Die Vermutung von Birch und Swinnerton-Dyer

Michael Stoll

Universität Bayreuth

Bayreuth
8. Januar 2009

UNIVERSITÄT BAYREUTH

Die Vermutung von Birch und Swinnerton-Dyer

Swinnerton-Dyer

©MFO

Michael Stoll

Universität Bayreuth

Bayreuth
8. Januar 2009

Birch

©W.A. Stein

Elliptische Kurven

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Die Bogenlänge einer Ellipse wird durch ein elliptisches Integral gemessen, das in natürlicher Weise auf einer elliptischen Kurve lebt.

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Die Bogenlänge einer Ellipse wird durch ein elliptisches Integral gemessen, das in natürlicher Weise auf einer elliptischen Kurve lebt.

Elliptische Kurven kommen vielfach in der Mathematik vor:

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Die Bogenlänge einer Ellipse wird durch ein elliptisches Integral gemessen, das in natürlicher Weise auf einer elliptischen Kurve lebt.

Elliptische Kurven kommen vielfach in der Mathematik vor:

- Algebraische Geometrie

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Die Bogenlänge einer Ellipse wird durch ein elliptisches Integral gemessen, das in natürlicher Weise auf einer elliptischen Kurve lebt.

Elliptische Kurven kommen vielfach in der Mathematik vor:

- Algebraische Geometrie
- Funktionentheorie (Riemannsche Flächen, Modulformen)

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Die Bogenlänge einer Ellipse wird durch ein elliptisches Integral gemessen, das in natürlicher Weise auf einer elliptischen Kurve lebt.

Elliptische Kurven kommen vielfach in der Mathematik vor:

- Algebraische Geometrie
- Funktionentheorie (Riemannsche Flächen, Modulformen)
- Diophantische Gleichungen (z.B. Beweis der Fermatschen Vermutung)

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Die Bogenlänge einer Ellipse wird durch ein elliptisches Integral gemessen, das in natürlicher Weise auf einer elliptischen Kurve lebt.

Elliptische Kurven kommen vielfach in der Mathematik vor:

- Algebraische Geometrie
- Funktionentheorie (Riemannsche Flächen, Modulformen)
- Diophantische Gleichungen (z.B. Beweis der Fermatschen Vermutung)
- Analytische Zahlentheorie (L-Reihen, B-SD-Vermutung)

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Die Bogenlänge einer Ellipse wird durch ein elliptisches Integral gemessen, das in natürlicher Weise auf einer elliptischen Kurve lebt.

Elliptische Kurven kommen vielfach in der Mathematik vor:

- Algebraische Geometrie
- Funktionentheorie (Riemannsche Flächen, Modulformen)
- Diophantische Gleichungen (z.B. Beweis der Fermatschen Vermutung)
- Analytische Zahlentheorie (L-Reihen, B-SD-Vermutung)
- Kryptographie

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Die Bogenlänge einer Ellipse wird durch ein elliptisches Integral gemessen, das in natürlicher Weise auf einer elliptischen Kurve lebt.

Elliptische Kurven kommen vielfach in der Mathematik vor:

- Algebraische Geometrie
- Funktionentheorie (Riemannsche Flächen, Modulformen)
- Diophantische Gleichungen (z.B. Beweis der Fermatschen Vermutung)
- Analytische Zahlentheorie (L-Reihen, B-SD-Vermutung)
- Kryptographie
- Algorithmische Zahlentheorie (Primzahltest, Faktorisierung)

Elliptische Kurven

Elliptische Kurven sind keine Ellipsen!

Die Bogenlänge einer Ellipse wird durch ein elliptisches Integral gemessen, das in natürlicher Weise auf einer elliptischen Kurve lebt.

Elliptische Kurven kommen vielfach in der Mathematik vor:

- Algebraische Geometrie
- Funktionentheorie (Riemannsche Flächen, Modulformen)
- Diophantische Gleichungen (z.B. Beweis der Fermatschen Vermutung)
- Analytische Zahlentheorie (L-Reihen, B-SD-Vermutung)
- Kryptographie
- Algorithmische Zahlentheorie (Primzahltest, Faktorisierung)

(Vorlesung im SoSe 2009 für die, die es genauer wissen wollen!)

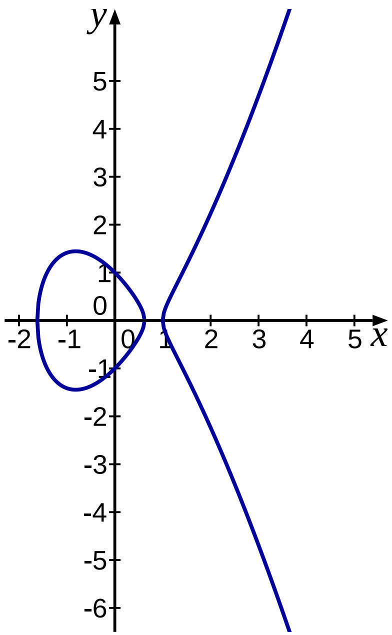
Elliptische Kurven

Elliptische Kurven

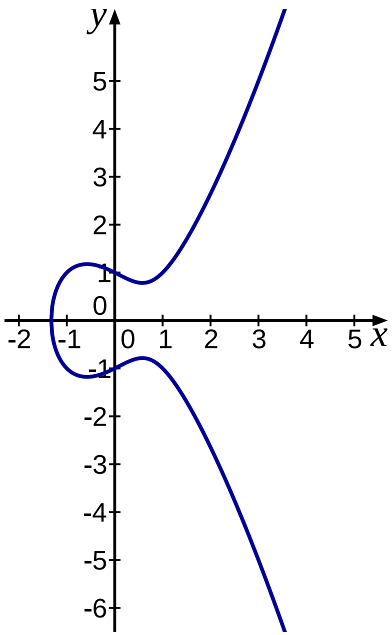
Eine Elliptische Kurve ist gegeben durch eine Gleichung

$$y^2 = x^3 + Ax + B$$

wobei A und B ganze Zahlen sind .



