UNIVERSITÄT
BAYREUTH

Frey-Kurven und die verallgemeinerte Fermatsche Gleichung

Michael Stoll
Universität Bayreuth

Verleihung der Ehrendoktorwürde an Gerhard Frey

Universität des Saarlandes, Saarbrücken

25. Juli 2014

Gerhard Frey und die Fermatsche Gleichung

Gerhard Frey und die Fermatsche Gleichung

Während seiner Saarbrücker Zeit
fand Gerhard Frey Mitte der 1980er Jahre
einen Zusammenhang
zwischen der Fermatschen Gleichung

$$a^n + b^n = c^n$$

und Vermutungen über elliptische Kurven

$$E\colon y^2 = x^3 + Ax + B\,.$$

Dies war ein entscheidender Schritt
für den Beweis der Fermatschen Vermutung.

Gerhard Frey und die Fermatsche Gleichung

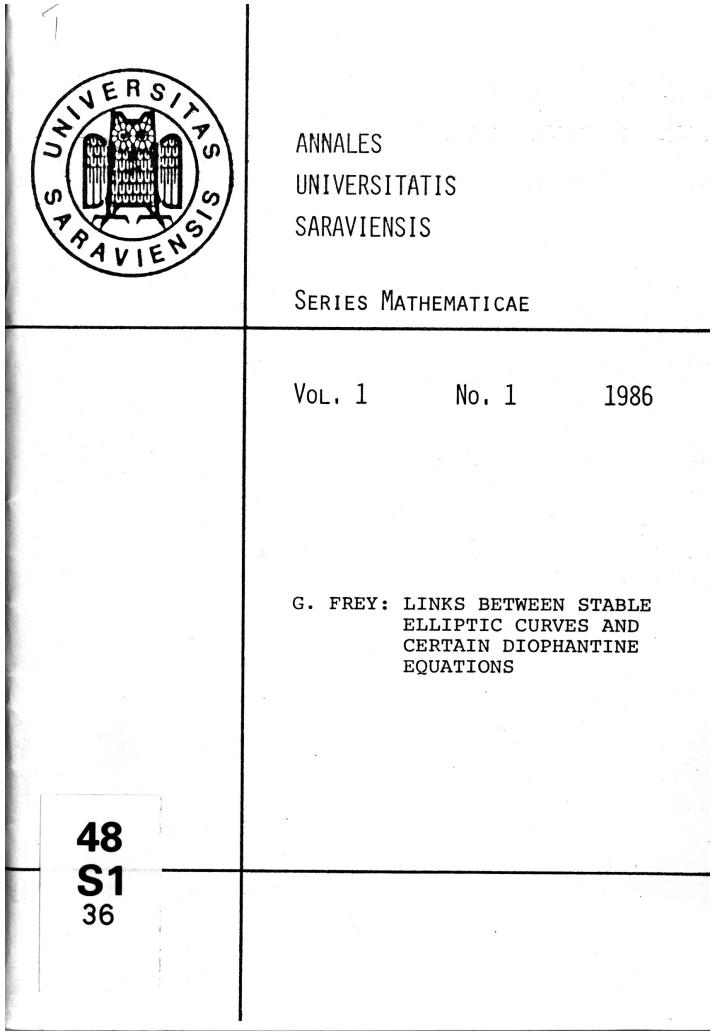
Während seiner Saarbrücker Zeit
fand Gerhard Frey Mitte der 1980er Jahre
einen Zusammenhang
zwischen der Fermatschen Gleichung

$$a^n + b^n = c^n$$

und Vermutungen über elliptische Kurven

$$E: y^2 = x^3 + Ax + B\,.$$

Dies war ein entscheidender Schritt
für den Beweis der Fermatschen Vermutung.



Die Behauptung von Fermat

Die Behauptung von Fermat

Pierre de Fermat (1601–1665)

Die Behauptung von Fermat

Pierre de Fermat (1601–1665)
im Rand seiner *Arithmetika* von **Diophant**:

Cubum autem in duos cubos,
aut quadratoquadratum in duos quadratoquadratos
et generaliter nullam in infinitum ultra quadratum potestatem
in duos eiusdem nominis fas est dividere,
cuius rei demonstrationem mirabilem sane detexi.
Hanc marginis exiguitas non caperet.

Die Behauptung von Fermat

Pierre de Fermat (1601–1665)
im Rand seiner *Arithmetika* von **Diophant**:

Cubum autem in duos cubos,
aut quadratoquadratum in duos quadratoquadratos
et generaliter nullam in infinitum ultra quadratum potestatem
in duos eiusdem nominis fas est dividere,
cuius rei demonstrationem mirabilem sane detexi.
Hanc marginis exiguitas non caperet:

$$a^n + b^n \neq c^n \qquad \text{für } a, b, c \in \mathbb{Z}_{>0},\ n > 2.$$

Die Behauptung von Fermat

Pierre de Fermat (1601–1665)
im Rand seiner *Arithmetika* von **Diophant**:

Cubum autem in duos cubos,
aut quadratoquadratum in duos quadratoquadratos
et generaliter nullam in infinitum ultra quadratum potestatem
in duos eiusdem nominis fas est dividere,
cuius rei demonstrationem mirabilem sane detexi.
Hanc marginis exiguitas non caperet:

$$a^n + b^n \neq c^n \qquad \text{für } a, b, c \in \mathbb{Z}_{>0},\ n > 2.$$

Heute besteht weitgehend Konsens,
dass Fermat keinen allgemeinen Beweis hatte (außer für $n = 3$(?) und 4).

Die Behauptung von Fermat

Pierre de Fermat (1601–1665)
im Rand seiner *Arithmetika* von **Diophant**:

Cubum autem in duos cubos,
aut quadratoquadratum in duos quadratoquadratos
et generaliter nullam in infinitum ultra quadratum potestatem
in duos eiusdem nominis fas est dividere,
cuius rei demonstrationem mirabilem sane detexi.
Hanc marginis exiguitas non caperet:

$$a^n + b^n \neq c^n \qquad \text{für } a, b, c \in \mathbb{Z}_{>0},\ n > 2.$$

Heute besteht weitgehend Konsens,
dass Fermat keinen allgemeinen Beweis hatte (außer für $n = 3$(?) und 4).

Wesentliche Fortschritte erst durch **Ernst Eduard Kummer** ~1850:
Die Aussage stimmt für alle (schwach) „regulären“ Primzahl-Exponenten.

Die Behauptung von Fermat

Pierre de Fermat (1601–1665)
im Rand seiner *Arithmetika* von **Diophant**:

Cubum autem in duos cubos,
aut quadratoquadratum in duos quadratoquadratos
et generaliter nullam in infinitum ultra quadratum potestatem
in duos eiusdem nominis fas est dividere,
cuius rei demonstrationem mirabilem sane detexi.
Hanc marginis exiguitas non caperet:

$$a^n + b^n \neq c^n \qquad \text{für } a, b, c \in \mathbb{Z}_{>0},\ n > 2.$$

Heute besteht weitgehend Konsens,
dass Fermat keinen allgemeinen Beweis hatte (außer für $n = 3$(?) und 4).

Wesentliche Fortschritte erst durch **Ernst Eduard Kummer** ~1850:
Die Aussage stimmt für alle (schwach) „regulären“ Primzahl-Exponenten.

