UNIVERSITÄT
BAYREUTH

Wie man eine diophantische Gleichung löst

Michael Stoll
Regionale Lehrerfortbildung

Graf-Münster-Gymnasium Bayreuth

27. Juni 2012

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

Beispiel:

$$x^3 + y^3 + z^3 = 29$$

mit $x, y, z \in \mathbb{Z}$.

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

Beispiel:

$$x^3 + y^3 + z^3 = 29$$

mit $x, y, z \in \mathbb{Z}$.

Lösung:

Zum Beispiel $x = 3$, $y = z = 1$.

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

Beispiel:

$$x^3 + y^3 + z^3 = 30$$

mit $x, y, z \in \mathbb{Z}$.

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

Beispiel:

$$x^3 + y^3 + z^3 = 30$$

mit $x, y, z \in \mathbb{Z}$.

Lösung:

Zum Beispiel $x = 2\,220\,422\,932$, $y = -2\,218\,888\,517$, $z = -283\,059\,965$.

(Beck et al., Juli 1999; publiziert in Math. Comp. 2007)

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

Beispiel:

$$x^3 + y^3 + z^3 = 31$$

mit $x, y, z \in \mathbb{Z}$.

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

Beispiel:

$$x^3 + y^3 + z^3 = 31$$

mit $x, y, z \in \mathbb{Z}$.

Lösung:

Keine, denn	x^3, y^3, z^3	$\equiv$	$-1, 0, 1 \bmod 9$,
und damit	$x^3 + y^3 + z^3$	$\equiv$	$-3, -2, -1, 0, 1, 2, 3 \bmod 9$,
aber	31	$\equiv$	$4 \bmod 9$.

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

Beispiel:

$$x^3 + y^3 + z^3 = 33$$

mit $x, y, z \in \mathbb{Z}$.

Diophantische Gleichungen

. . . sind Gleichungen

$$F(x_1, \ldots, x_n) = 0\,,$$

wobei F ein Polynom mit ganzzahligen Koeffizienten ist
und ganzzahlige oder rationale Lösungen gesucht werden.

Beispiel:

$$x^3 + y^3 + z^3 = 33$$

mit $x, y, z \in \mathbb{Z}$.

Lösung:

Unbekannt!

Hilberts Zehntes Problem

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.

Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden. läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

(David Hilbert, 1900)

Hilberts Zehntes Problem

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.

Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden. läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

(David Hilbert, 1900)

Hilbert war von der Lösbarkeit aller mathematischen Probleme überzeugt:

Diese Ueberzeugung von der Lösbarkeit eines jeden mathematischen Problems ist uns ein kräftiger Ansporn während der Arbeit; wir hören in uns den steten Zuruf: *Da ist das Problem, suche die Lösung. Du kannst sie durch reines Denken finden; denn in der Mathematik giebt es, kein Ignorabimus!*

Hilberts Zehntes Problem

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.

Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden. läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

(David Hilbert, 1900)

Satz (Davis, Putnam, Robinson 1961; Matiyasevich 1970)

Die Existenz von ganzzahligen Lösungen einer Polynomgleichung

$$F(x_1, \ldots, x_n) = 0$$

ist unentscheidbar.

Für Gleichungen in zwei Variablen könnte es aber besser aussehen!

Hilberts Zehntes Problem

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.

Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden. läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

(David Hilbert, 1900)

Satz (Davis, Putnam, Robinson 1961; Matiyasevich 1970)

Die Existenz von ganzzahligen Lösungen einer Polynomgleichung

$$F(x_1, \ldots, x_n) = 0$$

ist unentscheidbar.

Für Gleichungen in zwei Variablen könnte es aber besser aussehen!

Hilberts Zehntes Problem

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.

Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden. läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

(David Hilbert, 1900)

Satz (Davis, Putnam, Robinson 1961; Matiyasevich 1970)