$E_0 : y^2 = x^3 - 2x + 1$



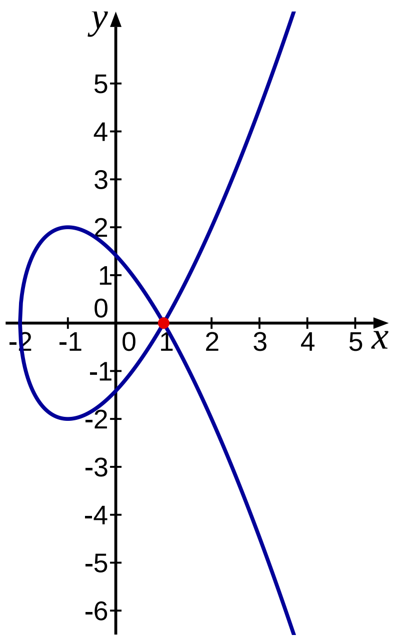
$E_1 : y^2 = x^3 - x + 1$

Elliptische Kurven

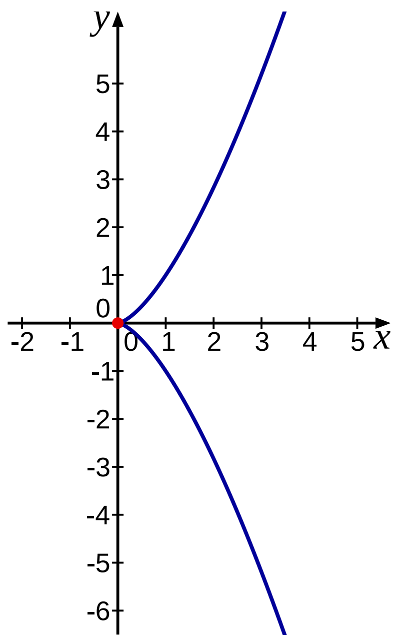
Eine Elliptische Kurve ist gegeben durch eine Gleichung

$$y^2 = x^3 + Ax + B$$

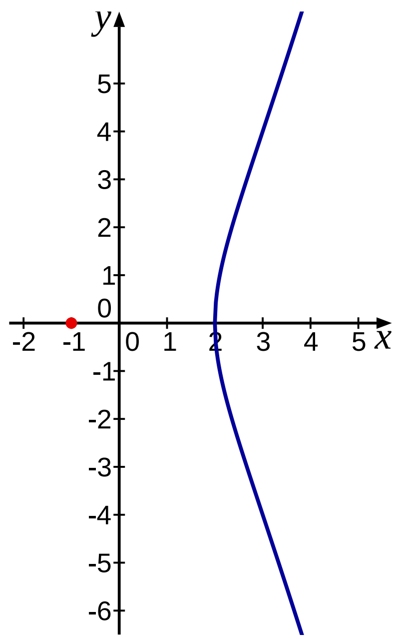
wobei A und B ganze Zahlen sind (mit $4A^3 + 27B^2 \neq 0$).



$y^2 = x^3 - 3x + 2$



$y^2 = x^3$



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

Elliptische Kurven

Eine Elliptische Kurve ist gegeben durch eine Gleichung

$$y^2 = x^3 + Ax + B$$

wobei A und B ganze Zahlen sind (mit $4A^3 + 27B^2 \neq 0$).

Wir interessieren uns für die rationalen Punkte der Kurve:
Paare (x, y) von rationalen Zahlen, die die Gleichung erfüllen.

Elliptische Kurven

Eine Elliptische Kurve ist gegeben durch eine Gleichung

$$y^2 = x^3 + Ax + B$$

wobei A und B ganze Zahlen sind (mit $4A^3 + 27B^2 \neq 0$).

Wir interessieren uns für die rationalen Punkte der Kurve:
Paare (x, y) von rationalen Zahlen, die die Gleichung erfüllen.

Es kann dabei entweder endlich viele (z.B. gar keine)
oder unendlich viele rationale Punkte geben.

Elliptische Kurven

Eine Elliptische Kurve ist gegeben durch eine Gleichung

$$y^2 = x^3 + Ax + B$$

wobei A und B ganze Zahlen sind (mit $4A^3 + 27B^2 \neq 0$).

Wir interessieren uns für die rationalen Punkte der Kurve:
Paare (x, y) von rationalen Zahlen, die die Gleichung erfüllen.

