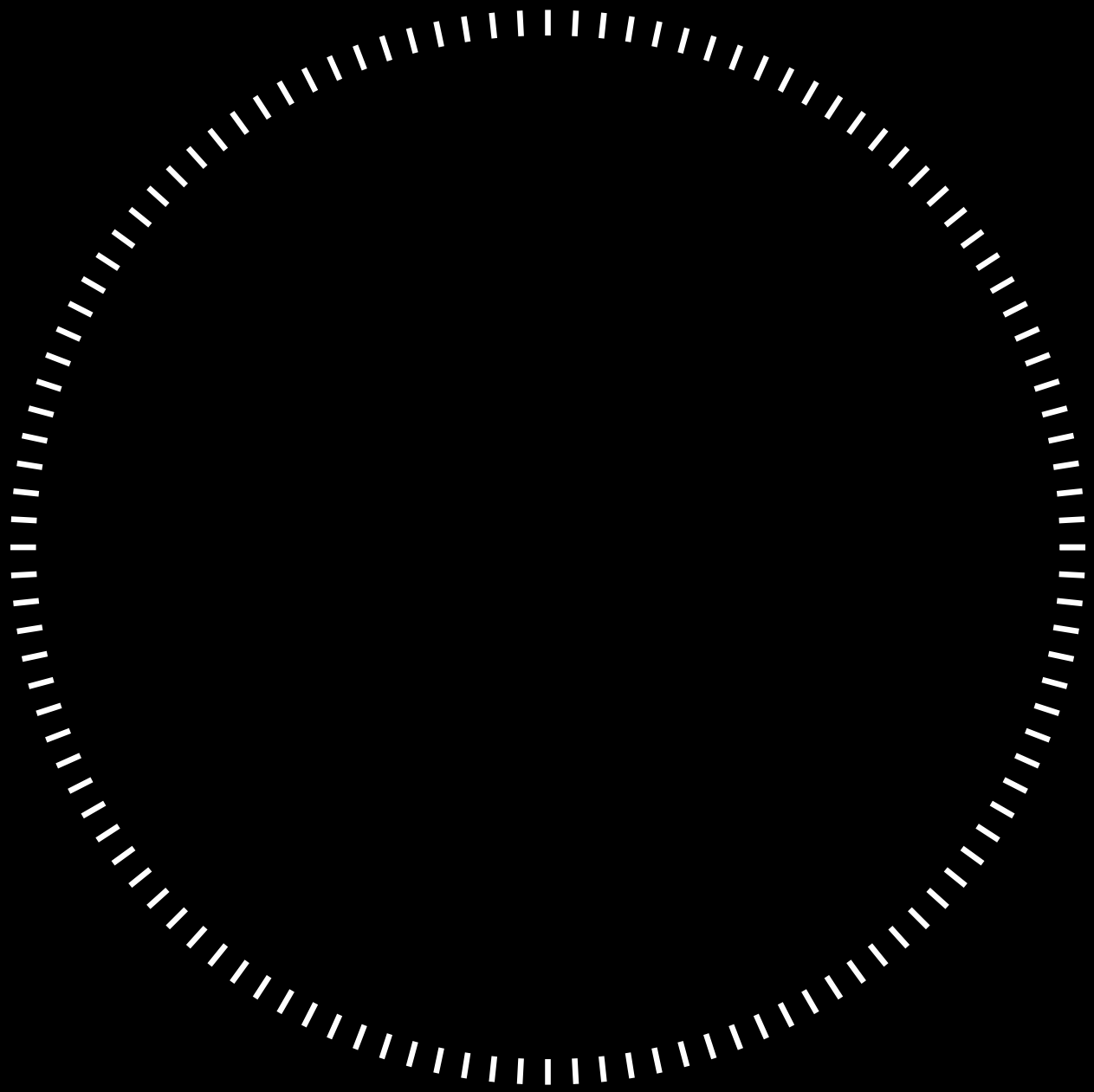
Per $\langle \text{G}, s, t \rangle$ maken we $\langle G, k \rangle$. Stel in:

$$\begin{aligned} V &:= V \cup \{*\} \\ E &:= E \cup \{\langle *, s \rangle, \langle t, * \rangle\} \end{aligned}$$