Bis 1980er Jahre: Numerische Kriterien liefern Gültigkeit für $n \leq 4\,000\,000$.

Die ursprüngliche Frey-Kurve

Die ursprüngliche Frey-Kurve

Wir können annehmen, dass $n = \ell \geq 5$ eine Primzahl ist.
Sei $(a, b, c) \in \mathbb{Z}^3$ eine nichttriviale Lösung ($abc \neq 0$) der Gleichung

$$a^\ell + b^\ell = c^\ell$$

mit (o.E.) a, b, c teilerfremd, a gerade und $b \equiv 1 \bmod 4$.

Die ursprüngliche Frey-Kurve

Wir können annehmen, dass $n = \ell \geq 5$ eine Primzahl ist.
Sei $(a, b, c) \in \mathbb{Z}^3$ eine nichttriviale Lösung ($abc \neq 0$) der Gleichung

$$a^\ell + b^\ell = c^\ell$$

mit (o.E.) a, b, c teilerfremd, a gerade und $b \equiv 1 \bmod 4$.

Frey betrachtet nun die elliptische Kurve

$$E_{a,b,c} \colon y^2 = x(x - a^\ell)(x + b^\ell)\,.$$

Die ursprüngliche Frey-Kurve

Wir können annehmen, dass $n = \ell \geq 5$ eine Primzahl ist.
Sei $(a, b, c) \in \mathbb{Z}^3$ eine nichttriviale Lösung ($abc \neq 0$) der Gleichung

$$a^\ell + b^\ell = c^\ell$$

mit (o.E.) a, b, c teilerfremd, a gerade und $b \equiv 1 \bmod 4$.

Frey betrachtet nun die elliptische Kurve

$$E_{a,b,c} \colon y^2 = x(x - a^\ell)(x + b^\ell)\,.$$

Diese Kurve müsste dermaßen ungewöhnliche Eigenschaften haben, dass sie nicht existieren sollte:

Die ursprüngliche Frey-Kurve

Wir können annehmen, dass $n = \ell \geq 5$ eine Primzahl ist.
Sei $(a, b, c) \in \mathbb{Z}^3$ eine nichttriviale Lösung ($abc \neq 0$) der Gleichung

$$a^\ell + b^\ell = c^\ell$$

mit (o.E.) a, b, c teilerfremd, a gerade und $b \equiv 1 \bmod 4$.

Frey betrachtet nun die elliptische Kurve

$$E_{a,b,c} \colon y^2 = x(x - a^\ell)(x + b^\ell)\,.$$

Diese Kurve müsste dermaßen ungewöhnliche Eigenschaften haben, dass sie nicht existieren sollte:

$E_{a,b,c}$ kann nicht modular sein

Die ursprüngliche Frey-Kurve

Wir können annehmen, dass $n = \ell \geq 5$ eine Primzahl ist.
Sei $(a, b, c) \in \mathbb{Z}^3$ eine nichttriviale Lösung ($abc \neq 0$) der Gleichung

$$a^\ell + b^\ell = c^\ell$$

mit (o.E.) a, b, c teilerfremd, a gerade und $b \equiv 1 \bmod 4$.

Frey betrachtet nun die elliptische Kurve

$$E_{a,b,c} \colon y^2 = x(x - a^\ell)(x + b^\ell)\,.$$

Diese Kurve müsste dermaßen ungewöhnliche Eigenschaften haben, dass sie nicht existieren sollte:

$E_{a,b,c}$ kann nicht modular sein

im Widerspruch zu einer Vermutung von Taniyama und Shimura.

Elliptische Kurven: Definition

Elliptische Kurven: Definition

Eine Elliptische Kurve E über $\mathbb{Q}$ ist gegeben durch eine Gleichung

$$E\colon y^2 = f(x) = x^3 + rx^2 + sx + t$$

mit $r, s, t \in \mathbb{Z}$
und f ohne mehrfache Nullstellen.

Elliptische Kurven: Definition

Eine Elliptische Kurve E über $\mathbb{Q}$ ist gegeben durch eine Gleichung

$$E\colon y^2 = f(x) = x^3 + rx^2 + sx + t$$

mit $r, s, t \in \mathbb{Z}$
und f ohne mehrfache Nullstellen.

Ihre Punkte sind Paare (ξ, η) mit $\eta^2 = f(\xi)$
und ein „Punkt im Unendlichen“ O.

Elliptische Kurven: Definition

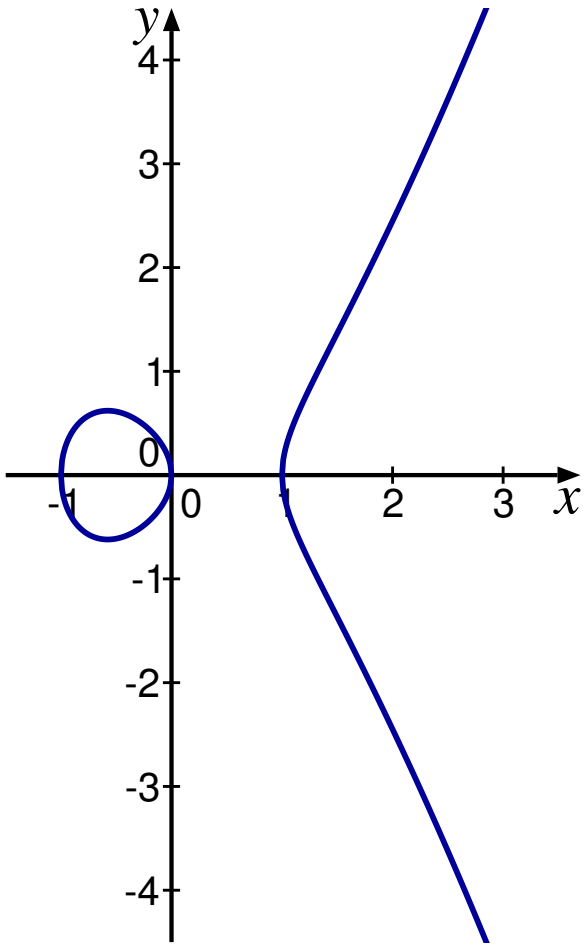
Eine Elliptische Kurve E über $\mathbb{Q}$ ist gegeben durch eine Gleichung

$$E\colon y^2 = f(x) = x^3 + rx^2 + sx + t$$

mit $r, s, t \in \mathbb{Z}$
und f ohne mehrfache Nullstellen.