Die Existenz von ganzzahligen Lösungen einer Polynomgleichung

$$F(x_1, \ldots, x_n) = 0$$

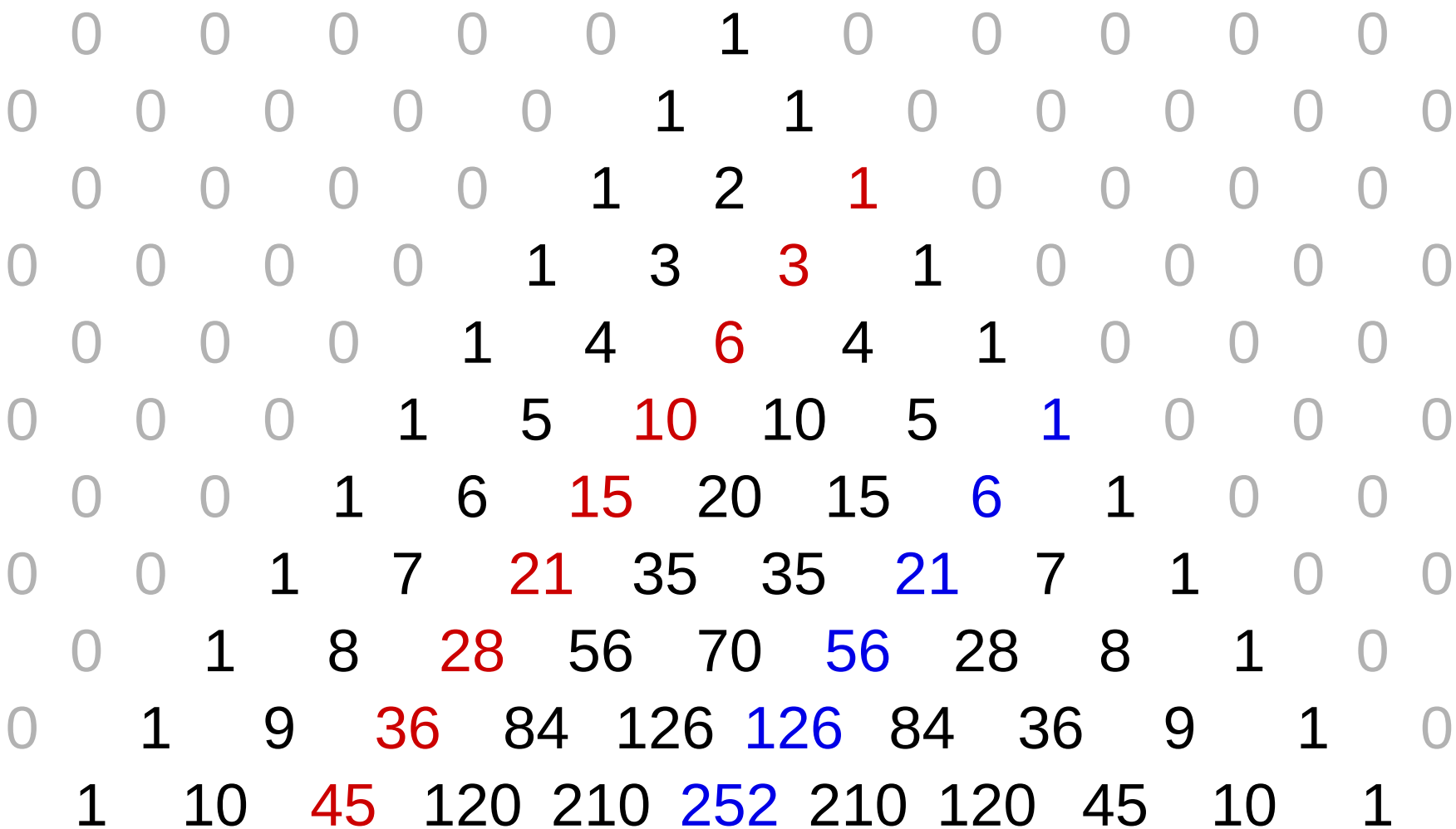
ist unentscheidbar.

Für Gleichungen in zwei Variablen könnte es aber besser aussehen!