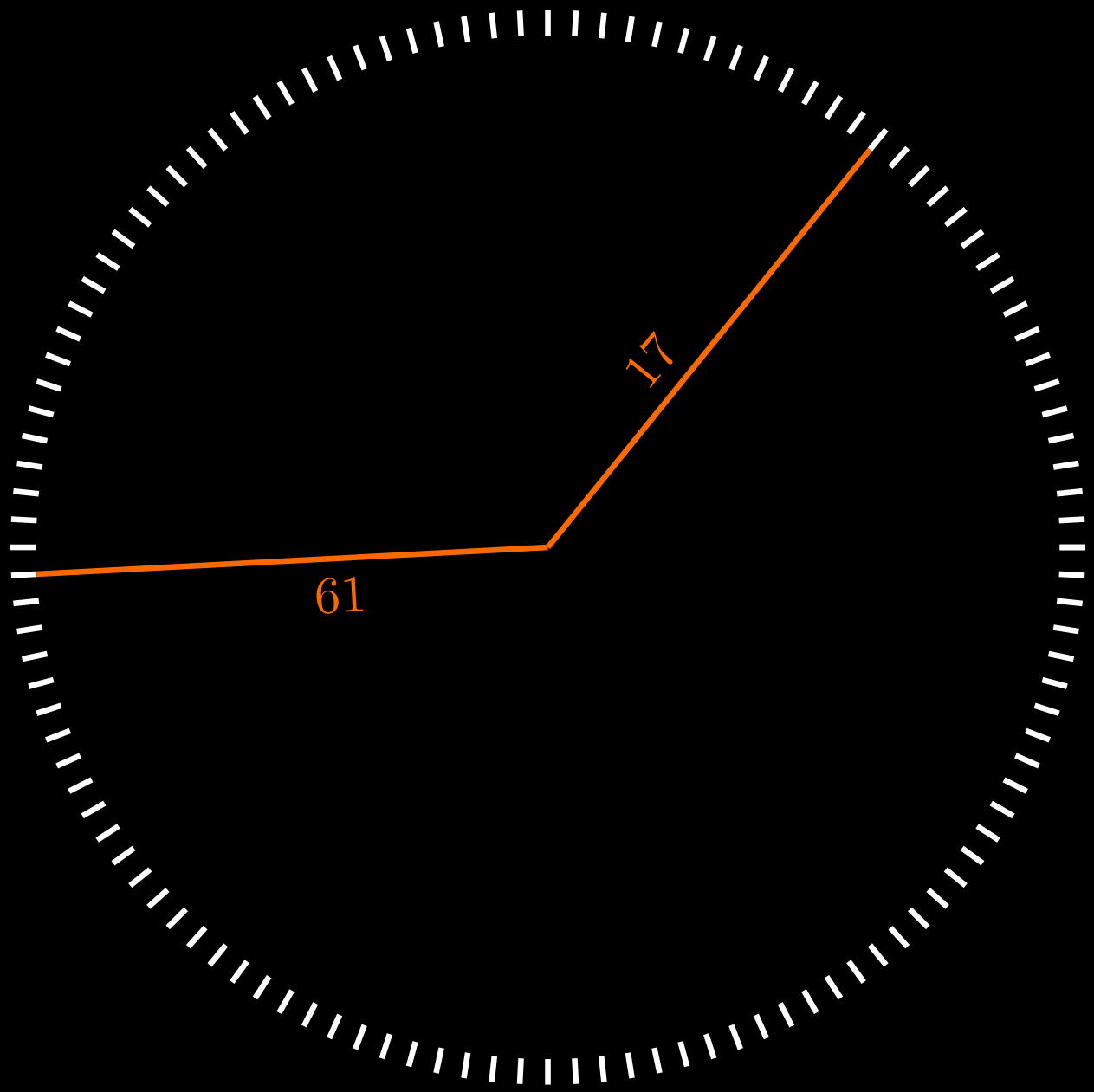
Stel $\langle G, s, t \rangle \in \text{HamPath}$. Dan is er een Hamiltoniaans pad tussen s en t. Dit pad heeft lengte $|V|$. Breidt het uit tot een pad wat begint in $*$. Dus $\langle G \rangle \in \text{HamLus}$

Stel $\langle G \rangle \in \text{HamLus}$. Nu is er een lus . Dit geeft een Hamiltoniaans pad in G tussen s en t. Dus $\langle G, s, t \rangle \in \text{HamPath}$. ■