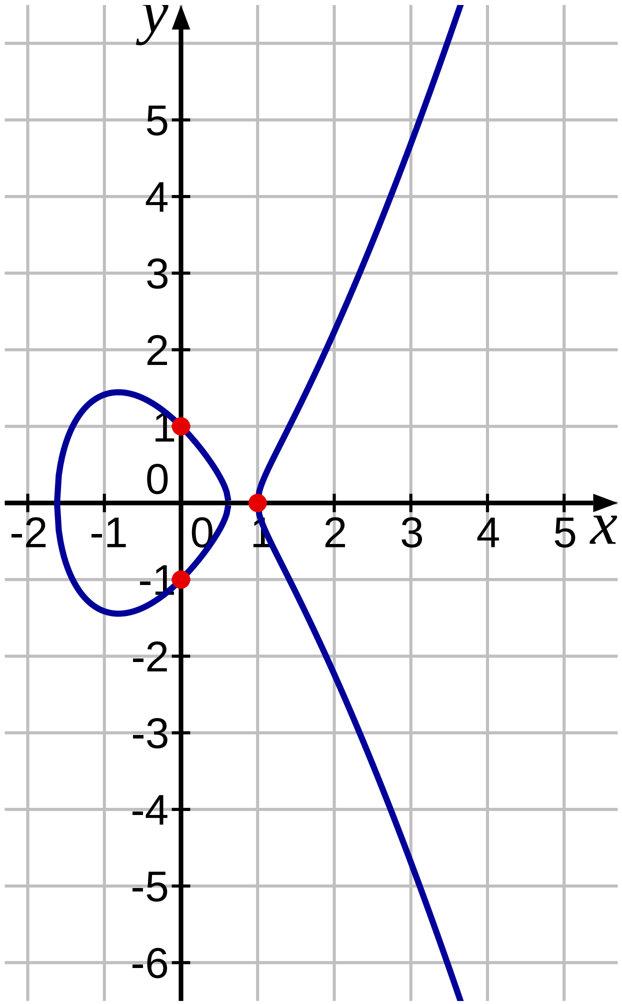
Es kann dabei entweder endlich viele (z.B. gar keine)
oder unendlich viele rationale Punkte geben.

Beispiele (siehe nächste Folie):

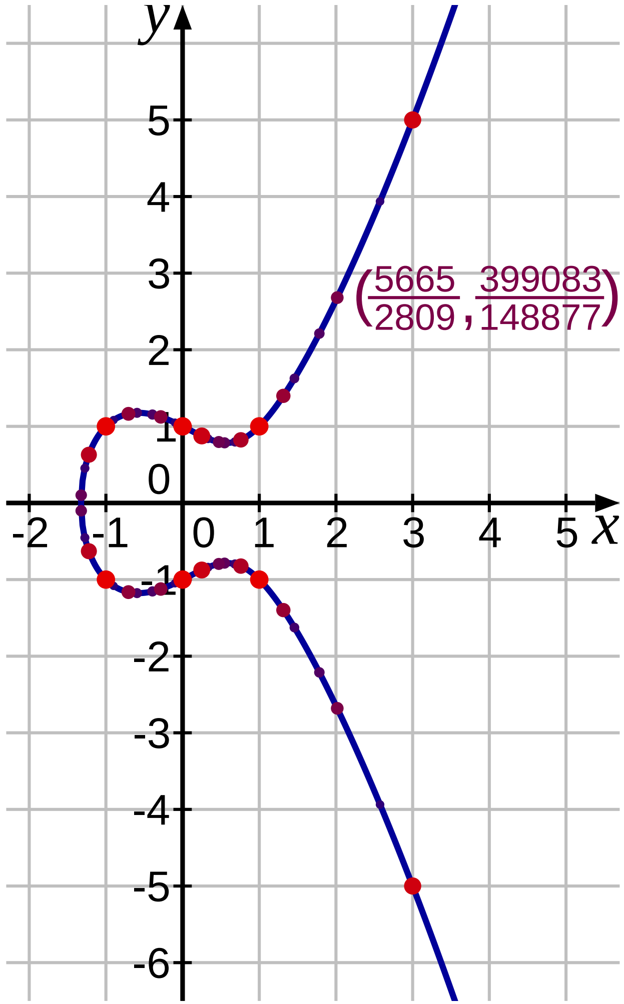
$E_0 : y^2 = x^3 - 2x + 1$ hat genau drei rationale Punkte;

$E_1 : y^2 = x^3 - x + 1$ hat unendlich viele rationale Punkte.

Zwei Beispiele



$$E_0 : y^2 = x^3 - 2x + 1$$



$$E_1 : y^2 = x^3 - x + 1$$

Noch ein Beispiel

Noch ein Beispiel

Der einfachste rationale Punkt auf der Kurve

$$y^2 = x^3 + 7823$$

ist gegeben durch

Noch ein Beispiel

Der einfachste rationale Punkt auf der Kurve

$$y^2 = x^3 + 7823$$

ist gegeben durch

$$x = \frac{2263582143321421502100209233517777}{119816734100955612^2}$$

$$y = \frac{186398152584623305624837551485596770028144776655756}{119816734100955613^3}$$

(MS, 2002).

Noch ein Beispiel

Der einfachste rationale Punkt auf der Kurve

$$y^2 = x^3 + 7823$$

ist gegeben durch

$$x = \frac{2263582143321421502100209233517777}{119816734100955612^2}$$

$$y = \frac{186398152584623305624837551485596770028144776655756}{119816734100955612^3}$$

(MS, 2002).

Das Auffinden von rationalen Punkten kann sehr schwierig sein!

Noch ein Beispiel

Der einfachste rationale Punkt auf der Kurve

$$y^2 = x^3 + 7823$$

ist gegeben durch

$$x = \frac{2263582143321421502100209233517777}{11981673410095561^2}$$

$$y = \frac{186398152584623305624837551485596770028144776655756}{11981673410095561^3}$$

(MS, 2002).

Das Auffinden von rationalen Punkten kann sehr schwierig sein!

Die Kurve hat noch unendlich viele weitere rationale Punkte.

Gruppenstruktur

Gruppenstruktur

Wie kann man diese ganzen Punkte finden?

Gruppenstruktur

Wie kann man diese ganzen Punkte finden?

Eine Gerade trifft die elliptische Kurve in drei Punkten
(mit Vielfachheit: ein Berührpunkt zählt doppelt).

Gruppenstruktur

Wie kann man diese ganzen Punkte finden?

Eine Gerade trifft die elliptische Kurve in drei Punkten
(mit Vielfachheit: ein Berührpunkt zählt doppelt).