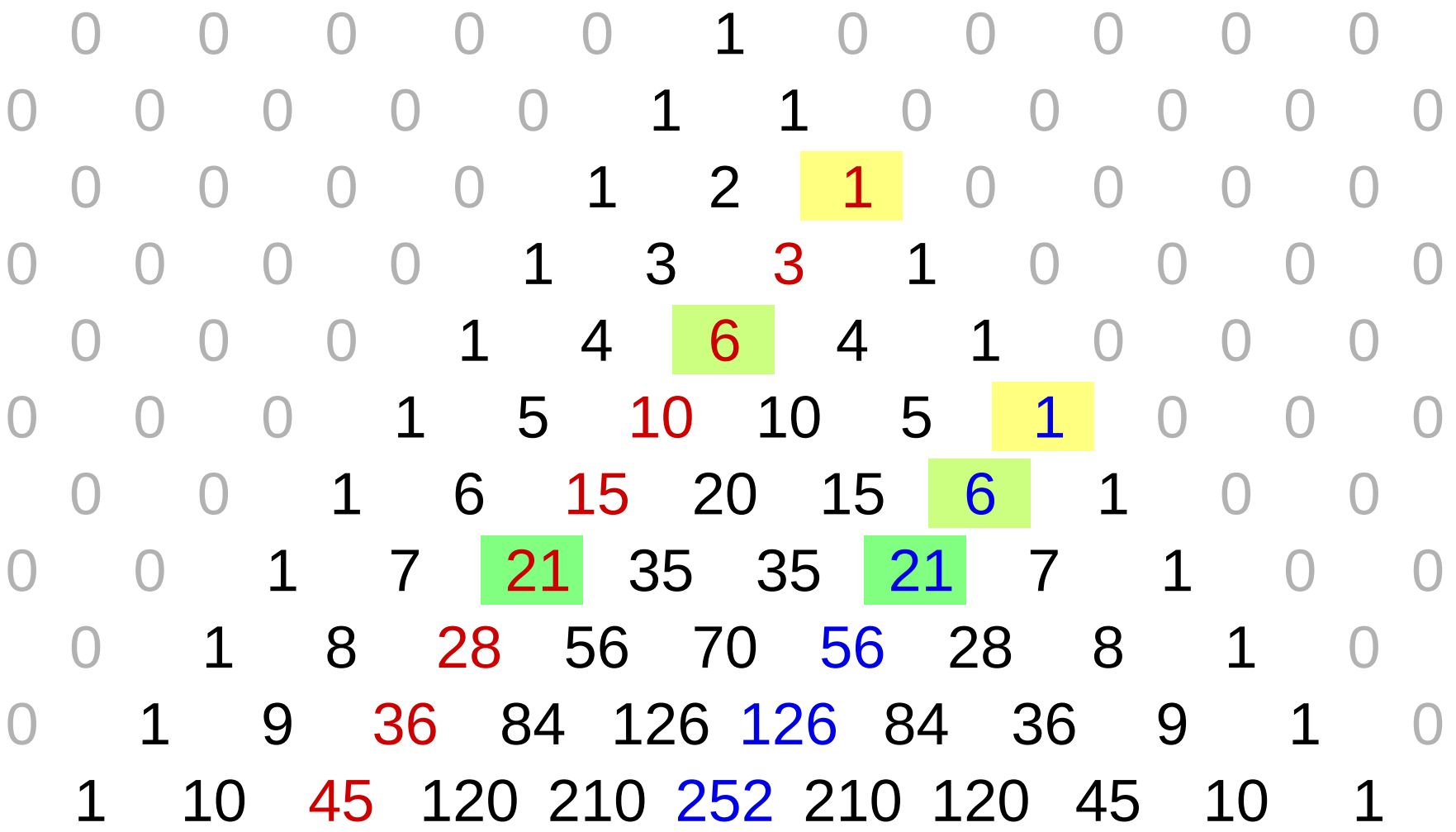
Das Pascalsche Dreieck

	0	0	0	0	0	1	0	0	0	0	0	
0	0	0	0	0	1	1	0	0	0	0	0	
	0	0	0	0	1	2	1	0	0	0	0	
0	0	0	0	1	3	3	1	0	0	0	0	
	0	0	0	1	4	6	4	1	0	0	0	
0	0	0	1	5	10	10	5	1	0	0	0	
	0	0	1	6	15	20	15	6	1	0	0	
0	0	1	7	21	35	35	21	7	1	0	0	
	0	1	8	28	56	70	56	28	8	1	0	
0	1	9	36	84	126	126	84	36	9	1	0	
	1	10	45	120	210	252	210	120	45	10	1	

Das Pascalsche Dreieck



Das Pascalsche Dreieck



Die Beispiel-Gleichung

$$\binom{y}{2} = \binom{x}{5}$$

Wir suchen die ganzzahligen Lösungen.

Es gilt $\binom{y}{2} = \binom{1-y}{2}$, also genügt es, $y \geq 1$ zu betrachten.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\binom{n}{2}$	0	0	1	3	6	10	15	21	28	36	45	55	66	78	91	105
$\binom{n}{5}$	0	0	0	0	0	1	6	21	56	126	252	462	792	1287	2002	3003

Weitere Lösungen: $x = 15,\ y = 78,$ $x = 19,\ y = 153\,.$

Die Beispiel-Gleichung

$$\binom{y}{2} = \binom{x}{5}$$

Wir suchen die ganzzahligen Lösungen.

Es gilt $\binom{y}{2} = \binom{1-y}{2}$, also genügt es, $y \geq 1$ zu betrachten.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\binom{n}{2}$	0	0	1	3	6	10	15	21	28	36	45	55	66	78	91	105
$\binom{n}{5}$	0	0	0	0	0	1	6	21	56	126	252	462	792	1287	2002	3003

Weitere Lösungen: $x = 15,\ y = 78,$ $x = 19,\ y = 153\,.$

Die Beispiel-Gleichung

$$\binom{y}{2} = \binom{x}{5}$$

Wir suchen die ganzzahligen Lösungen.

Es gilt $\binom{y}{2} = \binom{1-y}{2}$, also genügt es, $y \geq 1$ zu betrachten.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\binom{n}{2}$	0	0	1	3	6	10	15	21	28	36	45	55	66	78	91	105
$\binom{n}{5}$	0	0	0	0	0	1	6	21	56	126	252	462	792	1287	2002	3003

Weitere Lösungen: $x = 15,\ y = 78,$ $x = 19,\ y = 153\,.$

Die Beispiel-Gleichung

$$\binom{y}{2} = \binom{x}{5}$$

Wir suchen die ganzzahligen Lösungen.

Es gilt $\binom{y}{2} = \binom{1-y}{2}$, also genügt es, $y \geq 1$ zu betrachten.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\binom{n}{2}$	0	0	1	3	6	10	15	21	28	36	45	55	66	78	91	105
$\binom{n}{5}$	0	0	0	0	0	1	6	21	56	126	252	462	792	1287	2002	3003

Weitere Lösungen: $x = 15,\ y = 78,$ $x = 19,\ y = 153$.

Die Beispiel-Gleichung

$$\binom{y}{2} = \binom{x}{5}$$

Wir suchen die ganzzahligen Lösungen.

Es gilt $\binom{y}{2} = \binom{1-y}{2}$, also genügt es, $y \geq 1$ zu betrachten.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\binom{n}{2}$	0	0	1	3	6	10	15	21	28	36	45	55	66	78	91	105
$\binom{n}{5}$	0	0	0	0	0	1	6	21	56	126	252	462	792	1287	2002	3003

Weitere Lösungen: $x = 15,\ y = 78,$ $x = 19,\ y = 153\,.$

Die Beispiel-Gleichung

$$\binom{y}{2} = \binom{x}{5}$$

Wir suchen die ganzzahligen Lösungen.

Es gilt $\binom{y}{2} = \binom{1-y}{2}$, also genügt es, $y \geq 1$ zu betrachten.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\binom{n}{2}$	0	0	1	3	6	10	15	21	28	36	45	55	66	78	91	105
$\binom{n}{5}$	0	0	0	0	0	1	6	21	56	126	252	462	792	1287	2002	3003

Weitere Lösungen: $x = 15,\ y = 78,$ $x = 19,\ y = 153\,.$

Die Beispiel-Gleichung

$$\binom{y}{2} = \binom{x}{5}$$

Wir suchen die ganzzahligen Lösungen.