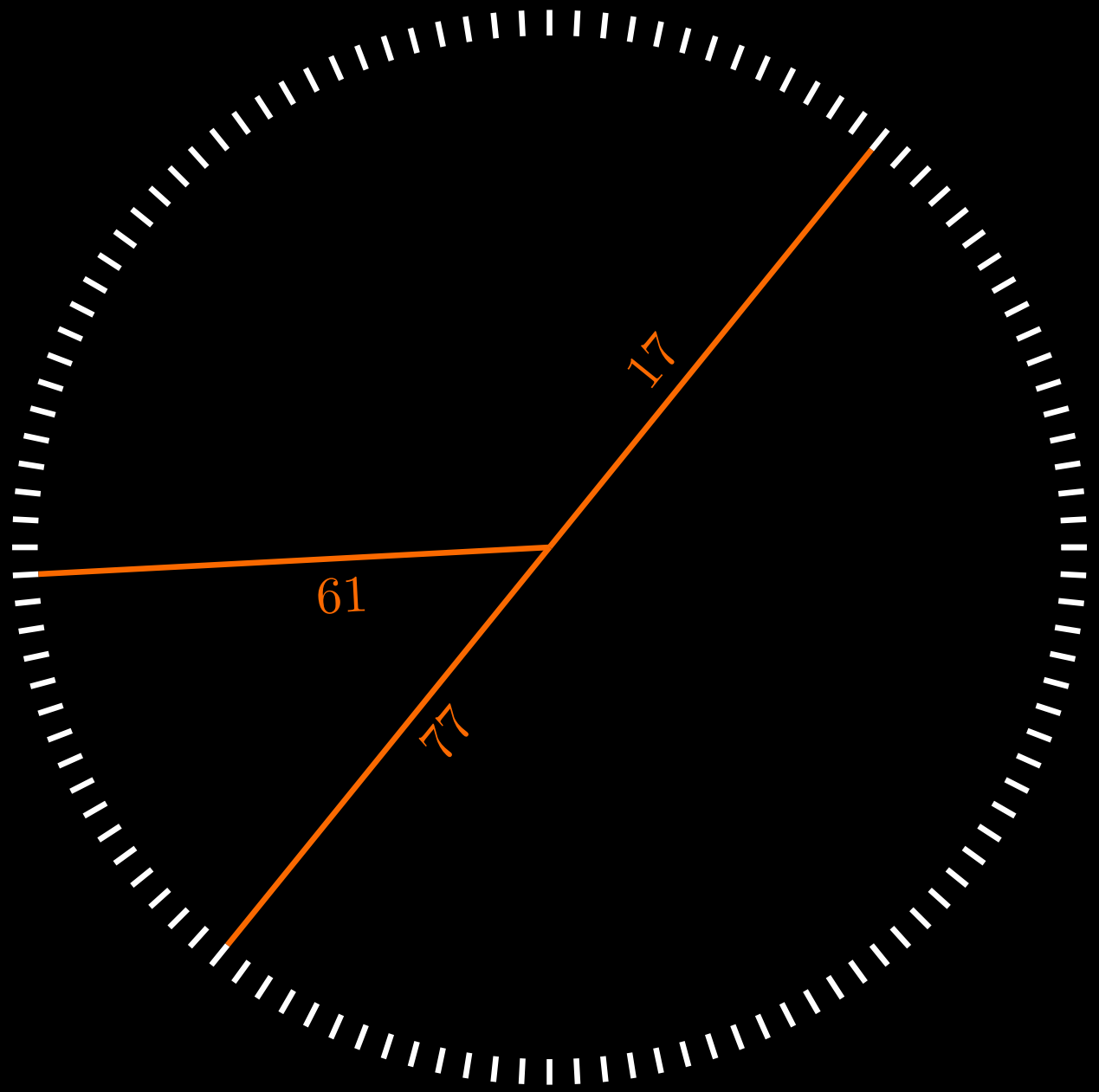
Modulorekenen



Modulorekenen



Modulorekenen



Multiplicatief Inverse

Multiplicatief Inverse

$$
\begin{aligned}
120 &= 1 \times 83 + 1 \times 37 \\
83 &= 2 \times 37 + 1 \times 9 \\
37 &= 4 \times 9 + 1 \times 1
\end{aligned}
$$

Multiplicatief Inverse

$$\begin{aligned} 120 &= 1 \times 83 + 1 \times 37 \\ 83 &= 2 \times 37 + 1 \times 9 \\ 37 &= 4 \times 9 + 1 \times 1 \end{aligned}$$

$$1 = 1 \times 37 + -4 \times 9$$

Multiplicatief Inverse

$$\begin{aligned} 120 &= 1 \times 83 + 1 \times 37 \\ 83 &= 2 \times 37 + 1 \times 9 \\ 37 &= 4 \times 9 + 1 \times 1 \end{aligned}$$

$$\begin{aligned} 1 &= 1 \times 37 + -4 \times 9 \\ &= 1 \times 37 + -4 \times (83 - 2 \times 37) \end{aligned}$$

