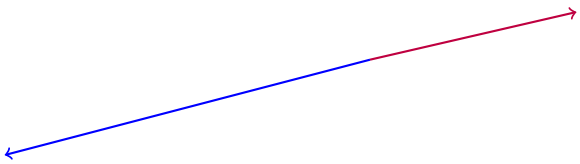
Gitter (latticer) – historie og anvendelser

Kristian Gjøsteen

Perleforum, 15. november 2019

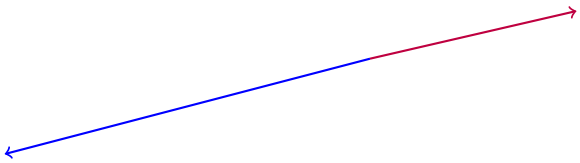
Gauss og to vektorer



Gauss ville finne den korteste lineærkombinasjonen av to vektorer i planet.

Carl Friedrich Gauss (1777-–1855)

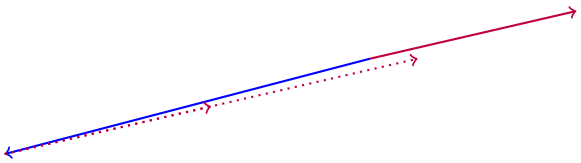
Gauss og to vektorer



Gauss ville finne den korteste heltalls-lineærkombinasjonen av to vektorer i planet.

Carl Friedrich Gauss
(1777-–1855)

Gauss og to vektorer



Gauss ville finne den korteste heltalls-lineærkombinasjonen av to vektorer i planet.

Carl Friedrich Gauss
(1777–1855)

Gauss og to vektorer

Carl Friedrich Gauss
(1777-–1855)

Gauss ville finne den korteste heltalls-lineærkombinasjonen av to vektorer i planet.

Gauss og to vektorer

Gauss ville finne den korteste heltalls-lineærkombinasjonen av to vektorer i planet.

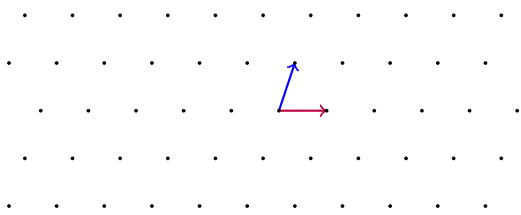
Carl Friedrich Gauss
(1777-–1855)

Gauss og to vektorer

Carl Friedrich Gauss
(1777-–1855)

Gauss ville finne den korteste heltalls-lineærkombinasjonen av to vektorer i planet.

Gauss og to vektorer



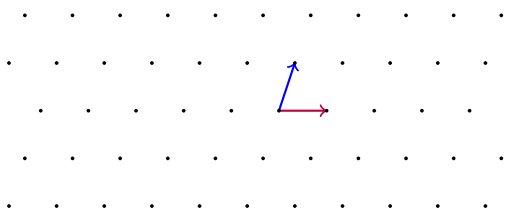
Carl Friedrich Gauss
(1777-–1855)

Gauss ville finne den korteste heltalls-lineærkombinasjonen av to vektorer i planet.

Hva er den korteste vektoren blant alle heltalls-lineærkombinasjonene?

$$\{a_1\mathbf{b}_1 + a_2\mathbf{b}_2 \quad | \; a_1, a_2 \quad \in \mathbb{Z}\}$$

Gauss og to vektorer



Carl Friedrich Gauss
(1777–1855)

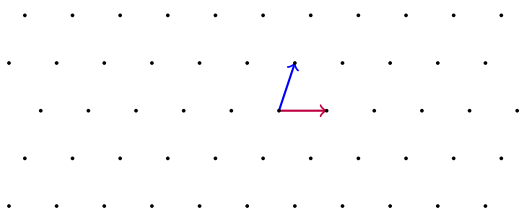
Gauss ville finne den korteste heltalls-lineærkombinasjonen av to vektorer i planet.

Hva er den korteste vektoren blant alle heltalls-lineærkombinasjonene?

Det er et naturlig spørsmål i høyere dimensjon også.

$$\{a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n \mid a_1, a_2, \ldots, a_n \in \mathbb{Z}\}$$

Gauss og to vektorer



Carl Friedrich Gauss
(1777-–1855)

Gauss ville finne den korteste heltalls-lineærkombinasjonen av to vektorer i planet.