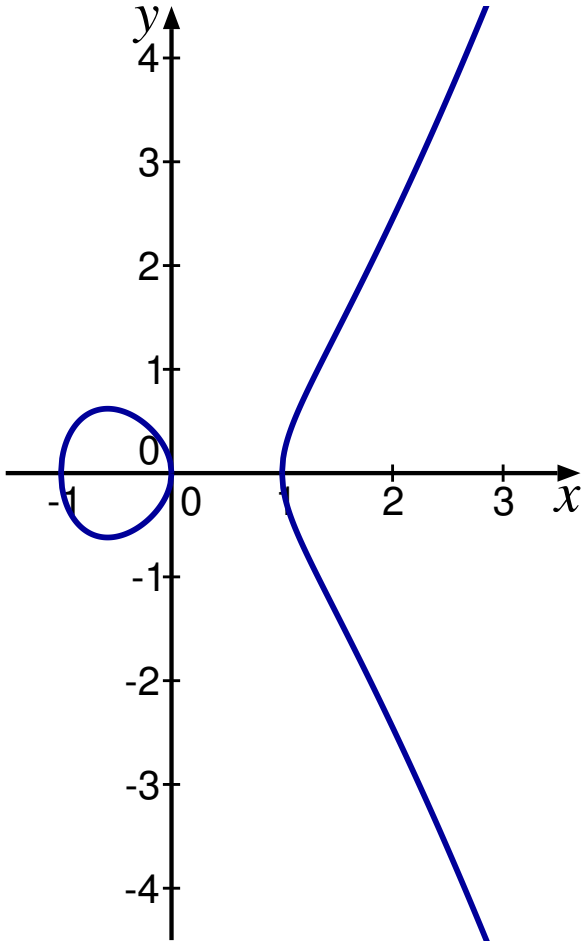
Ihre Punkte sind Paare (ξ, η) mit $\eta^2 = f(\xi)$ und ein „Punkt im Unendlichen“ O.

Rechts sieht man die reellen Punkte der elliptischen Kurve $y^2 = x^3 - x$.



$E\colon y^2 = x^3 - x$

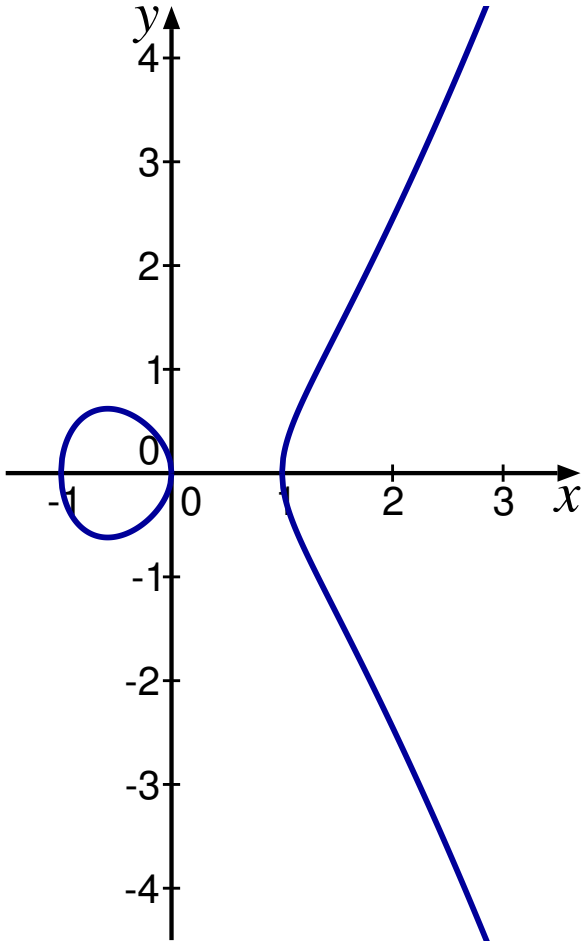
Elliptische Kurven: Gruppenstruktur



$E: y^2 = x^3 - x$

Elliptische Kurven: Gruppenstruktur

Die Punkte einer elliptischen Kurve
bilden eine abelsche Gruppe
mit dem Punkt O als Nullelement.

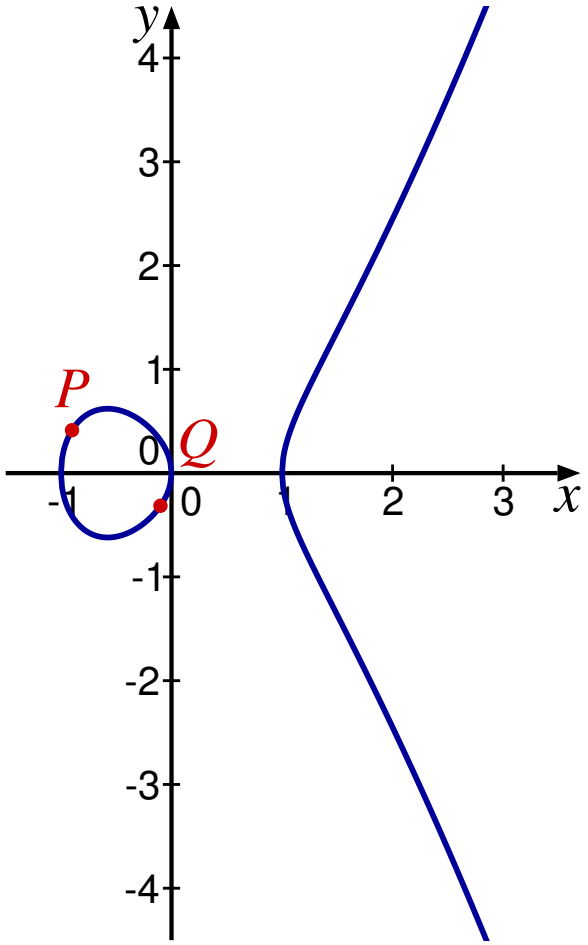


$E: y^2 = x^3 - x$

Elliptische Kurven: Gruppenstruktur

Die Punkte einer elliptischen Kurve bilden eine abelsche Gruppe mit dem Punkt O als Nullelement.

Die Summe zweier Punkte P und Q erhält man,

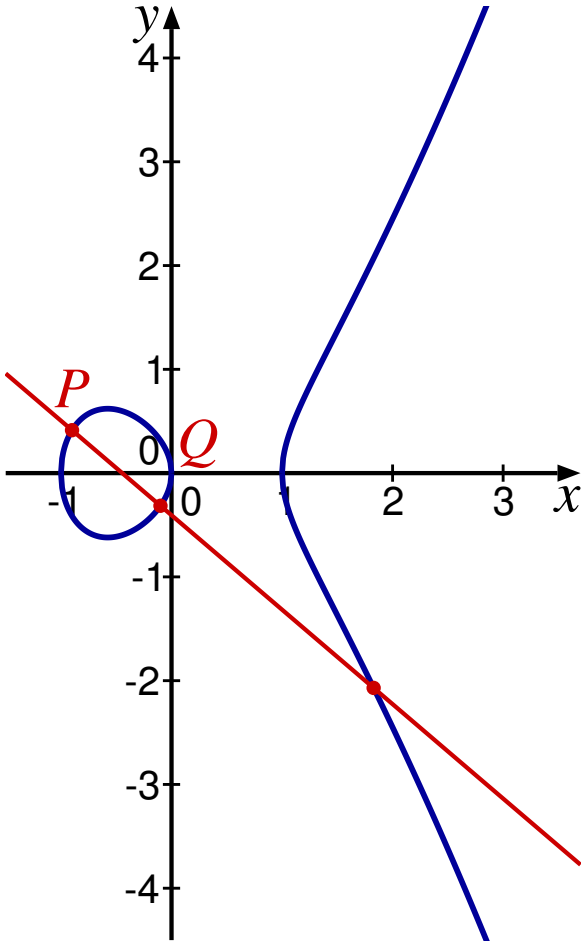


$E: y^2 = x^3 - x$

Elliptische Kurven: Gruppenstruktur

Die Punkte einer elliptischen Kurve
bilden eine abelsche Gruppe
mit dem Punkt O als Nullelement.