Wenn zwei davon rationale Punkte sind, dann auch der dritte.

Gruppenstruktur

Wie kann man diese ganzen Punkte finden?

Eine Gerade trifft die elliptische Kurve in drei Punkten
(mit Vielfachheit: ein Berührpunkt zählt doppelt).

Wenn zwei davon rationale Punkte sind, dann auch der dritte.

Damit das richtig funktioniert,
muss man einen zusätzlichen „Punkt im Unendlichen“ O hinzufügen,
der auf jeder senkrechten Geraden liegt
und ein rationaler Punkt der elliptischen Kurve ist.

Gruppenstruktur

Wie kann man diese ganzen Punkte finden?

Eine Gerade trifft die elliptische Kurve in drei Punkten
(mit Vielfachheit: ein Berührpunkt zählt doppelt).

Wenn zwei davon rationale Punkte sind, dann auch der dritte.

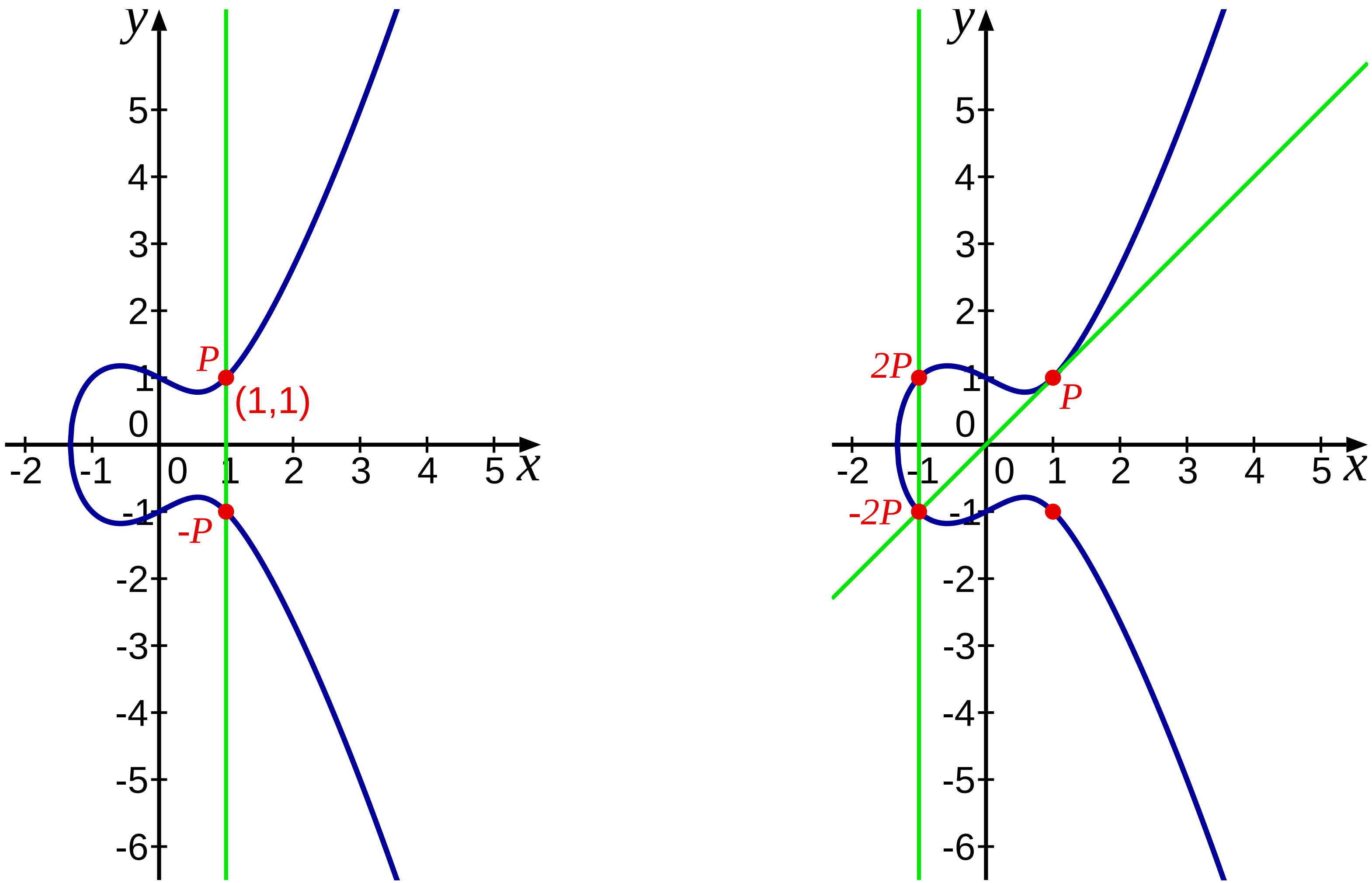
Damit das richtig funktioniert,
muss man einen zusätzlichen „Punkt im Unendlichen“ O hinzufügen,
der auf jeder senkrechten Geraden liegt
und ein rationaler Punkt der elliptischen Kurve ist.