Multiplicatief Inverse

$$\begin{aligned} 120 &= 1 \times 83 + 1 \times 37 \\ 83 &= 2 \times 37 + 1 \times 9 \\ 37 &= 4 \times 9 + 1 \times 1 \end{aligned}$$

$$\begin{aligned} 1 &= 1 \times 37 + -4 \times 9 \\ &= 1 \times 37 + -4 \times (83 - 2 \times 37) \\ &= 9 \times 37 + -4 \times 83 \end{aligned}$$

Multiplicatief Inverse

$$
\begin{aligned}
120 &= 1 \times 83 + 1 \times 37 \\
83 &= 2 \times 37 + 1 \times 9 \\
37 &= 4 \times 9 + 1 \times 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \times 37 + -4 \times 9 \\
&= 1 \times 37 + -4 \times (83 - 2 \times 37) \\
&= 9 \times 37 + -4 \times 83 \\
&= 9 \times (120 - 1 \times 83) + -4 \times 83
\end{aligned}
$$

Multiplicatief Inverse

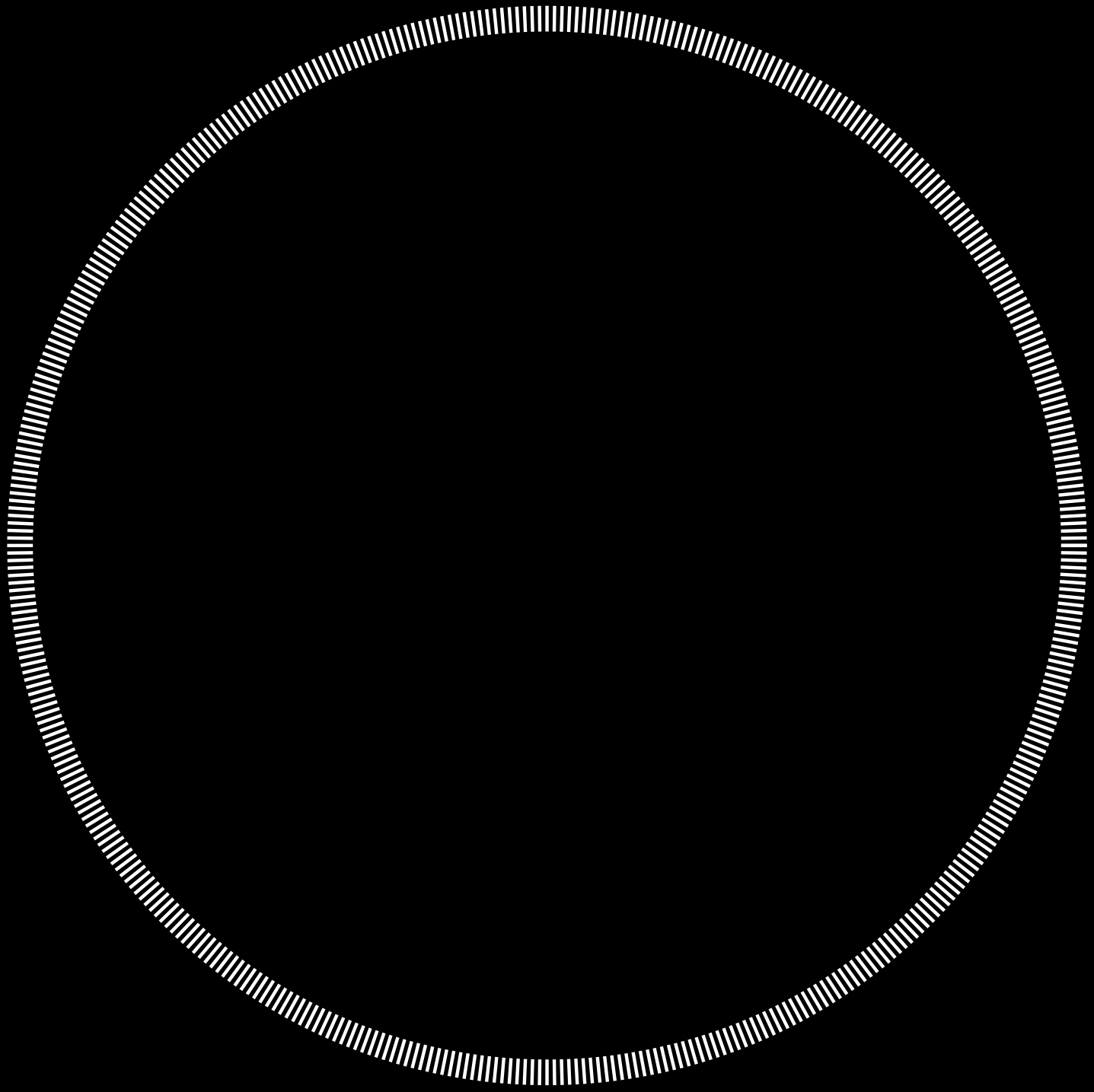
$$
\begin{aligned}
120 &= 1 \times 83 + 1 \times 37 \\
83 &= 2 \times 37 + 1 \times 9 \\
37 &= 4 \times 9 + 1 \times 1
\end{aligned}
$$