Hva er den korteste vektoren blant alle heltalls-lineærkombinasjonene?

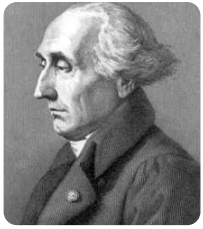
Det er et naturlig spørsmål i høyere dimensjon også.

$$\text{gitter} = \Lambda = \{a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n \mid a_1, a_2, \ldots, a_n \in \mathbb{Z}\} = \text{lattice}$$

Lagrange og fire kvadrater

Hvilke heltall kan skrives som summer av kvadrater:

$$m = a_1^2 + a_2^2 + \cdots + a_n^2$$



Joseph-Louis Lagrange
(1736–1813)

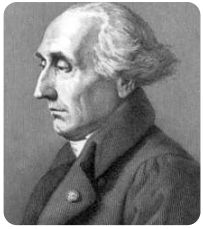
Lagrange og fire kvadrater

Hvilke heltall kan skrives som summer av kvadrater:

$$m = a_1^2 + a_2^2 + \cdots + a_n^2$$

Mer generelt: gitt en symmetrisk positiv definit matrise Q, hvilke heltall kan skrives som

$$m = \mathbf{a}^t Q \mathbf{a} = q(\mathbf{a}), \qquad \mathbf{a} \in \mathbb{Z}^n.$$



Joseph-Louis Lagrange
(1736–1813)

Lagrange og fire kvadrater

Hvilke heltall kan skrives som summer av kvadrater:

$$m = a_1^2 + a_2^2 + \cdots + a_n^2$$

Mer generelt: gitt en symmetrisk positiv definit matrise Q, hvilke heltall kan skrives som

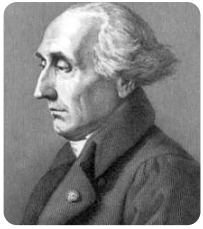
$$m = \mathbf{a}^t Q \mathbf{a} = q(\mathbf{a}), \qquad \mathbf{a} \in \mathbb{Z}^n.$$

Hvis U er et koordinatskifte på $\mathbb{Z}^n$, da er

$$q(U\mathbf{a}) = (U\mathbf{a})^t Q U\mathbf{a} = \mathbf{a}^t (U^t Q U)\mathbf{a} = q'(\mathbf{a}).$$

Altså representerer Q og $U^t Q U$ de samme tallene.

Siden $\det U = \pm 1$ er $|\det Q|$ en invariant.



Joseph-Louis Lagrange
(1736–1813)

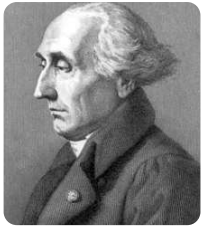
Lagrange og fire kvadrater

Hvilke heltall kan skrives som summer av kvadrater:

$$m = a_1^2 + a_2^2 + \cdots + a_n^2$$

Mer generelt: gitt en symmetrisk positiv definit matrise Q, hvilke heltall kan skrives som

$$m = \mathbf{a}^t Q\mathbf{a} = q(\mathbf{a}), \qquad \mathbf{a} \in \mathbb{Z}^n.$$



Joseph-Louis Lagrange
(1736–1813)

Men hva om vi liker formen $q(\mathbf{a}) = a_1^2 + a_2^2 + \cdots + a_n^2$?

Siden Q er sym. pos. def. finnes reell, ikke-singulær B slik at $Q = B^t B$ og

$$q(\mathbf{a}) = \mathbf{a}^t Q\mathbf{a} = \mathbf{a}^t B^t B\mathbf{a} = (B\mathbf{a})^t B\mathbf{a}.$$

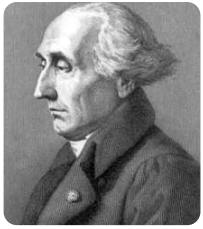
Lagrange og fire kvadrater

Hvilke heltall kan skrives som summer av kvadrater:

$$m = a_1^2 + a_2^2 + \cdots + a_n^2$$

Mer generelt: gitt en symmetrisk positiv definit matrise Q, hvilke heltall kan skrives som

$$m = \mathbf{a}^t Q\mathbf{a} = q(\mathbf{a}), \qquad \mathbf{a} \in \mathbb{Z}^n.$$



Joseph-Louis Lagrange
(1736–1813)

Men hva om vi liker formen $q(\mathbf{a}) = a_1^2 + a_2^2 + \cdots + a_n^2$?