Durch die Festsetzung

$$P + Q + R = O \iff P, Q, R \text{ sind die Schnittpunkte einer Geraden mit } E$$

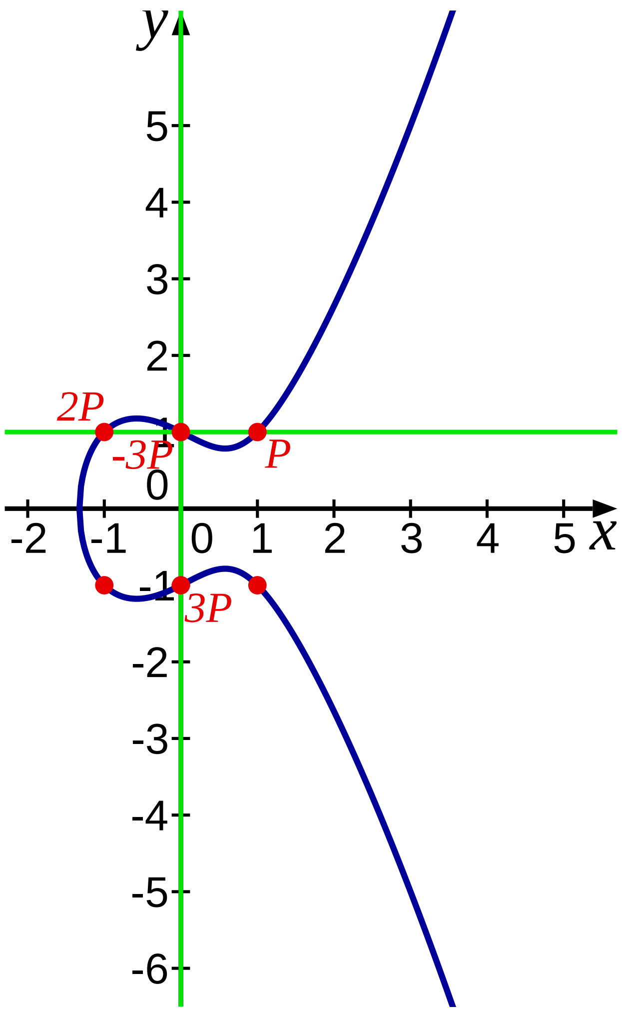
wird die Menge $E(\mathbb{Q})$ der rationalen Punkte eine Gruppe
mit O als neutralem Element.