Die Summe zweier Punkte P und Q
erhält man,
indem man eine Gerade durch P und Q legt

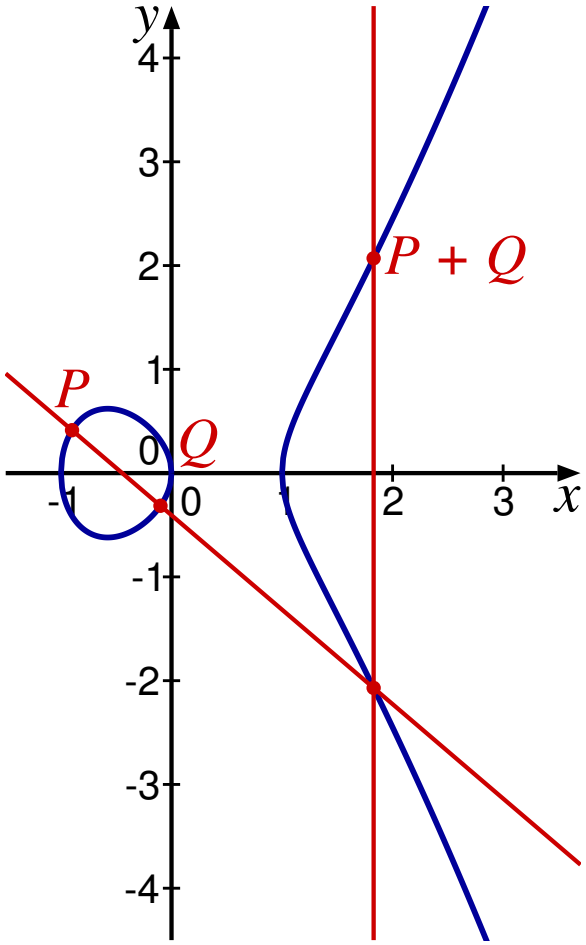


$E: y^2 = x^3 - x$

Elliptische Kurven: Gruppenstruktur

Die Punkte einer elliptischen Kurve
bilden eine abelsche Gruppe
mit dem Punkt O als Nullelement.

Die Summe zweier Punkte P und Q
erhält man,
indem man eine Gerade durch P und Q legt
und den dritten Schnittpunkt mit E
an der x-Achse spiegelt.



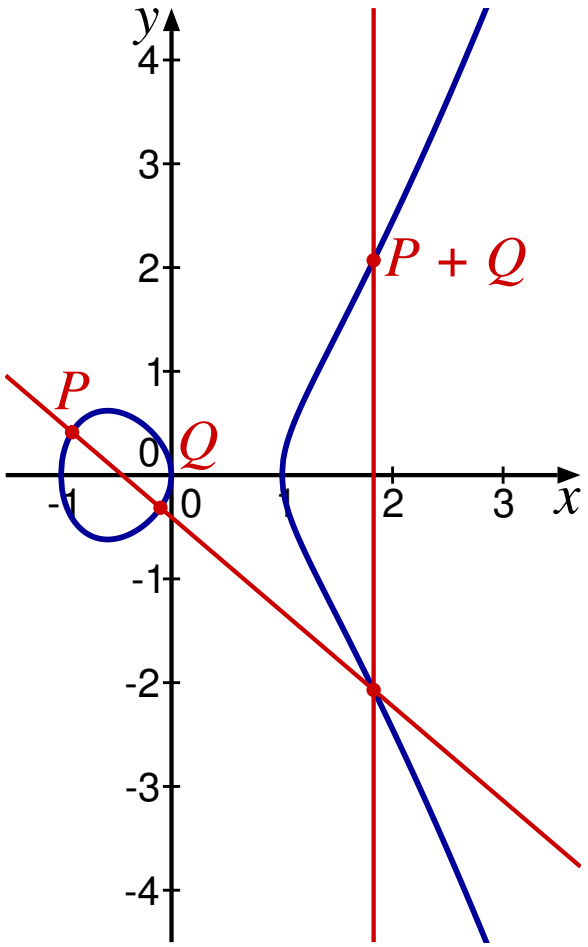
$E: y^2 = x^3 - x$

Elliptische Kurven: Gruppenstruktur

Die Punkte einer elliptischen Kurve
bilden eine abelsche Gruppe
mit dem Punkt O als Nullelement.

Die Summe zweier Punkte P und Q
erhält man,
indem man eine Gerade durch P und Q legt
und den dritten Schnittpunkt mit E
an der x-Achse spiegelt.

Die Punkte P mit $\ell \cdot P = O$
bilden eine Untergruppe $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.



$E: y^2 = x^3 - x$

Elliptische Kurven: Reduktion modulo $\mathfrak{p}$

Elliptische Kurven: Reduktion modulo p

Da die Koeffizienten von $f(x)$ ganze Zahlen sind,
kann man die Gleichung $y^2 = f(x)$ auch modulo p betrachten.
Dabei ist p eine Primzahl.
Wenn p die Diskriminante von f nicht teilt („gute Reduktion“),
dann erhält man eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_p$.

Elliptische Kurven: Reduktion modulo p

Da die Koeffizienten von $f(x)$ ganze Zahlen sind,
kann man die Gleichung $y^2 = f(x)$ auch modulo p betrachten.
Dabei ist p eine Primzahl.
Wenn p die Diskriminante von f nicht teilt („gute Reduktion“),
dann erhält man eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_p$.

Jede elliptische Kurve E hat zwei Invarianten,
die die „schlechte Reduktion“ messen:

- Die minimale Diskriminante Δ_E ($\approx \mathrm{disc}(f)$) und
- den Führer N_E.

Elliptische Kurven: Reduktion modulo p

Da die Koeffizienten von $f(x)$ ganze Zahlen sind,
kann man die Gleichung $y^2 = f(x)$ auch modulo p betrachten.
Dabei ist p eine Primzahl.
Wenn p die Diskriminante von f nicht teilt („gute Reduktion“),
dann erhält man eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_p$.

Jede elliptische Kurve E hat zwei Invarianten,
die die „schlechte Reduktion“ messen:

- Die minimale Diskriminante Δ_E ($\approx \operatorname{disc}(f)$) und
- den Führer N_E.

Für die Frey-Kurve $E_{a,b,c}$ gilt

$$\Delta_{E_{a,b,c}} = 2^{-8}(abc)^{2\ell} \quad \text{und} \quad N_{E_{a,b,c}} = \prod_{p \mid abc} p\,.$$

Elliptische Kurven: Modularität

Elliptische Kurven: Modularität

Unabhängig davon, ob E gute oder schlechte Reduktion bei p hat, können wir die $\mathbb{F}_p$-Punkte auf der reduzierten Kurve $E^{(p)}$ zählen.

Elliptische Kurven: Modularität

Unabhängig davon, ob E gute oder schlechte Reduktion bei p hat, können wir die $\mathbb{F}_p$-Punkte auf der reduzierten Kurve $E^{(p)}$ zählen.

Wir setzen $$a_p(E) = p + 1 - \#E^{(p)}(\mathbb{F}_p)\,.$$

(Hasse hat gezeigt, dass $|a_p| \leq 2\sqrt{p}$ ist.)