Es gilt $\binom{y}{2} = \binom{1-y}{2}$, also genügt es, $y \geq 1$ zu betrachten.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\binom{n}{2}$	0	0	1	3	6	10	15	21	28	36	45	55	66	78	91	105
$\binom{n}{5}$	0	0	0	0	0	1	6	21	56	126	252	462	792	1287	2002	3003

Weitere Lösungen: $x = 15,\ y = 78,$ $x = 19,\ y = 153\,.$

Die Beispiel-Gleichung

$$\binom{y}{2} = \binom{x}{5}$$

Wir suchen die ganzzahligen Lösungen.

Es gilt $\binom{y}{2} = \binom{1-y}{2}$, also genügt es, $y \geq 1$ zu betrachten.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\binom{n}{2}$	0	0	1	3	6	10	15	21	28	36	45	55	66	78	91	105
$\binom{n}{5}$	0	0	0	0	0	1	6	21	56	126	252	462	792	1287	2002	3003

Weitere Lösungen: $x = 15,\ y = 78,$ $x = 19,\ y = 153\,.$

Abschätzungen

Was können wir über die Lösungsmenge sagen?

Satz (Siegel 1929)

Eine Gleichung $F(x, y) = 0$ hat nur endlich viele ganzzahlige Lösungen, oder die Lösungen sind rational parametrisierbar.

Aber keine Abschätzung für die Größe der Lösungen!

Baker 1960er Jahre, „Linearformen in Logarithmen“

$$\Longrightarrow \qquad |x| < 10^{10^{10^{10^{600}}}} \qquad \text{für Lösungen } (x, y) \text{ unserer Gleichung.}$$

Viele Verbesserungen bis heute

$$\Longrightarrow \qquad |x| < 10^{10^{600}} \qquad \text{für Lösungen } (x, y) \text{ unserer Gleichung.}$$

Abschätzungen

Was können wir über die Lösungsmenge sagen?

Satz (Siegel 1929)

Eine Gleichung $F(x, y) = 0$ hat nur endlich viele ganzzahlige Lösungen, oder die Lösungen sind rational parametrisierbar.

Aber keine Abschätzung für die Größe der Lösungen!

Baker 1960er Jahre, „Linearformen in Logarithmen“

$$\Longrightarrow \qquad |x| < 10^{10^{10^{10^{600}}}} \qquad \text{für Lösungen } (x, y) \text{ unserer Gleichung.}$$

Viele Verbesserungen bis heute

$$\Longrightarrow \qquad |x| < 10^{10^{600}} \qquad \text{für Lösungen } (x, y) \text{ unserer Gleichung.}$$

Abschätzungen

Was können wir über die Lösungsmenge sagen?

Satz (Siegel 1929)

Eine Gleichung $F(x, y) = 0$ hat nur endlich viele ganzzahlige Lösungen, oder die Lösungen sind rational parametrisierbar.

Aber keine Abschätzung für die Größe der Lösungen!

Baker 1960er Jahre, „Linearformen in Logarithmen“

$$\Longrightarrow \qquad |x| < 10^{10^{10^{10^{600}}}} \qquad \text{für Lösungen } (x, y) \text{ unserer Gleichung.}$$

Viele Verbesserungen bis heute

$$\Longrightarrow \qquad |x| < 10^{10^{600}} \qquad \text{für Lösungen } (x, y) \text{ unserer Gleichung.}$$

Abschätzungen

Was können wir über die Lösungsmenge sagen?

Satz (Siegel 1929)

Eine Gleichung $F(x, y) = 0$ hat nur endlich viele ganzzahlige Lösungen, oder die Lösungen sind rational parametrisierbar.

Aber keine Abschätzung für die Größe der Lösungen!

Baker 1960er Jahre, „Linearformen in Logarithmen“

$$\Longrightarrow \qquad |x| < 10^{10^{10^{10^{600}}}} \qquad \text{für Lösungen } (x, y) \text{ unserer Gleichung.}$$

Viele Verbesserungen bis heute

$$\Longrightarrow \qquad |x| < 10^{10^{600}} \qquad \text{für Lösungen } (x, y) \text{ unserer Gleichung.}$$

Abschätzungen

Was können wir über die Lösungsmenge sagen?

Satz (Siegel 1929)

Eine Gleichung $F(x, y) = 0$ hat nur endlich viele ganzzahlige Lösungen, oder die Lösungen sind rational parametrisierbar.