Addition auf E_1

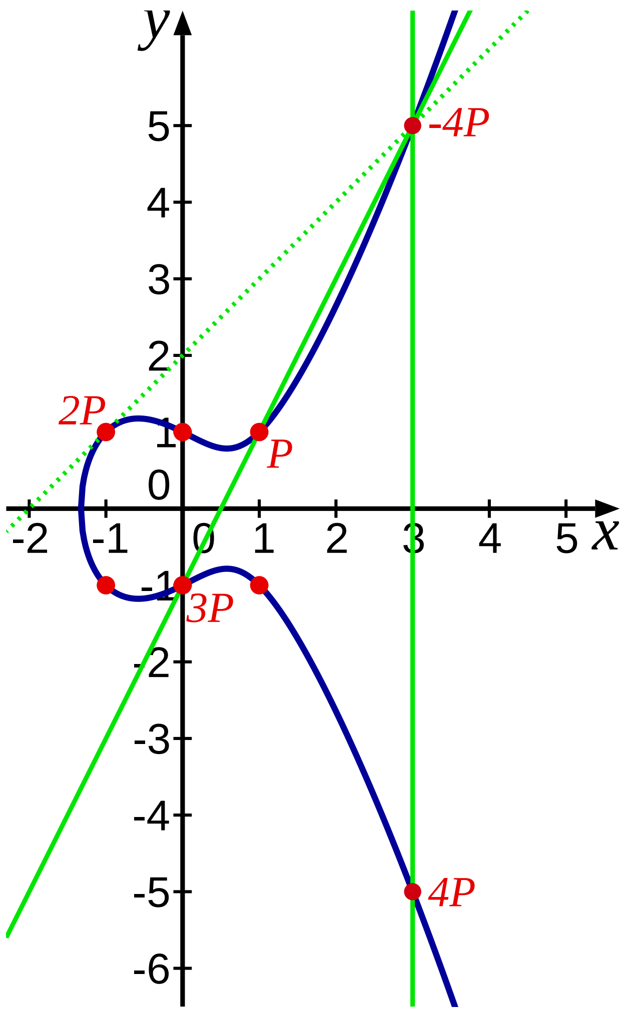


$$-P = (1, -1) \qquad 2 \cdot P = (-1, 1)$$

Addition auf E_1

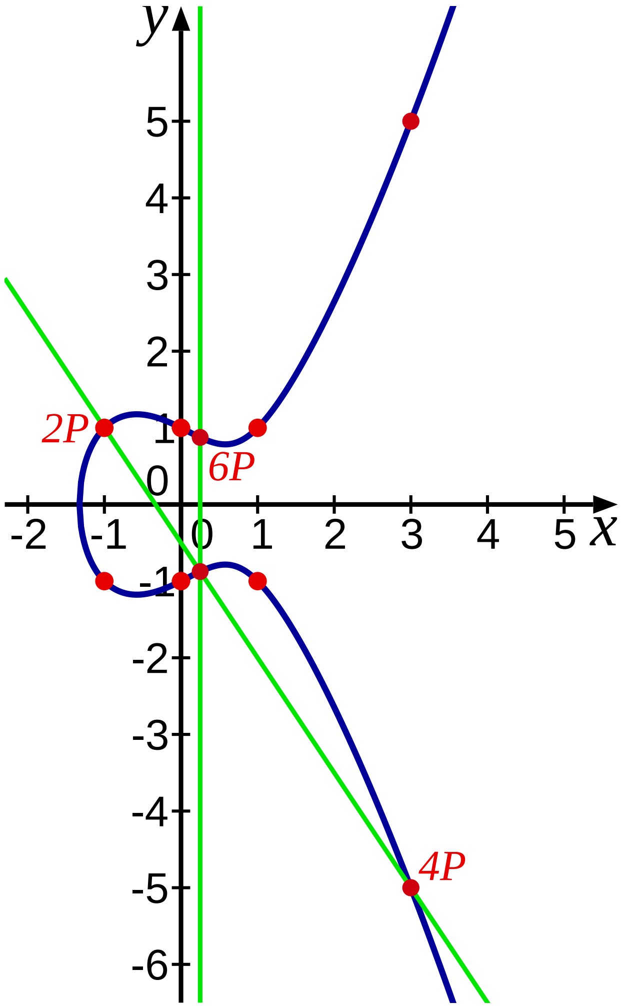


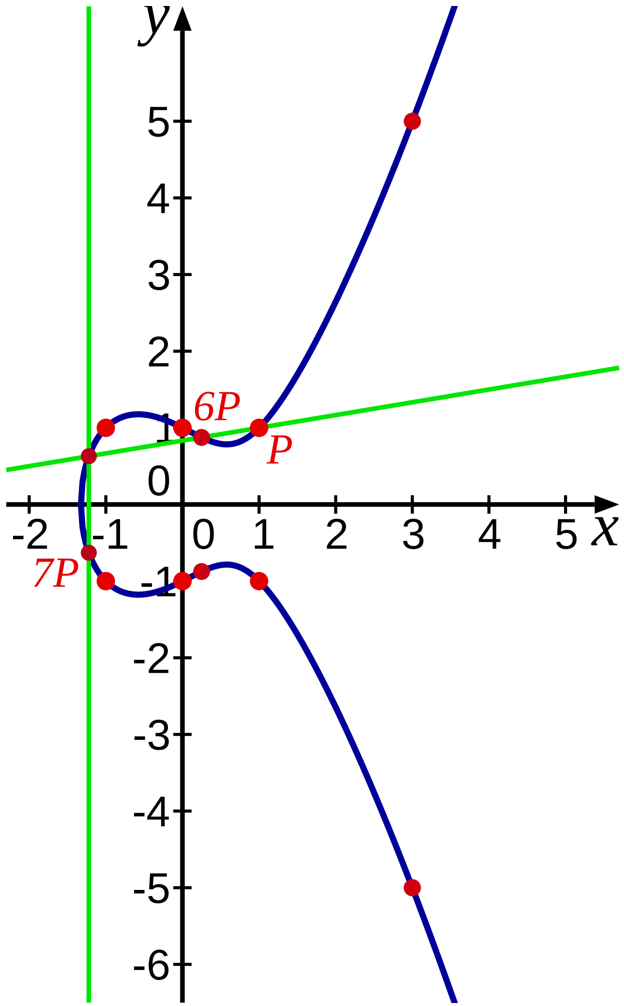
$$3 \cdot P = (0, -1)$$



$$4 \cdot P = (3, -5)$$

Addition auf E_1

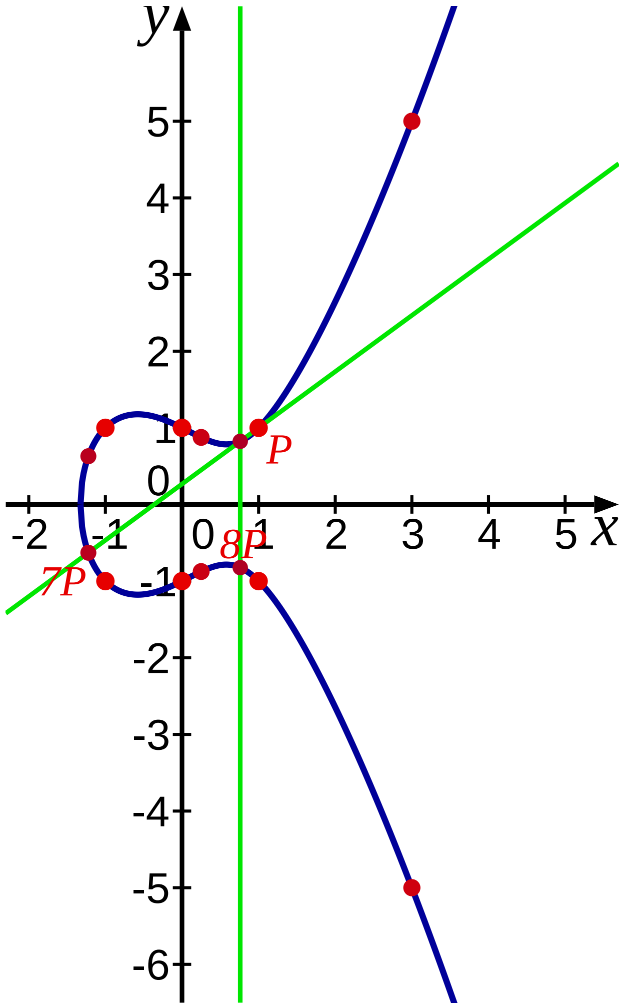




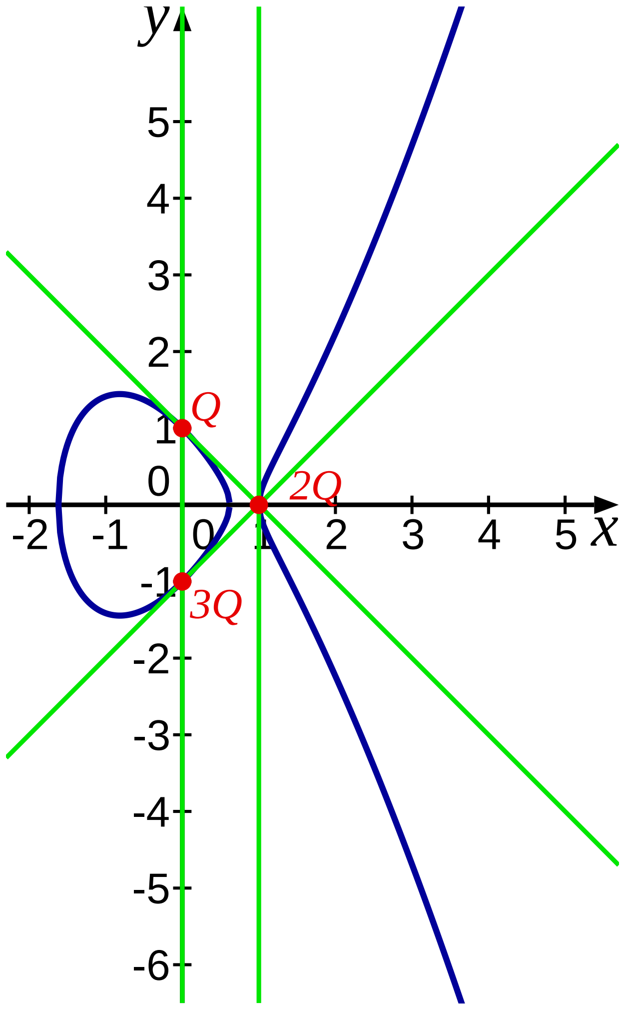
$$6 \cdot P = \left(\frac{1}{4}, \frac{7}{8}\right)$$

$$7 \cdot P = \left(-\frac{11}{9}, -\frac{17}{27}\right)$$

Addition auf E_1 und E_0



$$8 \cdot P = \left(\frac{19}{25}, -\frac{103}{125}\right)$$



$$4 \cdot Q = O$$

Gruppenstruktur

Gruppenstruktur

Für unsere Beispielkurven gilt

$$E_0(\mathbb{Q}) = \{O, Q, 2Q, 3Q\} \cong \mathbb{Z}/4\mathbb{Z}$$
$$E_1(\mathbb{Q}) = \{\ldots, -4P, -3P, -2P, -P, O, P, 2P, 3P, 4P, \ldots\} \cong \mathbb{Z}$$

Gruppenstruktur

Für unsere Beispielkurven gilt

$$E_0(\mathbb{Q}) = \{O, Q, 2Q, 3Q\} \cong \mathbb{Z}/4\mathbb{Z}$$
$$E_1(\mathbb{Q}) = \{\ldots, -4P, -3P, -2P, -P, O, P, 2P, 3P, 4P, \ldots\} \cong \mathbb{Z}$$

Satz (Mordell 1922):
Die Gruppe $E(\mathbb{Q})$ ist stets endlich erzeugt.

Gruppenstruktur

Für unsere Beispielkurven gilt

$$E_0(\mathbb{Q}) = \{O, Q, 2Q, 3Q\} \cong \mathbb{Z}/4\mathbb{Z}$$
$$E_1(\mathbb{Q}) = \{\dots, -4P, -3P, -2P, -P, O, P, 2P, 3P, 4P, \dots\} \cong \mathbb{Z}$$

Satz (Mordell 1922):
Die Gruppe $E(\mathbb{Q})$ ist stets endlich erzeugt.

Man kann also alle rationalen Punkte ausgehend von endlich vielen durch die Geraden-Konstruktion bekommen.

Gruppenstruktur

Für unsere Beispielkurven gilt

$$E_0(\mathbb{Q}) = \{O, Q, 2Q, 3Q\} \cong \mathbb{Z}/4\mathbb{Z}$$