Siden Q er sym. pos. def. finnes reell, ikke-singulær B slik at $Q = B^t B$ og

$$q(\mathbf{a}) = \mathbf{a}^t Q\mathbf{a} = \mathbf{a}^t B^t B\mathbf{a} = (B\mathbf{a})^t B\mathbf{a}.$$

Vi må se på

$$\Lambda = \{B\mathbf{a} \mid \mathbf{a} \in \mathbb{Z}^n\} \subseteq \mathbb{R}^n.$$

Latticer (gitter)

La $\mathbf{b}_1, \ldots, \mathbf{b}_n$ være en basis for $\mathbb{R}^n$. Latticen $\Lambda(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ er

$$\Lambda(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n \mid a_1, \ldots, a_n \in \mathbb{Z}\}.$$

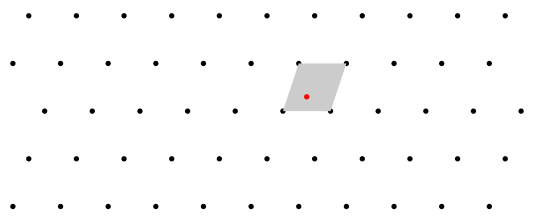
Latticer (gitter)

La $\mathbf{b}_1, \ldots, \mathbf{b}_n$ være en basis for $\mathbb{R}^n$. Latticen $\Lambda(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ er

$$\Lambda(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n \mid a_1, \ldots, a_n \in \mathbb{Z}\}.$$

Fundamentalområdet er $\mathcal{F} = \{\alpha_1\mathbf{b}_1 + \cdots + \alpha_n\mathbf{b}_n \mid 0 \leq \alpha_i < 1\}$. Ethvert punkt i rommet kan skrives som

$$\mathbf{z} = \mathbf{x} + \mathbf{e}, \qquad \mathbf{x} \in \Lambda, \mathbf{e} \in \mathcal{F}.$$



Latticer (gitter)

La $\mathbf{b}_1, \ldots, \mathbf{b}_n$ være en basis for $\mathbb{R}^n$. Latticen $\Lambda(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ er

$$\Lambda(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n \mid a_1, \ldots, a_n \in \mathbb{Z}\}.$$

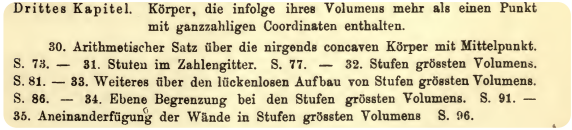
En lattice kan ha mange basiser. Hvis B er matrisen med $\mathbf{b}_i$ som kolonner er volumet av fundamentalområdet

$$\det \Lambda = |\det B|$$

uavhengig av hvilken basis som velges.

Minkowski og et volum

«Geometrie der Zahlen»:



Drittes Kapitel. Körper, die infolge ihres Volumens mehr als einen Punkt mit ganzzahligen Coordinaten enthalten.

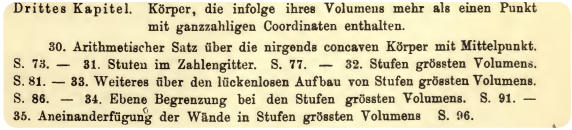
30. Arithmetischer Satz über die nirgends concaven Körper mit Mittelpunkt. S. 73. — 31. Stufen im Zahlengitter. S. 77. — 32. Stufen grössten Volumens. S. 81. — 33. Weiteres über den lückenlosen Aufbau von Stufen grössten Volumens. S. 86. — 34. Ebene Begrenzung bei den Stufen grössten Volumens. S. 91. — 35. Aneinanderfügung der Wände in Stufen grössten Volumens S. 96.

Teorem En mengde S som er symmetrisk og konveks og har større volum enn $2^n \det \Lambda$ inneholder et ikke-null latticepunkt.

Hermann Minkowski
(1864–1909)

Minkowski og et volum

«Geometrie der Zahlen»:



Drittes Kapitel. Körper, die infolge ihres Volumens mehr als einen Punkt mit ganzzahligen Coordinaten enthalten.