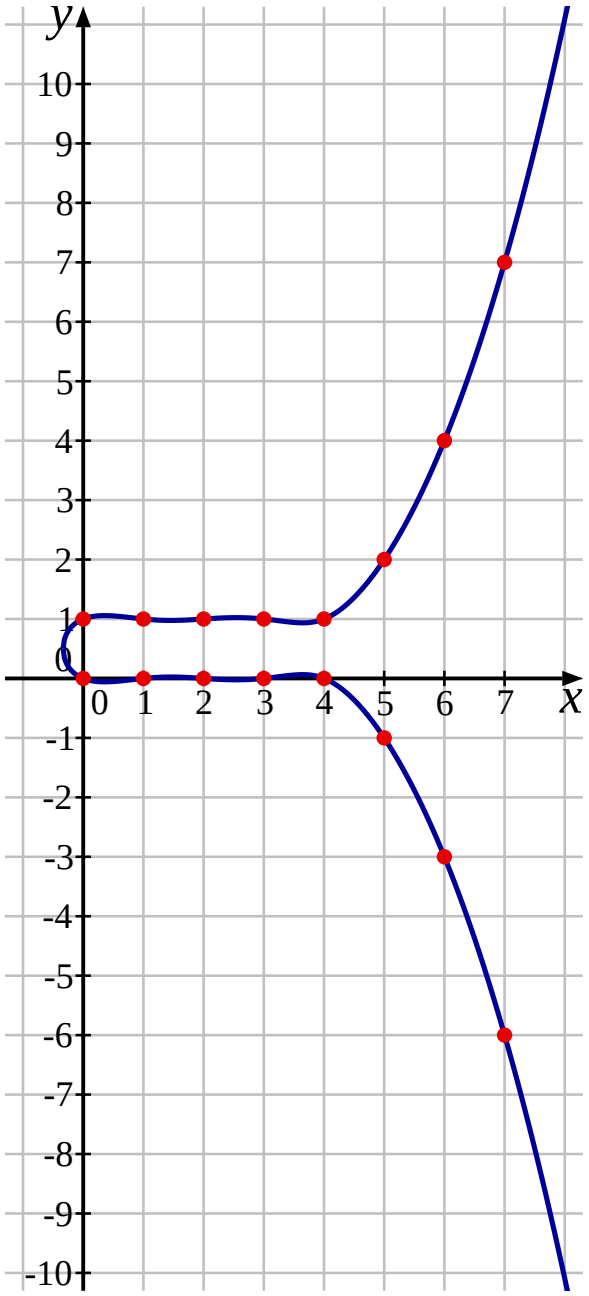
Aber keine Abschätzung für die Größe der Lösungen!

Baker 1960er Jahre, „Linearformen in Logarithmen“

$\Longrightarrow$ $|x| < 10^{10^{10^{10^{600}}}}$ für Lösungen (x, y) unserer Gleichung.

Viele Verbesserungen bis heute

$\Longrightarrow$ $|x| < 10^{10^{600}}$ für Lösungen (x, y) unserer Gleichung.



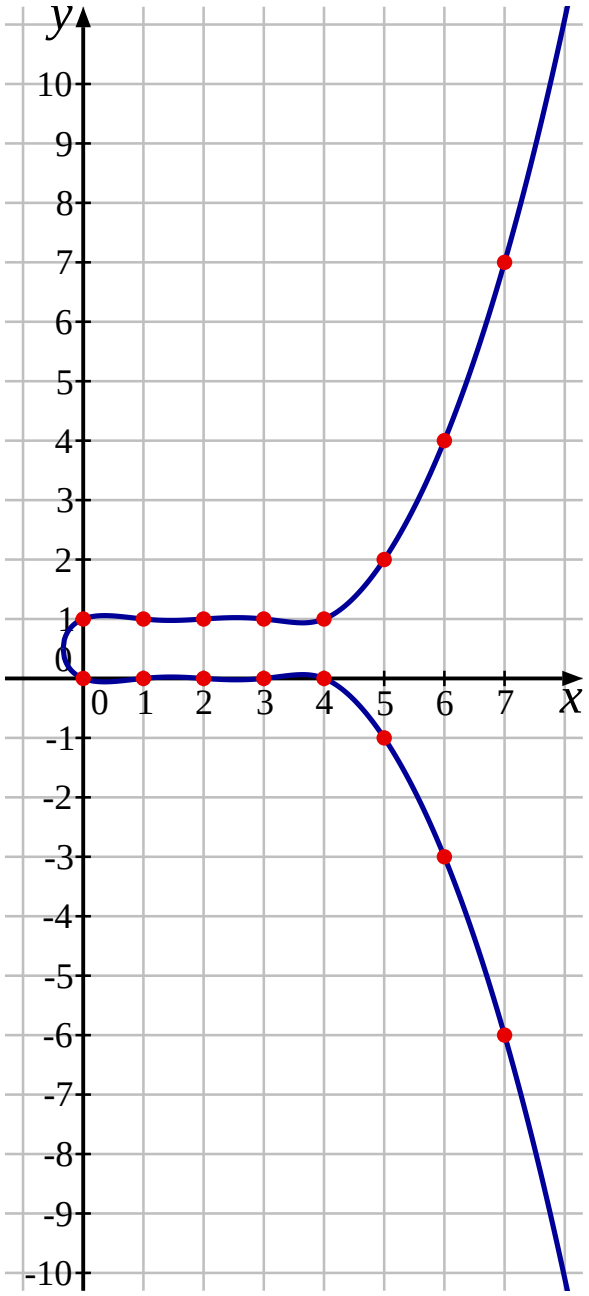
Etwas Geometrie

Unsere Gleichung beschreibt
eine ebene algebraische Kurve C;
wir wollen die Menge $C(\mathbb{Z})$
der ganzzahligen Punkte bestimmen.

Wir können C in eine abelsche Fläche J einbetten.

Mit den Punkten einer abelschen Fläche kann man rechnen.

Satz (Weil 1928)
$J(\mathbb{Z})$ ist eine endlich erzeugte abelsche Gruppe.