$$E_1(\mathbb{Q}) = \{\dots, -4P, -3P, -2P, -P, O, P, 2P, 3P, 4P, \dots\} \cong \mathbb{Z}$$

Satz (Mordell 1922):
Die Gruppe $E(\mathbb{Q})$ ist stets endlich erzeugt.

Man kann also alle rationalen Punkte ausgehend von endlich vielen durch die Geraden-Konstruktion bekommen.

In den Beispielen genügt sogar jeweils ein Punkt!

Problem

Problem

Man kennt bisher kein Verfahren,
mit dem man $E(\mathbb{Q})$ immer berechnen kann.

Problem

Man kennt bisher kein Verfahren,
mit dem man $E(\mathbb{Q})$ immer berechnen kann.

Insbesondere kann man nicht entscheiden,
ob $E(\mathbb{Q})$ unendlich ist oder nicht.

Problem

Man kennt bisher kein Verfahren,
mit dem man $E(\mathbb{Q})$ immer berechnen kann.

Insbesondere kann man nicht entscheiden,
ob $E(\mathbb{Q})$ unendlich ist oder nicht.

Es gibt aber Methoden, die meistens funktionieren.

Problem

Man kennt bisher kein Verfahren,
mit dem man $E(\mathbb{Q})$ immer berechnen kann.

Insbesondere kann man nicht entscheiden,
ob $E(\mathbb{Q})$ unendlich ist oder nicht.

Es gibt aber Methoden, die meistens funktionieren.

Eine Konsequenz der Gültigkeit der B-SD-Vermutung wäre,
dass diese Methoden tatsächlich immer funktionieren.
(Wenigstens im Prinzip.)

Modulare Arithmetik

Modulare Arithmetik

Einfachere Aufgabe:

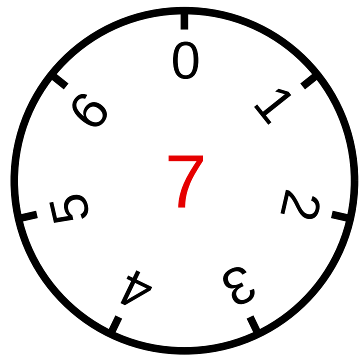
Wir rechnen statt mit rationalen Zahlen mit ganzen Zahlen „modulo p“:

Modulare Arithmetik

Einfachere Aufgabe:

Wir rechnen statt mit rationalen Zahlen mit ganzen Zahlen „modulo p“:

Wir betrachten zwei Zahlen als gleich,
wenn sie sich um ein Vielfaches von p unterscheiden.
Dabei ist p eine Primzahl.