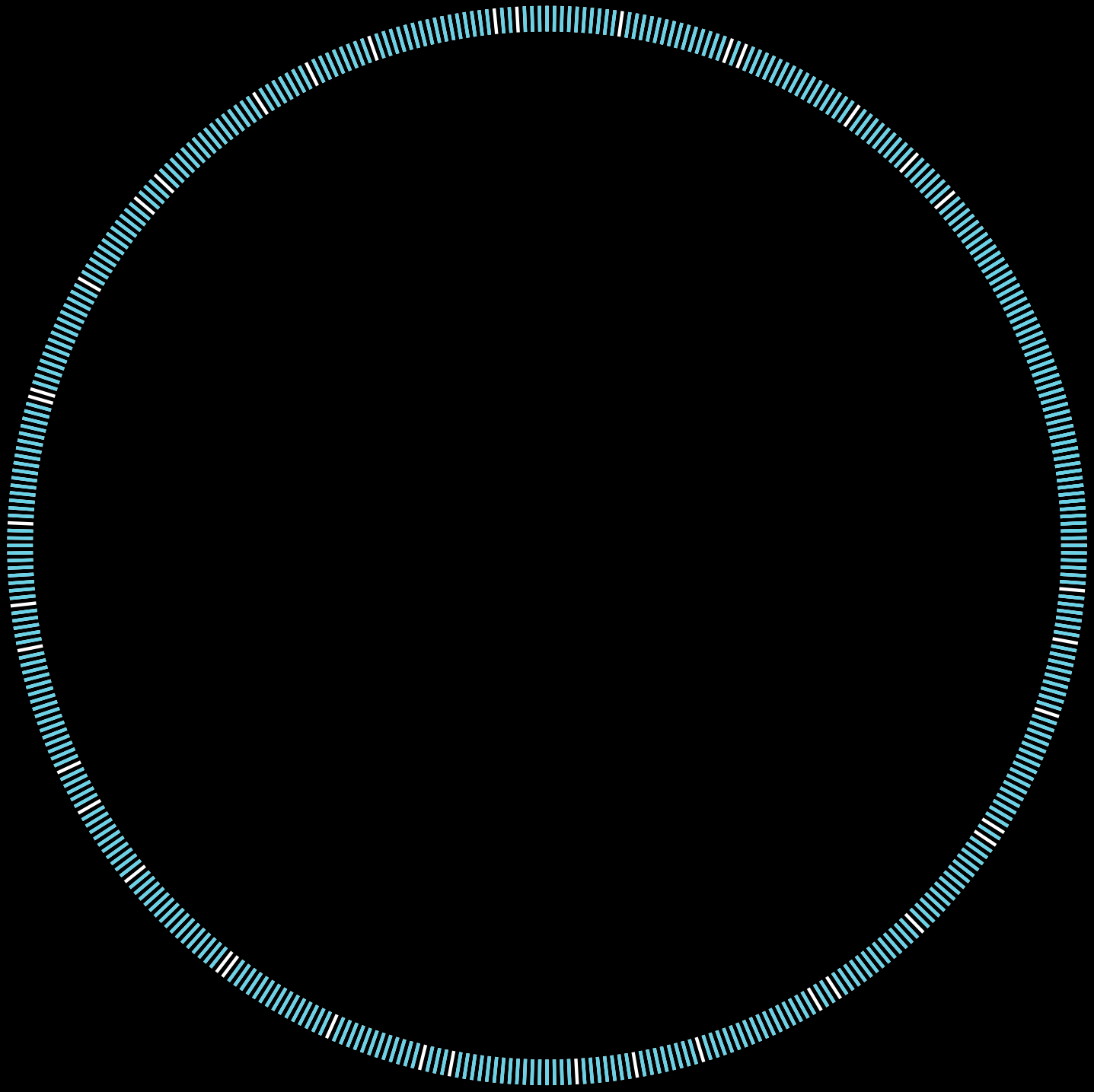
$$
\begin{aligned}
1 &= 1 \times 37 + -4 \times 9 \\
&= 1 \times 37 + -4 \times (83 - 2 \times 37) \\
&= 9 \times 37 + -4 \times 83 \\
&= 9 \times (120 - 1 \times 83) + -4 \times 83 \\
&= 9 \times 120 + -13 \times 83
\end{aligned}
$$