Elliptische Kurven: Modularität

Unabhängig davon, ob E gute oder schlechte Reduktion bei p hat, können wir die $\mathbb{F}_p$-Punkte auf der reduzierten Kurve $E^{(p)}$ zählen.

Wir setzen $$a_p(E) = p + 1 - \#E^{(p)}(\mathbb{F}_p)\,.$$

(Hasse hat gezeigt, dass $|a_p| \leq 2\sqrt{p}$ ist.)
Damit definiert man die L-Reihe von E als

$$L(E,s) = \prod_{p \text{ schlecht}} \frac{1}{1 - a_p p^{-s}} \prod_{p \text{ gut}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n \geq 1} \frac{a_n}{n^s}$$

Elliptische Kurven: Modularität

Unabhängig davon, ob E gute oder schlechte Reduktion bei p hat, können wir die $\mathbb{F}_p$-Punkte auf der reduzierten Kurve $E^{(p)}$ zählen.

Wir setzen $$a_p(E) = p + 1 - \#E^{(p)}(\mathbb{F}_p)\,.$$

(Hasse hat gezeigt, dass $|a_p| \leq 2\sqrt{p}$ ist.)
Damit definiert man die L-Reihe von E als

$$L(E,s) = \prod_{p \text{ schlecht}} \frac{1}{1 - a_p p^{-s}} \prod_{p \text{ gut}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n \geq 1} \frac{a_n}{n^s}$$

und eine holomorphe Funktion

$$f_E(z) = \sum_{n \geq 1} a_n q^n \qquad \text{mit } q = e^{2\pi i z}$$

auf der oberen Halbebene $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.

Elliptische Kurven: Modularität

Unabhängig davon, ob E gute oder schlechte Reduktion bei p hat, können wir die $\mathbb{F}_p$-Punkte auf der reduzierten Kurve $E^{(p)}$ zählen.

Wir setzen $$a_p(E) = p + 1 - \#E^{(p)}(\mathbb{F}_p)\,.$$

(Hasse hat gezeigt, dass $|a_p| \leq 2\sqrt{p}$ ist.)
Damit definiert man die L-Reihe von E als

$$L(E,s) = \prod_{p \text{ schlecht}} \frac{1}{1 - a_p p^{-s}} \prod_{p \text{ gut}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n \geq 1} \frac{a_n}{n^s}$$

und eine holomorphe Funktion

$$f_E(z) = \sum_{n \geq 1} a_n q^n \qquad \text{mit } q = e^{2\pi i z}$$

auf der oberen Halbebene $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.

E heißt modular, wenn f_E eine Modulform (vom Level N_E) ist.

Modulformen

Modulformen

Eine Modulform vom (Gewicht 2 und) Level N
ist eine holomorphe Funktion $f\colon \mathbb{H} \to \mathbb{C}$, so dass

$$\frac{1}{(cNz+d)^2} f\left(\frac{az+b}{cNz+d}\right) = f(z) \quad \text{für alle } a,b,c,d \in \mathbb{Z} \text{ mit } ad - bcN = 1\,.$$

Modulformen

Eine Modulform vom (Gewicht 2 und) Level N
ist eine holomorphe Funktion $f\colon \mathbb{H} \to \mathbb{C}$, so dass

$$\frac{1}{(cNz+d)^2} f\left(\frac{az+b}{cNz+d}\right) = f(z) \quad \text{für alle } a,b,c,d \in \mathbb{Z} \text{ mit } ad - bcN = 1.$$

Insbesondere ist $f(z+1) = f(z)$, also hat f eine Fourier-Entwicklung

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n \quad \text{mit } q = e^{2\pi i z}.$$

Für Modulformen verlangt man zusätzlich u.a. $a_n = 0$ für $n < 0$.

Modulformen

Eine Modulform vom (Gewicht 2 und) Level N
ist eine holomorphe Funktion $f\colon \mathbb{H} \to \mathbb{C}$, so dass

$$\frac{1}{(cNz+d)^2} f\left(\frac{az+b}{cNz+d}\right) = f(z) \quad \text{für alle } a,b,c,d \in \mathbb{Z} \text{ mit } ad - bcN = 1.$$

Insbesondere ist $f(z+1) = f(z)$, also hat f eine Fourier-Entwicklung

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n \quad \text{mit } q = e^{2\pi i z}.$$

Für Modulformen verlangt man zusätzlich u.a. $a_n = 0$ für $n < 0$.

Spitzenformen sind spezielle Modulformen, für die $a_0 = 0$ gilt.
Die Spitzenformen vom Level N
bilden einen endlich-dimensionalen $\mathbb{C}$-Vektorraum $S_2(N)$.

Modulformen

Eine Modulform vom (Gewicht 2 und) Level N
ist eine holomorphe Funktion $f\colon \mathbb{H} \to \mathbb{C}$, so dass

$$\frac{1}{(cNz+d)^2} f\left(\frac{az+b}{cNz+d}\right) = f(z) \quad \text{für alle } a,b,c,d \in \mathbb{Z} \text{ mit } ad - bcN = 1.$$

Insbesondere ist $f(z+1) = f(z)$, also hat f eine Fourier-Entwicklung

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n \quad \text{mit } q = e^{2\pi i z}.$$

Für Modulformen verlangt man zusätzlich u.a. $a_n = 0$ für $n < 0$.

Spitzenformen sind spezielle Modulformen, für die $a_0 = 0$ gilt.
Die Spitzenformen vom Level N
bilden einen endlich-dimensionalen $\mathbb{C}$-Vektorraum $S_2(N)$.
Wenn E modular ist, dann ist f_E eine Spitzenform.

Beweis der Fermatschen Vermutung

Beweis der Fermatschen Vermutung

Andrew Wiles (mit Hilfe von **Richard Taylor**) bewies 1994/95,
dass alle elliptischen Kurven mit quadratfreiem Führer modular sind.

Beweis der Fermatschen Vermutung

Andrew Wiles (mit Hilfe von **Richard Taylor**) bewies 1994/95,
dass alle elliptischen Kurven mit quadratfreiem Führer modular sind.
Insbesondere ist $E_{a,b,c}$ modular.

Beweis der Fermatschen Vermutung

Andrew Wiles (mit Hilfe von **Richard Taylor**) bewies 1994/95,
dass alle elliptischen Kurven mit quadratfreiem Führer modular sind.
Insbesondere ist $E_{a,b,c}$ modular.
(Inzwischen weiß man, dass alle elliptischen Kurven über $\mathbb{Q}$ modular sind.)

Beweis der Fermatschen Vermutung

Andrew Wiles (mit Hilfe von **Richard Taylor**) bewies 1994/95,
dass alle elliptischen Kurven mit quadratfreiem Führer modular sind.
Insbesondere ist $E_{a,b,c}$ modular.
(Inzwischen weiß man, dass alle elliptischen Kurven über $\mathbb{Q}$ modular sind.)

Ken Ribet hatte ~1986 eine Vermutung von **Jean-Pierre Serre** gezeigt,
die impliziert, dass es eine Spitzenform f vom Level 2 geben müsste,
deren Fourierkoeffizienten zu denen von $f_{E_{a,b,c}}$ mod ℓ kongruent sind.