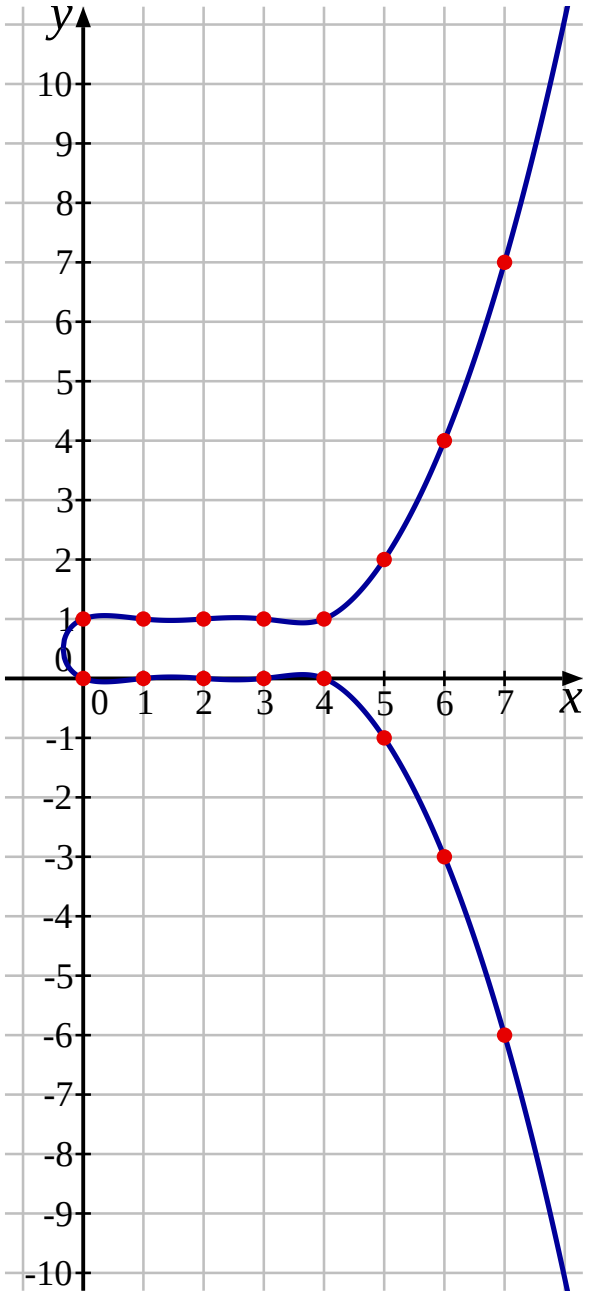
Etwas Geometrie

Unsere Gleichung beschreibt
eine ebene algebraische Kurve C;
wir wollen die Menge $C(\mathbb{Z})$
der ganzzahligen Punkte bestimmen.

Wir können C in eine abelsche Fläche J
einbetten.

Mit den Punkten einer abelschen Fläche
kann man rechnen.

Satz (Weil 1928)
$J(\mathbb{Z})$ ist eine endlich erzeugte abelsche Gruppe.



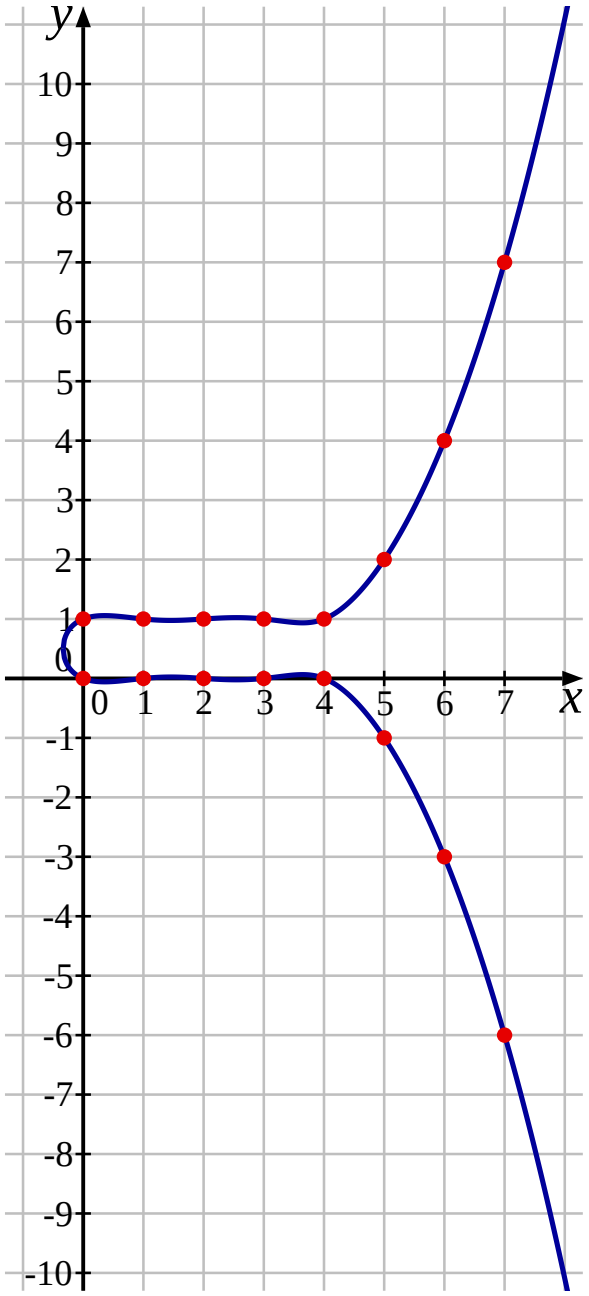
Etwas Geometrie

Unsere Gleichung beschreibt
eine ebene algebraische Kurve C;
wir wollen die Menge $C(\mathbb{Z})$
der ganzzahligen Punkte bestimmen.