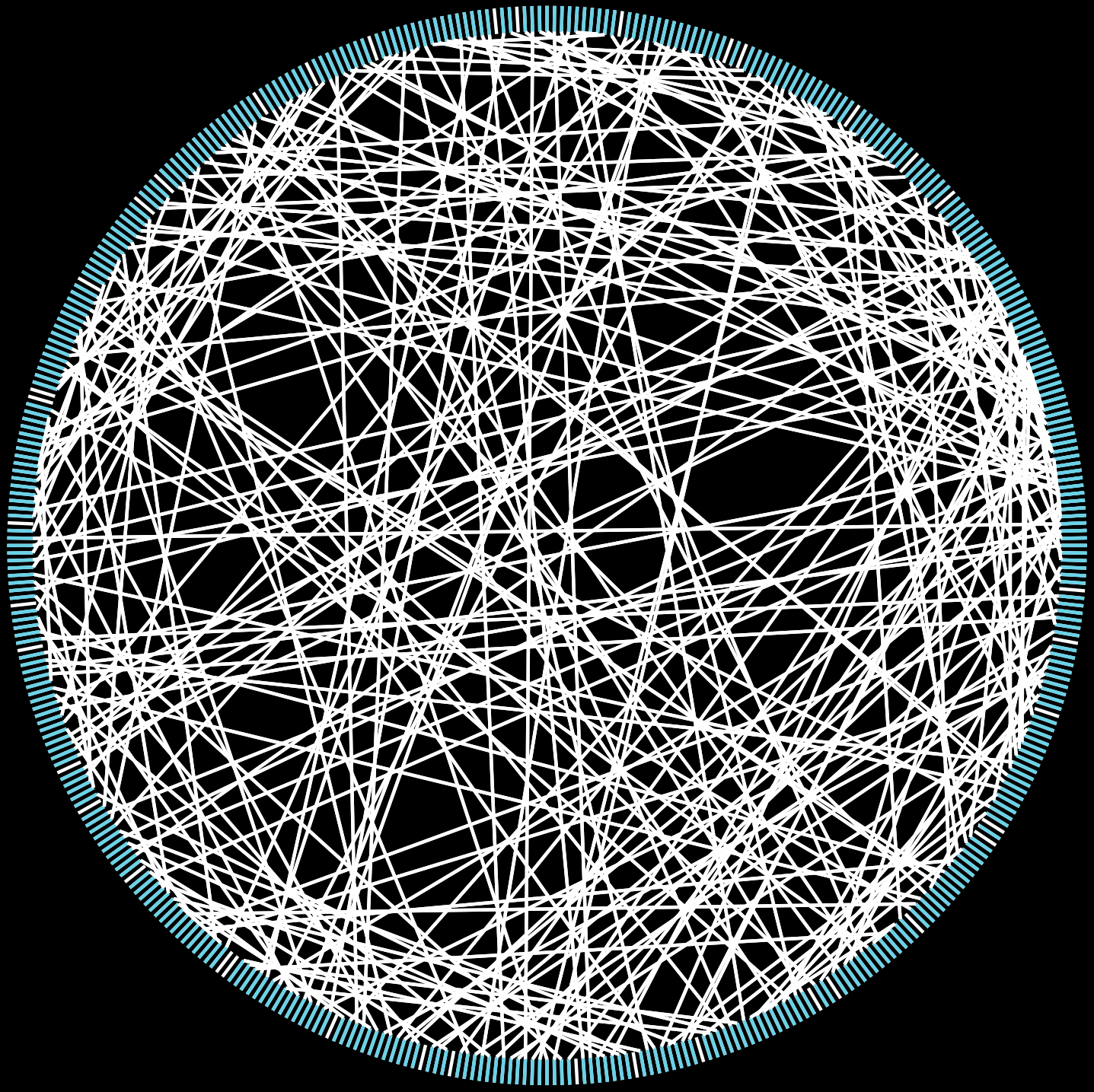
Multiplicatief Inverse

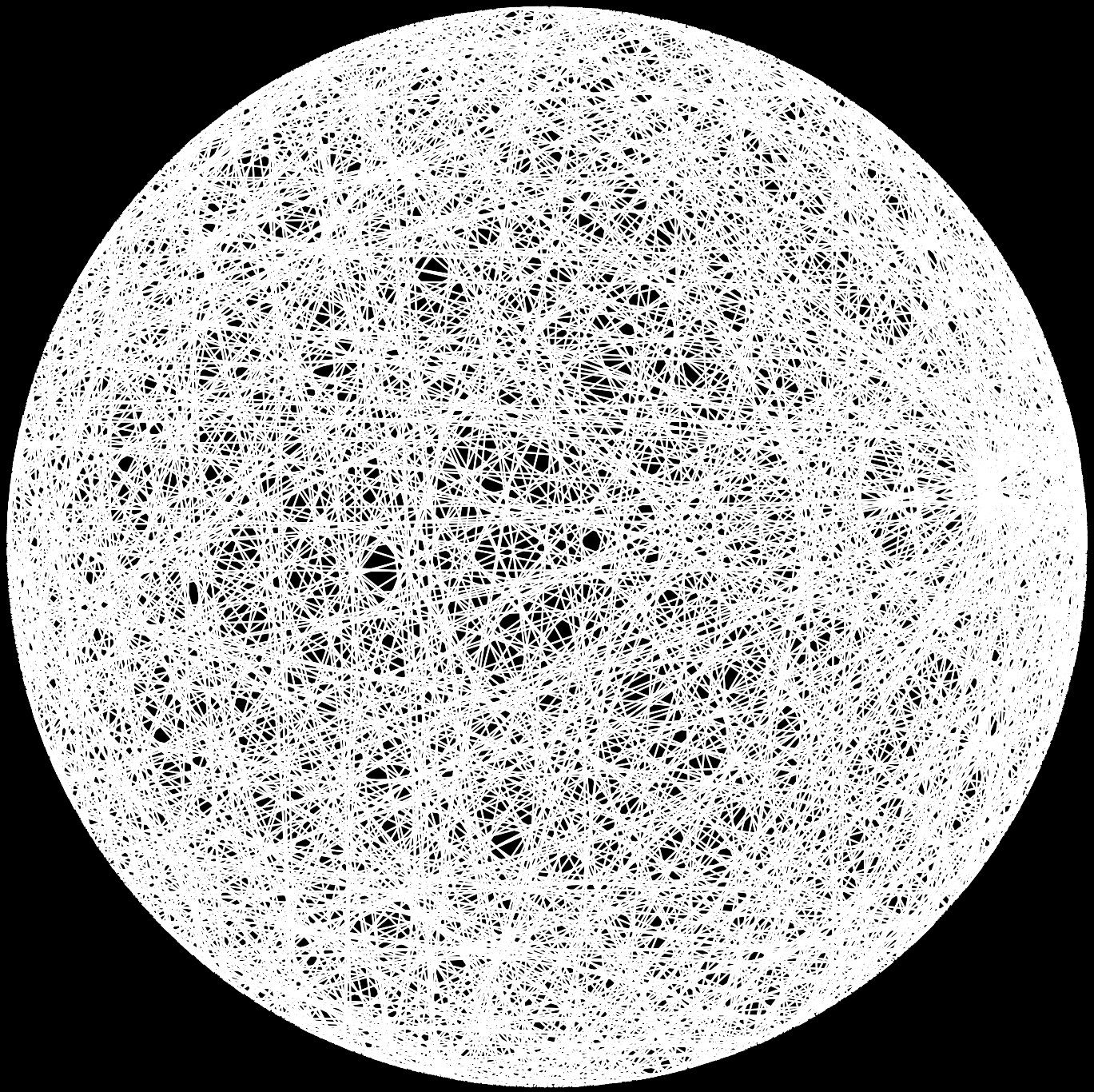
$$
\begin{aligned}
120 &= 1 \times 83 + 1 \times 37 \\
83 &= 2 \times 37 + 1 \times 9 \\
37 &= 4 \times 9 + 1 \times 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 1 \times 37 + -4 \times 9 \\
&= 1 \times 37 + -4 \times (83 - 2 \times 37) \\
&= 9 \times 37 + -4 \times 83 \\
&= 9 \times (120 - 1 \times 83) + -4 \times 83 \\
&= 9 \times 120 + -13 \times 83 \\
&= -74 \times 120 + 107 \times 83
\end{aligned}
$$