Beweis der Fermatschen Vermutung

Andrew Wiles (mit Hilfe von **Richard Taylor**) bewies 1994/95,
dass alle elliptischen Kurven mit quadratfreiem Führer modular sind.
Insbesondere ist $E_{a,b,c}$ modular.
(Inzwischen weiß man, dass alle elliptischen Kurven über $\mathbb{Q}$ modular sind.)

Ken Ribet hatte ~1986 eine Vermutung von **Jean-Pierre Serre** gezeigt,
die impliziert, dass es eine Spitzenform f vom Level 2 geben müsste,
deren Fourierkoeffizienten zu denen von $f_{E_{a,b,c}}$ mod ℓ kongruent sind.
(Dafür braucht man $N_{E_{a,b,c}}$ quadratfrei und $\Delta_{E_{a,b,c}} = 2^e z^\ell$.
Das hat mit galoistheoretischen Eigenschaften von $E[\ell]$ zu tun.)

Beweis der Fermatschen Vermutung

Andrew Wiles (mit Hilfe von **Richard Taylor**) bewies 1994/95,
dass alle elliptischen Kurven mit quadratfreiem Führer modular sind.
Insbesondere ist $E_{a,b,c}$ modular.
(Inzwischen weiß man, dass alle elliptischen Kurven über $\mathbb{Q}$ modular sind.)

Ken Ribet hatte ~1986 eine Vermutung von **Jean-Pierre Serre** gezeigt,
die impliziert, dass es eine Spitzenform f vom Level 2 geben müsste,
deren Fourierkoeffizienten zu denen von $f_{E_{a,b,c}}$ mod ℓ kongruent sind.
(Dafür braucht man $N_{E_{a,b,c}}$ quadratfrei und $\Delta_{E_{a,b,c}} = 2^e z^\ell$.
Das hat mit galoistheoretischen Eigenschaften von $E[\ell]$ zu tun.)

Aber $S_2(2) = \{0\}$, Widerspruch!

Beweis der Fermatschen Vermutung

Andrew Wiles (mit Hilfe von **Richard Taylor**) bewies 1994/95,
dass alle elliptischen Kurven mit quadratfreiem Führer modular sind.
Insbesondere ist $E_{a,b,c}$ modular.
(Inzwischen weiß man, dass alle elliptischen Kurven über $\mathbb{Q}$ modular sind.)

Ken Ribet hatte ~1986 eine Vermutung von **Jean-Pierre Serre** gezeigt,
die impliziert, dass es eine Spitzenform f vom Level 2 geben müsste,
deren Fourierkoeffizienten zu denen von $f_{E_{a,b,c}}$ mod ℓ kongruent sind.
(Dafür braucht man $N_{E_{a,b,c}}$ quadratfrei und $\Delta_{E_{a,b,c}} = 2^e z^\ell$.
Das hat mit galoistheoretischen Eigenschaften von $E[\ell]$ zu tun.)

Aber $S_2(2) = \{0\}$, Widerspruch!

Die Frey-Kurve liefert die entscheidende Verknüpfung
zwischen der Fermatschen Gleichung und der Theorie der Modulformen.

Die verallgemeinerte Fermatsche Gleichung

Die verallgemeinerte Fermatsche Gleichung

Nachdem die Fermatsche Vermutung bewiesen ist,
kann man versuchen, sie zu verallgemeinern:
Man betrachtet die verallgemeinerte Fermatsche Gleichung

$$a^p + b^q = c^r$$

mit $p, q, r \geq 2$ und $a, b, c \in \mathbb{Z}$ teilerfremd.

Die verallgemeinerte Fermatsche Gleichung

Nachdem die Fermatsche Vermutung bewiesen ist,
kann man versuchen, sie zu verallgemeinern:
Man betrachtet die verallgemeinerte Fermatsche Gleichung

$$a^p + b^q = c^r$$

mit $p, q, r \geq 2$ und $a, b, c \in \mathbb{Z}$ teilerfremd.

Ein wesentlicher Parameter ist die „Euler-Charakteristik“

$$\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1, \qquad -1 < \chi \leq \tfrac{1}{2}.$$

Die verallgemeinerte Fermatsche Gleichung

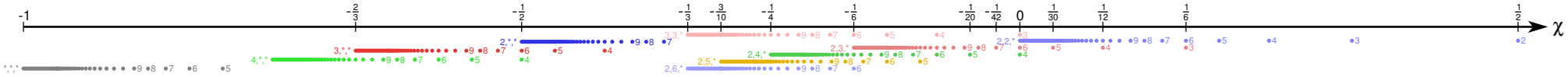
Nachdem die Fermatsche Vermutung bewiesen ist,
kann man versuchen, sie zu verallgemeinern:
Man betrachtet die verallgemeinerte Fermatsche Gleichung

$$a^p + b^q = c^r$$

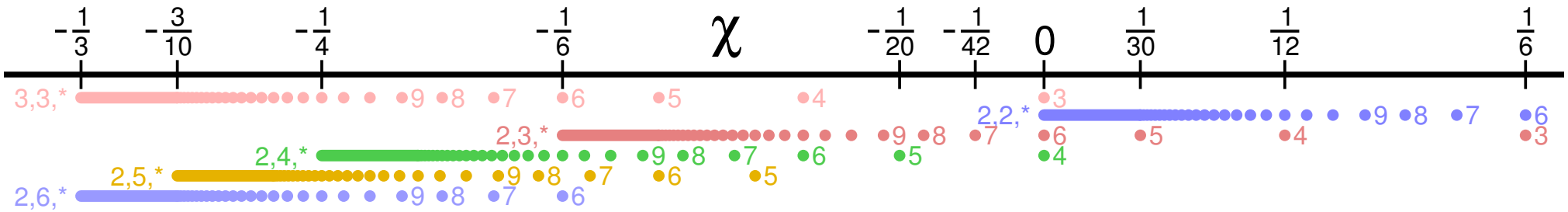
mit $p, q, r \geq 2$ und $a, b, c \in \mathbb{Z}$ teilerfremd.

Ein wesentlicher Parameter ist die „Euler-Charakteristik“

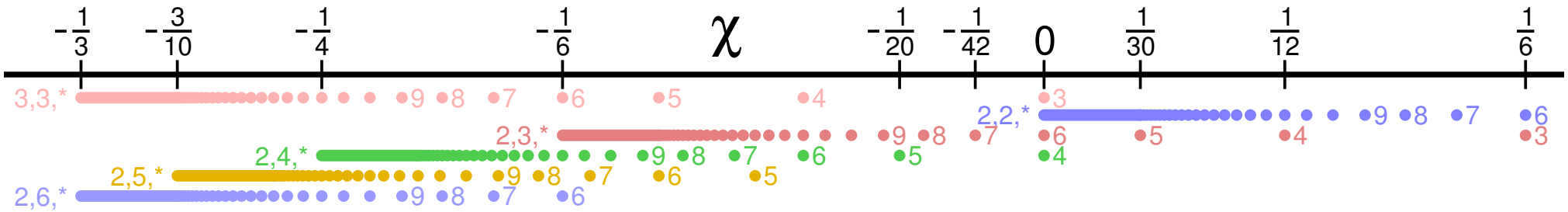
$$\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1, \qquad -1 < \chi \leq \frac{1}{2}.$$