30. Arithmetischer Satz über die nirgends concaven Körper mit Mittelpunkt. S. 73. — 31. Stufen im Zahlengitter. S. 77. — 32. Stufen grössten Volumens. S. 81. — 33. Weiteres über den lückenlosen Aufbau von Stufen grössten Volumens. S. 86. — 34. Ebene Begrenzung bei den Stufen grössten Volumens. S. 91. — 35. Aneinanderfügung der Wände in Stufen grössten Volumens S. 96.

Teorem En mengde S som er symmetrisk og konveks og har større volum enn $2^n \det \Lambda$ inneholder et ikke-null latticepunkt.

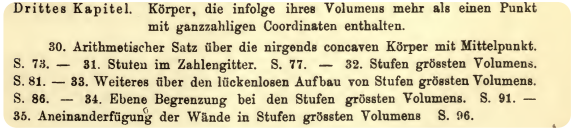
Hermites teorem Λ har et ikke-null latticepunkt kortere enn

$$\sqrt{n} \det(\Lambda)^{1/n}.$$

Hermann Minkowski
(1864–1909)

Minkowski og et volum

«Geometrie der Zahlen»:



Drittes Kapitel. Körper, die infolge ihres Volumens mehr als einen Punkt mit ganzzahligen Coordinaten enthalten.

30. Arithmetischer Satz über die nirgends concaven Körper mit Mittelpunkt. S. 73. — 31. Stufen im Zahlengitter. S. 77. — 32. Stufen grössten Volumens. S. 81. — 33. Weiteres über den lückenlosen Aufbau von Stufen grössten Volumens. S. 86. — 34. Ebene Begrenzung bei den Stufen grössten Volumens. S. 91. — 35. Aneinanderfügung der Wände in Stufen grössten Volumens S. 96.

Hermann Minkowski
(1864–1909)

Teorem En mengde S som er symmetrisk og konveks og har større volum enn $2^n \det \Lambda$ inneholder et ikke-null latticepunkt.

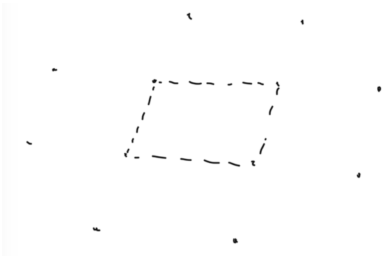
Hermites teorem Λ har et ikke-null latticepunkt kortere enn

$$\sqrt{n}\det(\Lambda)^{1/n}.$$

Hvorfor? La S være boksen med sider $2\det(\Lambda)^{1/n}$. Boksen har volum $2^n \det(\Lambda)$, så den inneholder et latticepunkt $\mathbf{x}$. Men hver koordinat er høyst $\det(\Lambda)^{1/n}$, så lengden er høyst

$$\sqrt{x_1^2 + \cdots + x_n^2} \leq \sqrt{n}\det(\Lambda)^{1/n}.$$

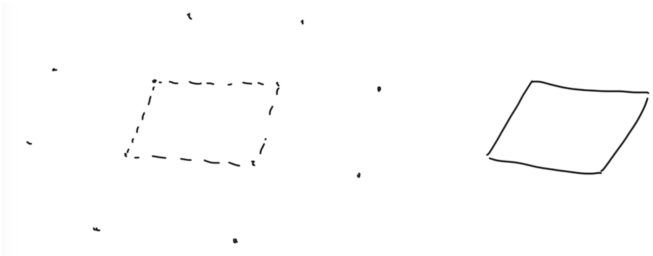
Weierstrass og en smultring



En lattice Λ kan bo i det komplekse planet.

Karl Weierstrass
(1815–1897)

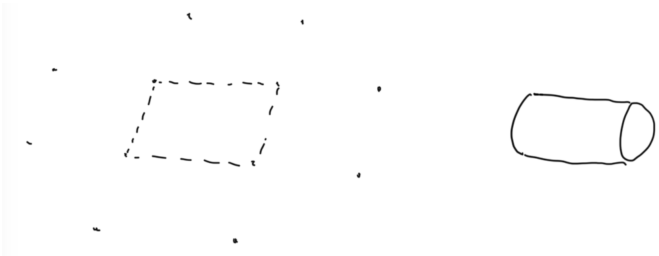
Weierstrass og en smultring



Karl Weierstrass
(1815–1897)

En lattice Λ kan bo i det komplekse planet.