Wir können C in eine abelsche Fläche J
einbetten.

Mit den Punkten einer abelschen Fläche
kann man rechnen.

Satz (Weil 1928)
$J(\mathbb{Z})$ ist eine endlich erzeugte abelsche Gruppe.



Etwas Geometrie

Unsere Gleichung beschreibt
eine ebene algebraische Kurve C;
wir wollen die Menge $C(\mathbb{Z})$
der ganzzahligen Punkte bestimmen.

Wir können C in eine abelsche Fläche J
einbetten.

Mit den Punkten einer abelschen Fläche
kann man rechnen.

Satz (Weil 1928)
$J(\mathbb{Z})$ ist eine endlich erzeugte abelsche Gruppe.

Die Gruppe

In unserem Fall gibt es sechs Punkte $P_1, \ldots, P_6 \in J(\mathbb{Z})$,
die wir explizit bestimmen können,
so dass jeder Punkt P in $J(\mathbb{Z})$ eindeutig geschrieben werden kann als

$$P = n_1 \cdot P_1 + n_2 \cdot P_2 + n_3 \cdot P_3 + n_4 \cdot P_4 + n_5 \cdot P_5 + n_6 \cdot P_6$$

mit ganzen Zahlen $n_1, n_2, n_3, n_4, n_5, n_6$.

Ist $P \in C(\mathbb{Z})$, dann gilt

$$\log |x(P)| \approx n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 + n_6^2 \,.$$

Aus der Abschätzung $|x(P)| < 10^{10^{600}}$ folgt dann (in etwa)

$$|n_1|, |n_2|, |n_3|, |n_4|, |n_5|, |n_6| < 10^{300} \,.$$

Die Größe des Suchraums verkleinert sich auf etwa 10^{1800}!

Die Gruppe

In unserem Fall gibt es sechs Punkte $P_1, \ldots, P_6 \in J(\mathbb{Z})$,
die wir explizit bestimmen können,
so dass jeder Punkt P in $J(\mathbb{Z})$ eindeutig geschrieben werden kann als

$$P = n_1 \cdot P_1 + n_2 \cdot P_2 + n_3 \cdot P_3 + n_4 \cdot P_4 + n_5 \cdot P_5 + n_6 \cdot P_6$$

mit ganzen Zahlen $n_1, n_2, n_3, n_4, n_5, n_6$.

Ist $P \in C(\mathbb{Z})$, dann gilt

$$\log |x(P)| \approx n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 + n_6^2 \,.$$

Aus der Abschätzung $|x(P)| < 10^{10^{600}}$ folgt dann (in etwa)

$$|n_1|, |n_2|, |n_3|, |n_4|, |n_5|, |n_6| < 10^{300} \,.$$

Die Größe des Suchraums verkleinert sich auf etwa 10^{1800}!

Die Gruppe

In unserem Fall gibt es sechs Punkte $P_1, \ldots, P_6 \in J(\mathbb{Z})$,
die wir explizit bestimmen können,
so dass jeder Punkt P in $J(\mathbb{Z})$ geschrieben werden kann als

$$P = n_1 \cdot P_1 + n_2 \cdot P_2 + n_3 \cdot P_3 + n_4 \cdot P_4 + n_5 \cdot P_5 + n_6 \cdot P_6$$

mit ganzen Zahlen $n_1, n_2, n_3, n_4, n_5, n_6$.

Ist $P \in C(\mathbb{Z})$, dann gilt

$$\log |x(P)| \approx n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 + n_6^2 \,.$$

Aus der Abschätzung $|x(P)| < 10^{10^{600}}$ folgt dann (in etwa)

$$|n_1|, |n_2|, |n_3|, |n_4|, |n_5|, |n_6| < 10^{300} \,.$$

Die Größe des Suchraums verkleinert sich auf etwa 10^{1800}!

Die Gruppe

In unserem Fall gibt es sechs Punkte $P_1, \ldots, P_6 \in J(\mathbb{Z})$,
die wir explizit bestimmen können,
so dass jeder Punkt P in $J(\mathbb{Z})$ eindeutig geschrieben werden kann als

$$P = n_1 \cdot P_1 + n_2 \cdot P_2 + n_3 \cdot P_3 + n_4 \cdot P_4 + n_5 \cdot P_5 + n_6 \cdot P_6$$

mit ganzen Zahlen $n_1, n_2, n_3, n_4, n_5, n_6$.

Ist $P \in C(\mathbb{Z})$, dann gilt

$$\log |x(P)| \approx n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 + n_6^2 \,.$$

Aus der Abschätzung $|x(P)| < 10^{10^{600}}$ folgt dann (in etwa)

$$|n_1|, |n_2|, |n_3|, |n_4|, |n_5|, |n_6| < 10^{300} \,.$$

Die Größe des Suchraums verkleinert sich auf etwa 10^{1800}!

Verkleinerung des Heuhaufens

Die Zahlen $n_1, \ldots, n_6$ sind klein genug, dass man mit ihnen rechnen kann.

Allerdings ist der Suchraum noch immer viel zu groß,
als dass man ihn komplett absuchen könnte.

Deshalb betrachten wir zunächst ein einfacheres Problem:

Wir finden heraus, welche Lösungen es modulo p gibt,
und von welchen $n_1, \ldots, n_6$ sie repräsentiert werden.