Die drei Fälle

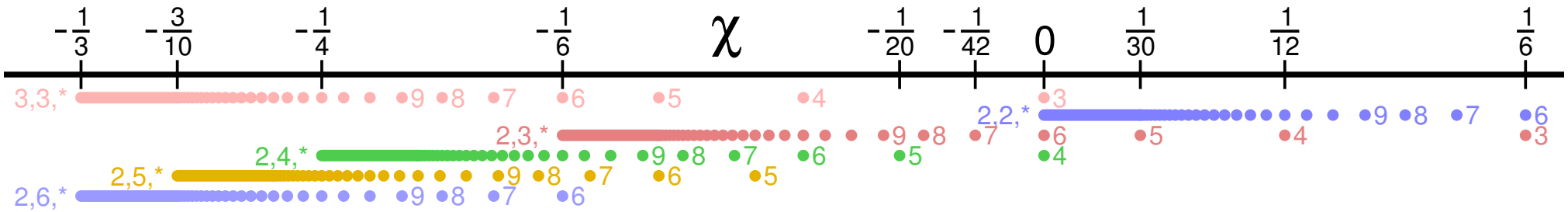


Die drei Fälle



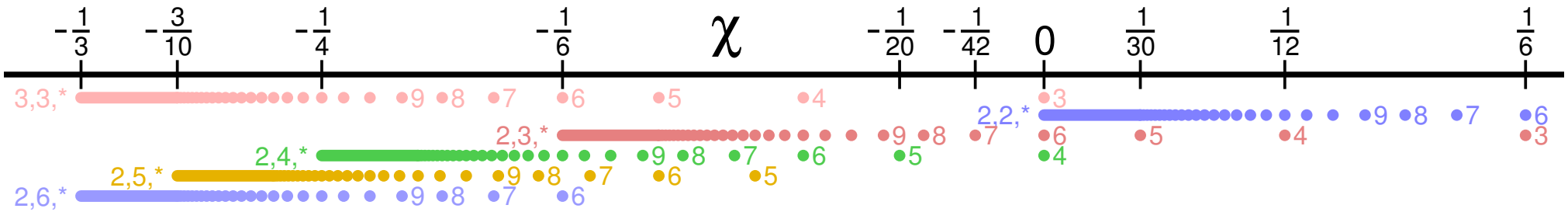
- $\chi > 0$: $(2,2,n)$, $(2,3,3)$, $(2,3,4)$, $(2,3,5)$ und Permutationen
  $\Rightarrow$ unendlich viele Lösungen; endlich viele parametrisierte Familien
  (Beukers 1998; explizite Lösungen: Mordell, Zagier, Edwards).

Die drei Fälle



- $\chi > 0$: $(2,2,n)$, $(2,3,3)$, $(2,3,4)$, $(2,3,5)$ und Permutationen
  $\Rightarrow$ unendlich viele Lösungen; endlich viele parametrisierte Familien
  (Beukers 1998; explizite Lösungen: Mordell, Zagier, Edwards).
- $\chi = 0$: $(2,4,4)$, $(2,3,6)$, $(3,3,3)$ und Permutationen
  $\Rightarrow$ nur triviale Lösungen und $1^6 + 2^3 = 3^2$
  (Fermat, Euler).

Die drei Fälle



- $\chi > 0$: $(2,2,n)$, $(2,3,3)$, $(2,3,4)$, $(2,3,5)$ und Permutationen
  $\Rightarrow$ unendlich viele Lösungen; endlich viele parametrisierte Familien
  (Beukers 1998; explizite Lösungen: Mordell, Zagier, Edwards).
- $\chi = 0$: $(2,4,4)$, $(2,3,6)$, $(3,3,3)$ und Permutationen
  $\Rightarrow$ nur triviale Lösungen und $1^6 + 2^3 = 3^2$
  (Fermat, Euler).
- $\chi < 0$: Der ganze Rest
  $\Rightarrow$ endlich viele Lösungen
  (Darmon und Granville 1995).

Bekannte Lösungen für $\chi < 0$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2,$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4,$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9,$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2,$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3,$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7,$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2,$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel
sind die mit χ am nächsten bei 0.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$,
sind die mit χ ($-1/42$,) am nächsten bei 0.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$,
sind die mit χ ($-1/42$, $-1/24$,) am nächsten bei 0.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$, $(2,4,5)$
sind die mit χ ($-1/42$, $-1/24$, $-1/20$) am nächsten bei 0.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$, $(2,4,5)$ und $(2,3,9)$
sind die mit χ ($-1/42$, $-1/24$, $-1/20$ und $-1/18$) am nächsten bei 0.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$, $(2,4,5)$ und $(2,3,9)$
sind die mit χ ($-1/42$, $-1/24$, $-1/20$ und $-1/18$) am nächsten bei 0.
Die Anzahl der Lösungen verhält sich entsprechend.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$, $(2,4,5)$ und $(2,3,9)$
sind die mit χ ($-1/42$, $-1/24$, $-1/20$ und $-1/18$) am nächsten bei 0.
Die Anzahl der Lösungen (5,) verhält sich entsprechend.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$, $(2,4,5)$ und $(2,3,9)$
sind die mit χ ($-1/42$, $-1/24$, $-1/20$ und $-1/18$) am nächsten bei 0.
Die Anzahl der Lösungen (5, 3,) verhält sich entsprechend.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$, $(2,4,5)$ und $(2,3,9)$
sind die mit χ ($-1/42$, $-1/24$, $-1/20$ und $-1/18$) am nächsten bei 0.
Die Anzahl der Lösungen (5, 3, 2) verhält sich entsprechend.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$, $(2,4,5)$ und $(2,3,9)$
sind die mit χ ($-1/42$, $-1/24$, $-1/20$ und $-1/18$) am nächsten bei 0.
Die Anzahl der Lösungen (5, 3, 2 und 2) verhält sich entsprechend.

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$, $(2,4,5)$ und $(2,3,9)$
sind die mit χ ($-1/42$, $-1/24$, $-1/20$ und $-1/18$) am nächsten bei 0.
Die Anzahl der Lösungen (5, 3, 2 und 2) verhält sich entsprechend.

Man weiß, dass es für diese Tripel keine weiteren Lösungen gibt.
(Bruin für $(2,3,8)$, $(2,4,5)$, $(2,3,9)$; Poonen-Schaefer-Stoll für $(2,3,7)$)

Bekannte Lösungen für $\chi < 0$

Für $\chi < 0$ kennt man folgende zehn Lösungen
(bis auf Permutation und Vorzeichen):

$$1^n + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2.$$

Die vorkommenden Exponententripel $(2,3,7)$, $(2,3,8)$, $(2,4,5)$ und $(2,3,9)$
sind die mit χ ($-1/42$, $-1/24$, $-1/20$ und $-1/18$) am nächsten bei 0.
Die Anzahl der Lösungen (5, 3, 2 und 2) verhält sich entsprechend.

Man weiß, dass es für diese Tripel keine weiteren Lösungen gibt.
(Bruin für $(2,3,8)$, $(2,4,5)$, $(2,3,9)$; Poonen-Schaefer-Stoll für $(2,3,7)$)

Für viele weitere Tripel wurde gezeigt,
dass es keine nichttrivialen Lösungen gibt (außer evtl. $1^n + 2^3 = 3^2$).