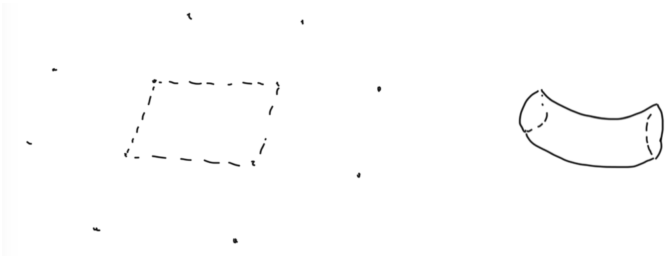
Weierstrass og en smultring



Karl Weierstrass
(1815–1897)

En lattice Λ kan bo i det komplekse planet.

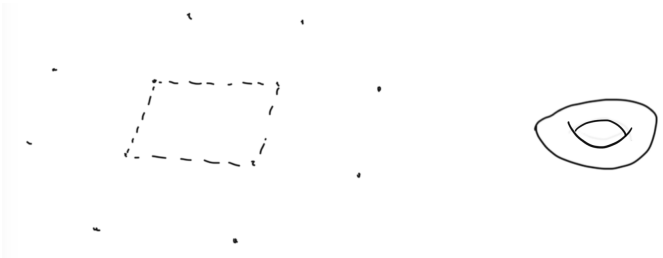
Weierstrass og en smultring



Karl Weierstrass
(1815–1897)

En lattice Λ kan bo i det komplekse planet.

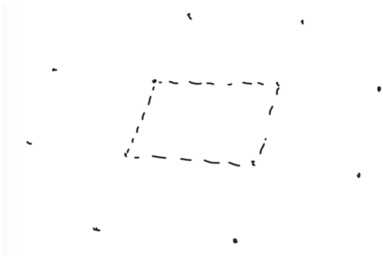
Weierstrass og en smultring

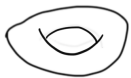


Karl Weierstrass
(1815–1897)

En lattice Λ kan bo i det komplekse planet.

Weierstrass og en smultring





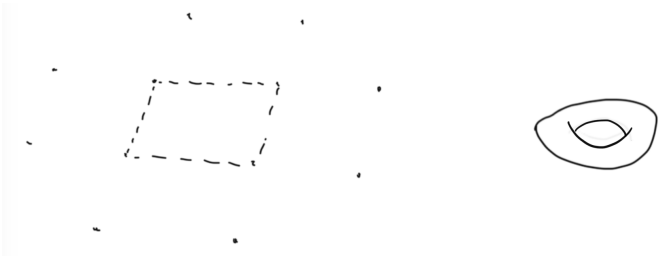
Karl Weierstrass
(1815–1897)

Vi definerer Weierstrass $\wp$-funksjon som

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{z-\omega} - \frac{1}{\omega}, \text{ og} \qquad \wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Den avbilder altså torusen ned på en elliptisk kurve.

Weierstrass og en smultring



Karl Weierstrass
(1815–1897)

Komplekse tall τ slik at $\tau\Lambda \subseteq \Lambda$ gir avbildninger på kurven.

Hvis det er mer enn $\mathbb{Z}$ har vi kompleks multiplikasjon.

Krypto i mørke middelalderen (80-tallet)

I kryptografiens barndom var det å finne utvalg av tall som summerte seg til gitte summer (subset sum, knapsack problem) populært, og mange forsøkte å lage kryptosystemer basert på slike problemer.

Et vanlig triks var å «kamuflere» et lett problem, f.eks. med å gange alle tallene med et tilfeldig tall modulo et stort tall.

Enkel $s_1, s_2, \ldots, s_n$ (f.eks. $s_i \geq 2s_{i-1}$)

Kamuflert $t_1, t_2, \ldots, t_n$ (f.eks. $t_i = s_{\pi(i)} e \bmod N$)

Krypteringsnøkkelen er den «kamuflerte» summen. Dekrypteringsnøkkelen er det tilfeldige tallet og modulusen.

Krypto i mørke middelalderen (80-tallet)

I kryptografiens barndom var det å finne utvalg av tall som summerte seg til gitte summer (subset sum, knapsack problem) populært, og mange forsøkte å lage kryptosystemer basert på slike problemer.

Et vanlig triks var å «kamuflere» et lett problem, f.eks. med å gange alle tallene med et tilfeldig tall modulo et stort tall.