Euler's ϕ

$$\phi(n) := \#\left\{\begin{array}{c}\text{getallen tussen } 1 \text{ en } n \\ \text{relatief priem met } n\end{array}\right\}$$

Priem

Lemma
Als p priem, dan $\phi(p) = p - 1$.

Priem

Lemma
Als p priem, dan $\phi(p) = p - 1$.

Bewijs.
De enige delers van p zijn 1 en p.

Priem

Lemma
Als p priem, dan $\phi(p) = p - 1$.

Bewijs.

De enige delers van p zijn 1 en p. Dus alle getallen tussen 1 en p hebben grootste gemene deler 1 met p. $\blacksquare$

Multiplicatief

Lemma
Als n en m relatief priem, dan $\phi(n \times m) = \phi(n) \times \phi(m)$.

Multiplicatief

Lemma
Als n en m relatief priem, dan $\phi(n \times m) = \phi(n) \times \phi(m)$.

Euler's Stelling

$$x^{\phi(n)} = 1 \mod n$$

Priemtest

$$\left\{ \langle m \rangle \;\middle|\; m \text{ is priem} \right\}$$

Ontbinden in Priemfactoren
is lastig

Ron Rivest

Adi Shamir

Leonard Adleman

Ron Rivest

Adi Shamir

Leonard Adleman

RSA

Bob

1. Kies priemen p en q.
2. Bereken $n := pq - p - q + 1$.
3. Gok een getal e tussen 0 en pq met $\gcd(e, n) = 1$.
4. Bereken een getal d zodat $ed = 1 \mod n$.
5. Verzend $\langle pq, e \rangle$ naar **Alice**.

RSA

$\phi(pq)$

Bob

1. Kies priemen p en q.
2. Bereken $n := pq - p - q + 1$.
3. Gok een getal e tussen 0 en pq met $\gcd(e, n) = 1$.
4. Bereken een getal d zodat $ed = 1 \mod n$.
5. Verzend $\langle pq, e \rangle$ naar **Alice**.

Alice

1. Codeer boodschap als getal x tussen 0 en pq.
2. Verzend x^e naar **Bob**.

RSA

$\phi(pq)$

Bob

1. Kies priemen p en q.
2. Bereken $n := pq - p - q + 1$.
3. Gok een getal e tussen 0 en pq met $\gcd(e, n) = 1$.
4. Bereken een getal d zodat $ed = 1 \mod n$.
5. Verzend $\langle pq, e \rangle$ naar **Alice**.

Alice

1. Codeer boodschap als getal x tussen 0 en pq.
2. Verzend x^e naar **Bob**.

$$(x^e)^d$$

RSA

$\phi(pq)$

Bob

1. Kies priemen p en q.
2. Bereken $n := pq - p - q + 1$.
3. Gok een getal e tussen 0 en pq met $\gcd(e, n) = 1$.
4. Bereken een getal d zodat $ed = 1 \mod n$.
5. Verzend $\langle pq, e \rangle$ naar **Alice**.

Alice

1. Codeer boodschap als getal x tussen 0 en pq.
2. Verzend x^e naar **Bob**.

$$(x^e)^d = x^{ed}$$

RSA

$\phi(pq)$

$d \times e + k \times n = 1$

Bob

1. Kies priemen p en q.
2. Bereken $n := pq - p - q + 1$.
3. Gok een getal e tussen 0 en pq met $\gcd(e, n) = 1$.
4. Bereken een getal d zodat $ed = 1 \mod n$.
5. Verzend $\langle pq, e \rangle$ naar **Alice**.

Alice

1. Codeer boodschap als getal x tussen 0 en pq.
2. Verzend x^e naar **Bob**.

$$(x^e)^d = x^{ed} = x^{1-k\phi(pq)} = x$$

Extra Werkcollege

Drift 21 Sweelinckzaal 9:00 tot 12:45

donderdag aanstaande