Frey-Kurven für $(2, 3, \ell)$

Frey-Kurven für $(2, 3, \ell)$

Sei $\ell \geq 7$ eine Primzahl.
Einer nichttrivialen Lösung $(a, b, c) \in \mathbb{Z}^3$ mit a, b, c teilerfremd von

$$a^2 + b^3 = c^\ell$$

ordnen wir die Frey-Kurve

$$E_{a,b,c} \colon y^2 = x^3 + 3bx - 2a$$

zu.

Frey-Kurven für $(2,3,\ell)$

Sei $\ell \geq 7$ eine Primzahl.
Einer nichttrivialen Lösung $(a,b,c) \in \mathbb{Z}^3$ mit a,b,c teilerfremd von

$$a^2 + b^3 = c^\ell$$

ordnen wir die Frey-Kurve

$$E_{a,b,c} \colon y^2 = x^3 + 3bx - 2a$$

zu. Diese Kurve hat Invarianten

$$\Delta_{E_{a,b,c}} = 2^r 3^s c^\ell \quad \text{und} \quad N_{E_{a,b,c}} = 2^{r'} 3^{s'} \prod_{5 \leq p \mid c} p\,.$$

Frey-Kurven für $(2,3,\ell)$

Sei $\ell \geq 7$ eine Primzahl.
Einer nichttrivialen Lösung $(a,b,c) \in \mathbb{Z}^3$ mit a,b,c teilerfremd von

$$a^2 + b^3 = c^\ell$$

ordnen wir die Frey-Kurve

$$E_{a,b,c} \colon y^2 = x^3 + 3bx - 2a$$

zu. Diese Kurve hat Invarianten

$$\Delta_{E_{a,b,c}} = 2^r 3^s c^\ell \quad \text{und} \quad N_{E_{a,b,c}} = 2^{r'} 3^{s'} \prod_{5 \leq p \mid c} p\,.$$

Modularität und der Satz von Ribet liefern:

$$E_{a,b,c}[\ell] \cong E[\ell] \quad \text{als Galois-Moduln, „bis auf quadratischen Twist“}$$

für eine elliptische Kurve E aus einer Liste von 13 Kurven
(plus Sonderfälle für $\ell = 7$ oder 13).

Getwistete Modulkurven

Getwistete Modulkurven

Für eine feste elliptische Kurve E und gegebene Primzahl ℓ
entsprechen die elliptischen Kurven E' mit $E'[\ell] \cong E[\ell]$
rationalen Punkten auf einem Paar von Kurven $X_E^+(\ell)$ und $X_E^-(\ell)$.

Getwistete Modulkurven

Für eine feste elliptische Kurve E und gegebene Primzahl ℓ
entsprechen die elliptischen Kurven E' mit $E'[\ell] \cong E[\ell]$
rationalen Punkten auf einem Paar von Kurven $X_E^+(\ell)$ und $X_E^-(\ell)$.

Im Fall $\ell = 7$ kann man diese Kurven explizit hinschreiben, z.B.:

$$X_{96a1}^+(7)\colon\ -2x^3y - 2x^3z + 6x^2yz + 3xy^3 - 9xy^2z + 3xyz^2 - xz^3 + 3y^3z - yz^3 = 0$$

als Gleichung in der projektiven Ebene.

Getwistete Modulkurven

Für eine feste elliptische Kurve E und gegebene Primzahl ℓ
entsprechen die elliptischen Kurven E' mit $E'[\ell] \cong E[\ell]$
rationalen Punkten auf einem Paar von Kurven $X_E^+(\ell)$ und $X_E^-(\ell)$.

Im Fall $\ell = 7$ kann man diese Kurven explizit hinschreiben, z.B.:

$$X_{96a1}^+(7)\colon\ -2x^3y - 2x^3z + 6x^2yz + 3xy^3 - 9xy^2z + 3xyz^2 - xz^3 + 3y^3z - yz^3 = 0$$

als Gleichung in der projektiven Ebene.

Bjorn Poonen, Ed Schaefer und mir ist es gelungen,
die (relevanten) rationalen Punkte auf all diesen Kurven
(einschließlich der „Sonderfälle“) zu finden.

Getwistete Modulkurven

Für eine feste elliptische Kurve E und gegebene Primzahl ℓ
entsprechen die elliptischen Kurven E' mit $E'[\ell] \cong E[\ell]$
rationalen Punkten auf einem Paar von Kurven $X_E^+(\ell)$ und $X_E^-(\ell)$.

Im Fall $\ell = 7$ kann man diese Kurven explizit hinschreiben, z.B.:

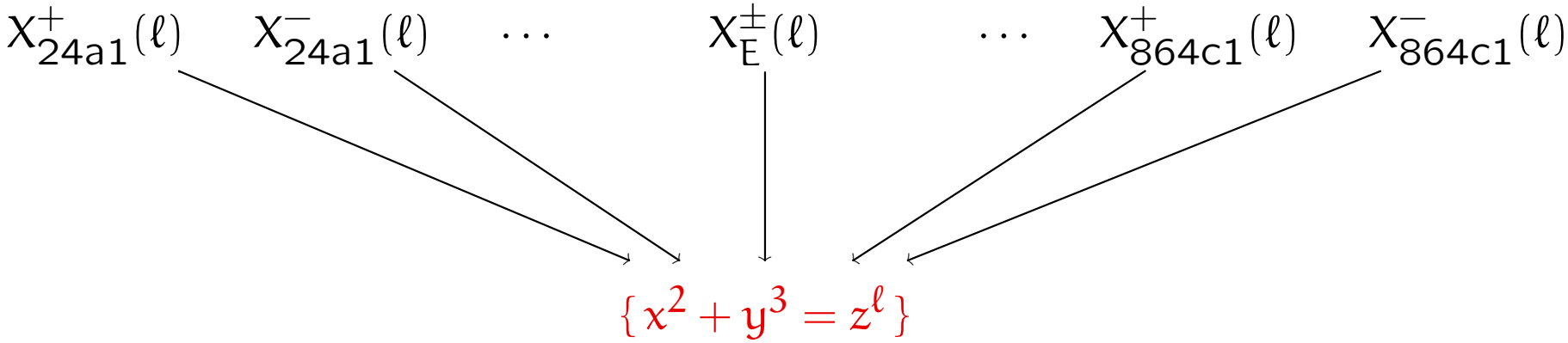
$$X_{96a1}^+(7)\colon\ -2x^3y - 2x^3z + 6x^2yz + 3xy^3 - 9xy^2z + 3xyz^2 - xz^3 + 3y^3z - yz^3 = 0$$

als Gleichung in der projektiven Ebene.

Bjorn Poonen, Ed Schaefer und mir ist es gelungen,
die (relevanten) rationalen Punkte auf all diesen Kurven
(einschließlich der „Sonderfälle“) zu finden.

Dadurch konnten wir zeigen,
dass es für $(2, 3, 7)$ keine weiteren Lösungen gibt.

Vielen Dank für Ihre Aufmerksamkeit!



$E \in \{24a1,\ 27a1,\ 32a1,\ 36a1,\ 54a1,\ 96a1,\ 108a1,$
$216a1,\ 216b1,\ 288a1,\ 864a1,\ 864b1,\ 864c1\}.$