Enkel $s_1, s_2, \ldots, s_n$ (f.eks. $s_i \geq 2s_{i-1}$)

Kamuflert $t_1, t_2, \ldots, t_n$ (f.eks. $t_i = s_{\pi(i)} e \bmod N$)

Krypteringsnøkkelen er den «kamuflerte» summen. Dekrypteringsnøkkelen er det tilfeldige tallet og modulusen.

Jeg krypterer ved å summere et utvalg av tall fra krypteringsnøkkelen.

Krypto i mørke middelalderen (80-tallet)

I kryptografiens barndom var det å finne utvalg av tall som summerte seg til gitte summer (subset sum, knapsack problem) populært, og mange forsøkte å lage kryptosystemer basert på slike problemer.

Et vanlig triks var å «kamuflere» et lett problem, f.eks. med å gange alle tallene med et tilfeldig tall modulo et stort tall.

Enkel $s_1, s_2, \ldots, s_n$ (f.eks. $s_i \geq 2s_{i-1}$)

Kamuflert $t_1, t_2, \ldots, t_n$ (f.eks. $t_i = s_{\pi(i)} e \bmod N$)

Krypteringsnøkkelen er den «kamuflerte» summen. Dekrypteringsnøkkelen er det tilfeldige tallet og modulusen.

Jeg krypterer ved å summere et utvalg av tall fra krypteringsnøkkelen.

Du tar bort kamuflasjon (ganger med inversen modulo det store tallet), løser det lette problemet og finner tilbake til mitt utvalg av tall.

Shamir fyller en sekk

Gitt positive heltall $s_1, s_2, \ldots, s_n$, finn de av dem som summerer seg til et gitt heltall z.

Adi Shamir
(1952–)

Shamir fyller en sekk

Gitt positive heltall $s_1, s_2, \ldots, s_n$, finn de av dem som summerer seg til et gitt heltall z.

Alternativt: Finn $a_1, \ldots, a_n \in \{0, 1\}$ slik at $\sum_{i=1}^{n} a_i s_i = z$.

Adi Shamir
(1952–)

Shamir fyller en sekk

Gitt positive heltall $s_1, s_2, \ldots, s_n$, finn de av dem som summerer seg til et gitt heltall z.

Alternativt: Finn $a_1, \ldots, a_n \in \{0, 1\}$ slik at $\sum_{i=1}^{n} a_i s_i = z$.

For denne løsningen har vi at

$$(a_1, a_2, \ldots, a_n, 1)B = (a_1, a_2, \ldots, a_n, 0) \qquad \text{hvor } B = \begin{pmatrix} 1 & & & s_1 \\ & \ddots & & \vdots \\ & & 1 & s_n \\ & & & -z \end{pmatrix}.$$

Adi Shamir
(1952–)

Shamir fyller en sekk

Gitt positive heltall $s_1, s_2, \ldots, s_n$, finn de av dem som summerer seg til et gitt heltall z.

Alternativt: Finn $a_1, \ldots, a_n \in \{0, 1\}$ slik at $\sum_{i=1}^{n} a_i s_i = z$.

For denne løsningen har vi at

$$(a_1, a_2, \ldots, a_n, 1)B = (a_1, a_2, \ldots, a_n, 0) \qquad \text{hvor } B = \begin{pmatrix} 1 & & & s_1 \\ & \ddots & & \vdots \\ & & 1 & s_n \\ & & & -z \end{pmatrix}.$$

Adi Shamir (1952–)

«De fleste» slike summer er store, så de fleste heltalls-lineærkombinasjoner av radene i B er lange vektorer, mens løsningen vi vil ha er svært kort.

Shamir fyller en sekk

Gitt positive heltall $s_1, s_2, \ldots, s_n$, finn de av dem som summerer seg til et gitt heltall z.

Alternativt: Finn $a_1, \ldots, a_n \in \{0, 1\}$ slik at $\sum_{i=1}^{n} a_i s_i = z$.

For denne løsningen har vi at

$$(a_1, a_2, \ldots, a_n, 1)B = (a_1, a_2, \ldots, a_n, 0) \qquad \text{hvor } B = \begin{pmatrix} 1 & & & s_1 \\ & \ddots & & \vdots \\ & & 1 & s_n \\ & & & -z \end{pmatrix}.$$

Adi Shamir (1952–)

«De fleste» slike summer er store, så de fleste heltalls-lineærkombinasjoner av radene i B er lange vektorer, mens løsningen vi vil ha er svært kort.