Dies ist ein (relativ kleines) endliches Problem und daher lösbar.

Für jede Primzahl p erhalten wir Bedingungen,
die $n_1, \ldots, n_6$ erfüllen müssen.

Verkleinerung des Heuhaufens

Die Zahlen $n_1, \ldots, n_6$ sind klein genug, dass man mit ihnen rechnen kann.

Allerdings ist der Suchraum noch immer viel zu groß,
als dass man ihn komplett absuchen könnte.

Deshalb betrachten wir zunächst ein einfacheres Problem:

Wir finden heraus, welche Lösungen es modulo p gibt,
und von welchen $n_1, \ldots, n_6$ sie repräsentiert werden.

Dies ist ein (relativ kleines) endliches Problem und daher lösbar.

Für jede Primzahl p erhalten wir Bedingungen,
die $n_1, \ldots, n_6$ erfüllen müssen.

Verkleinerung des Heuhaufens

Die Zahlen $n_1, \ldots, n_6$ sind klein genug, dass man mit ihnen rechnen kann.

Allerdings ist der Suchraum noch immer viel zu groß,
als dass man ihn komplett absuchen könnte.

Deshalb betrachten wir zunächst ein einfacheres Problem:

Wir finden heraus, welche Lösungen es modulo p gibt,
und von welchen $n_1, \ldots, n_6$ sie repräsentiert werden.

Dies ist ein (relativ kleines) endliches Problem und daher lösbar.

Für jede Primzahl p erhalten wir Bedingungen,
die $n_1, \ldots, n_6$ erfüllen müssen.

Verkleinerung des Heuhaufens

Die Zahlen $n_1, \ldots, n_6$ sind klein genug, dass man mit ihnen rechnen kann.

Allerdings ist der Suchraum noch immer viel zu groß,
als dass man ihn komplett absuchen könnte.

Deshalb betrachten wir zunächst ein einfacheres Problem:

Wir finden heraus, welche Lösungen es modulo p gibt,
und von welchen $n_1, \ldots, n_6$ sie repräsentiert werden.

Dies ist ein (relativ kleines) endliches Problem und daher lösbar.

Für jede Primzahl p erhalten wir Bedingungen,
die $n_1, \ldots, n_6$ erfüllen müssen.

Verkleinerung des Heuhaufens

Die Zahlen $n_1, \ldots, n_6$ sind klein genug, dass man mit ihnen rechnen kann.

Allerdings ist der Suchraum noch immer viel zu groß,
als dass man ihn komplett absuchen könnte.

Deshalb betrachten wir zunächst ein einfacheres Problem:

Wir finden heraus, welche Lösungen es modulo p gibt,
und von welchen $n_1, \ldots, n_6$ sie repräsentiert werden.

Dies ist ein (relativ kleines) endliches Problem und daher lösbar.

Für jede Primzahl p erhalten wir Bedingungen,
die $n_1, \ldots, n_6$ erfüllen müssen.

Arbeit für den Computer

Wir wollen viele dieser Bedingungen mit einander kombinieren.

Dazu muss man die Primzahlen geschickt auswählen
und die benötigten Algorithmen sorgfältig und effizient programmieren.

Nach etlichen Stunden Rechenzeit ist der größte Teil des Heuhaufens weg,
und man hat gezeigt:

Ist (x, y) eine ganzzahlige Lösung,
dann ist x entweder klein und die Lösung bekannt,
oder x ist sehr groß: $|x| > 10^{10^{600}}$.

Arbeit für den Computer

Wir wollen viele dieser Bedingungen mit einander kombinieren.

Dazu muss man die Primzahlen geschickt auswählen
und die benötigten Algorithmen sorgfältig und effizient programmieren.

Nach etlichen Stunden Rechenzeit ist der größte Teil des Heuhaufens weg,
und man hat gezeigt:

Ist (x, y) eine ganzzahlige Lösung,
dann ist x entweder klein und die Lösung bekannt,
oder x ist sehr groß: $|x| > 10^{10^{600}}$.

Arbeit für den Computer

Wir wollen viele dieser Bedingungen mit einander kombinieren.

Dazu muss man die Primzahlen geschickt auswählen
und die benötigten Algorithmen sorgfältig und effizient programmieren.

Nach etlichen Stunden Rechenzeit ist der größte Teil des Heuhaufens weg,
und man hat gezeigt:

Ist (x, y) eine ganzzahlige Lösung,
dann ist x entweder klein und die Lösung bekannt,
oder x ist sehr groß: $|x| > 10^{10^{600}}$.

Arbeit für den Computer

Wir wollen viele dieser Bedingungen mit einander kombinieren.

Dazu muss man die Primzahlen geschickt auswählen
und die benötigten Algorithmen sorgfältig und effizient programmieren.

Nach etlichen Stunden Rechenzeit ist der größte Teil des Heuhaufens weg,
und man hat gezeigt:

Ist (x, y) eine ganzzahlige Lösung,
dann ist x entweder klein und die Lösung bekannt,
oder x ist sehr groß: $|x| > 10^{10^{600}}$.

Das Ergebnis

Satz (Bugeaud, Mignotte, Siksek, Stoll, Tengely)

Sind $x, y \in \mathbb{Z}$ mit $$\binom{y}{2} = \binom{x}{5},$$

dann gilt $$x \in \{0, 1, 2, 3, 4, 5, 6, 7, 15, 19\}.$$

[Algebra & Number Theory **2**, No. 8, 859–885 (2008)]