Hvis vi kan finne korte heltalls-lineærkombinasjoner er det rimelig at vi kan finne $(a_1, a_2, \ldots, a_n, 0)$.

Coppersmith og en liten rot

Vi har fått et polynom $f(X) = \sum_{i=0}^{d} f_i X^i$ som har et nullpunkt x_0 modulo N med $|x_0| < T$. Vi vil finne x_0.

Don Coppersmith
(c. 1950–)

Coppersmith og en liten rot

Vi har fått et polynom $f(X) = \sum_{i=0}^{d} f_i X^i$ som har et nullpunkt x_0 modulo N med $|x_0| < T$. Vi vil finne x_0.

Hvis vi kan finne en heltalls-lineærkombinasjon

$$h(X) = \sum_{i=0}^{d} h_i X^i = cf(X) + \sum_{i=0}^{d-1} a_i N X^i$$

slik at $\sum_i |h_i| T^i \leq N$, da er

$$h(x_0) = 0$$

fordi $h(x_0) \equiv 0 \pmod{N}$ og $|h(x_0)| \leq \sum_i |h_i| |x_0|^i \leq \sum_i |h_i| T^i < N$.

Newtons metode finner lett x_0.

Don Coppersmith
(c. 1950–)

Coppersmith og en liten rot

Vi har fått et polynom $f(X) = \sum_{i=0}^{d} f_i X^i$ som har et nullpunkt x_0 modulo N med $|x_0| < T$. Vi vil finne x_0.

Vi vil finne $h(X) = cf(X) + \sum_{i=0}^{d-1} a_i N X^i$ slik at $h(x_0) = 0$ over heltallene.

Se på matrisen

$$B = \begin{pmatrix} N & & & & \\ & NT & & & \\ & & NT^2 & & \\ & & & \ddots & \\ f_0 & f_1 T & f_2 T^2 & \dots & f_d T^d \end{pmatrix}.$$

Hvis vi kan finne heltall $a_0, a_1, \dots, a_{d-1}$ og c slik at vektoren $(a_0, a_1, \dots, a_{d-1}, c)B$ er kort, da har vi $h(X)$.

Don Coppersmith
(c. 1950–)

Lovász og to Lenstra-er

Hendrik Lenstra
(1949–)

Arjen Lenstra
(1956–)

László Lovász
(1948–)

LLL-algoritmen tar en vilkårlig basis og gir oss en bedre basis og en tilnærming til korteste latticepunkt. Algoritmen er rask.

LLL-algoritmen ligner litt på det Gauss gjorde, men arbeider med Gram-Schmidt-basisen og tillater litt slakk når basisvektorer skal byttes om.

Ring Learning With Errors

Vi har $R = \mathbb{F}_q[X]/(f(X))$ for et pent polynom $f(X)$ og passe stort primtall q.

- p er et lite primtall, $a \in R$.
- $s, e \in R$ er «korte», $b = as + pe$.

Ring Learning With Errors

Vi har $R = \mathbb{F}_q[X]/(f(X))$ for et pent polynom $f(X)$ og passe stort primtall q.

- p er et lite primtall, $a \in R$.
- $s, e \in R$ er «korte», $b = as + pe$.

Vi krypterer $m \in \{0, 1, \ldots, p-1\}$ ved å velge «korte» r, f, g og regne ut

$$x = ar + pf \qquad \text{og} \qquad w = br + pg + m.$$

Ring Learning With Errors

Vi har $R = \mathbb{F}_q[X]/(f(X))$ for et pent polynom $f(X)$ og passe stort primtall q.

- p er et lite primtall, $a \in R$.
- $s, e \in R$ er «korte», $b = as + pe$.

Vi krypterer $m \in \{0, 1, \ldots, p-1\}$ ved å velge «korte» r, f, g og regne ut

$$x = ar + pf \qquad \text{og} \qquad w = br + pg + m.$$

Vi dekrypterer ved å regne ut

$$w - xs = asr + per + pg + m - ars + pfs = m + p(\text{«kort»}).$$

Ring Learning With Errors

Vi har $R = \mathbb{F}_q[X]/(f(X))$ for et pent polynom $f(X)$ og passe stort primtall q.

- p er et lite primtall, $a \in R$.
- $s, e \in R$ er «korte», $b = as + pe$.

Vi krypterer $m \in \{0, 1, \ldots, p-1\}$ ved å velge «korte» r, f, g og regne ut

$$x = ar + pf \qquad \text{og} \qquad w = br + pg + m.$$

Vi dekrypterer ved å regne ut

$$w - xs = asr + per + pg + m - ars + pfs = m + p(\text{«kort»}).$$

Multiplikasjon med a er en lineæravbildning med matrise A:

$$\Lambda(A) = \{\mathbf{x} \in \mathbb{Z}^n \mid \exists \mathbf{y} : A\mathbf{y} \equiv \mathbf{x} \pmod{q}\}.$$

Hvorfor gidder vi: Plagsomme fysikere

En stor nok kvantedatamaskin vil bryte dagens kryptografi.

Peter Shor
(1959–)

Hvorfor gidder vi: Plagsomme fysikere

En stor nok kvantedatamaskin vil bryte dagens kryptografi.

Fysikerene prøver å lage kvantedatamaskiner nå om dagen. I høst ble det rapportert et gjennombrudd: De kan løse et kunstig og uinteressant problem raskere enn en klassisk datamaskin.

Peter Shor
(1959–)

Hvorfor gidder vi: Plagsomme fysikere

En stor nok kvantedatamaskin vil bryte dagens kryptografi.

Fysikerene prøver å lage kvantedatamaskiner nå om dagen. I høst ble det rapportert et gjennombrudd: De kan løse et kunstig og uinteressant problem raskere enn en klassisk datamaskin.

Ingen vet når (eller om) fysikerne klarer å lage tilstrekkelig store kvantedatamaskiner. Men vi er ikke villig til å vedde på at fysikerne ikke får det til, før eller siden.

Peter Shor
(1959–)

Hvorfor gidder vi: Plagsomme fysikere

En stor nok kvantedatamaskin vil bryte dagens kryptografi.

Fysikerene prøver å lage kvantedatamaskiner nå om dagen. I høst ble det rapportert et gjennombrudd: De kan løse et kunstig og uinteressant problem raskere enn en klassisk datamaskin.

Ingen vet når (eller om) fysikerne klarer å lage tilstrekkelig store kvantedatamaskiner. Men vi er ikke villig til å vedde på at fysikerne ikke får det til, før eller siden.

Lattice-basert kryptografi ser ut til å være kvantesikker.

Peter Shor
(1959–)

Hvorfor gidder vi: Plagsomt personvern

Hvis vi har to krypteringer:

$$w_1 = qs_1 + pr_1 + m_1 \qquad w_2 = qs_2 + pr_2 + m_2$$

Craig Gentry
(1973–)

Hvorfor gidder vi: Plagsomt personvern

Hvis vi har to krypteringer:

$$w_1 = qs_1 + pr_1 + m_1 \qquad w_2 = qs_2 + pr_2 + m_2$$

Da får vi:

$$w_1 + w_2 = q(s_1 + s_2) + p(r_1 + r_2) + m_1$$

Craig Gentry
(1973–)

Hvorfor gidder vi: Plagsomt personvern

Hvis vi har to krypteringer:

$$w_1 = qs_1 + pr_1 + m_1 \qquad w_2 = qs_2 + pr_2 + m_2$$

Da får vi:

$$w_1 + w_2 = q(s_1 + s_2) + p(r_1 + r_2) + m_1$$

Craig Gentry
(1973–)

Og vi får

$$w_1 w_2 = q(qs_1 + ps_1 r_2 + s_1 m_2 + ps_2 r_1 + s_2 m_1) + p(pr_1 r_2 + r_1 m_2 + r_2 m_1) + m_1 m_2$$

Hvorfor gidder vi: Plagsomt personvern

Hvis vi har to krypteringer:

$$w_1 = qs_1 + pr_1 + m_1 \qquad w_2 = qs_2 + pr_2 + m_2$$

Da får vi:

$$w_1 + w_2 = q(s_1 + s_2) + p(r_1 + r_2) + m_1$$

Craig Gentry
(1973–)

Og vi får

$$w_1 w_2 = q(qs_1 + ps_1 r_2 + s_1 m_2 + ps_2 r_1 + s_2 m_1) + p(pr_1 r_2 + r_1 m_2 + r_2 m_1) + m_1 m_2$$

Vi kan regne på krypterte data!

Spørsmål?