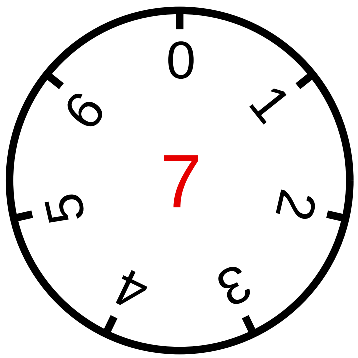


Modulare Arithmetik

Einfachere Aufgabe:

Wir rechnen statt mit rationalen Zahlen mit ganzen Zahlen „modulo p“:

Wir betrachten zwei Zahlen als gleich,
wenn sie sich um ein Vielfaches von p unterscheiden.
Dabei ist p eine Primzahl.



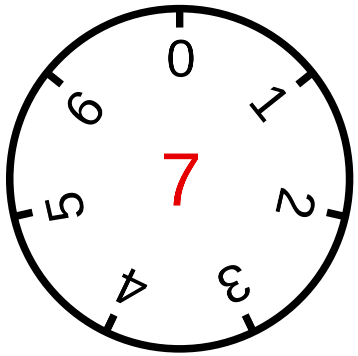
Beispiel $(p = 7)$: $(-2)^3 - (-2) + 1 = -5$ „=“ $9 = 3^2$,
also ist $(-2, 3)$ ein Punkt modulo 7 auf E_1.

Modulare Arithmetik

Einfachere Aufgabe:

Wir rechnen statt mit rationalen Zahlen mit ganzen Zahlen „modulo p“:

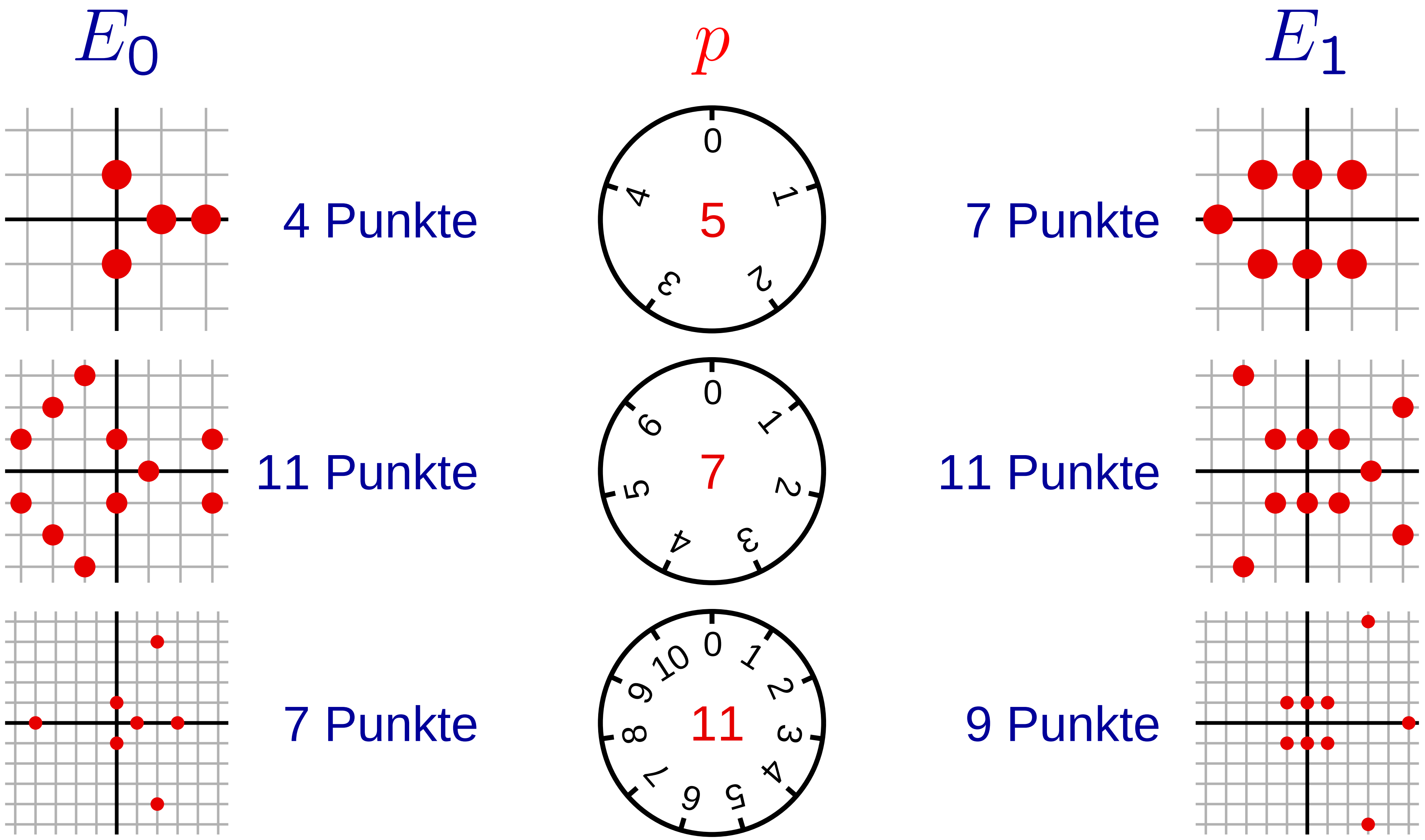
Wir betrachten zwei Zahlen als gleich,
wenn sie sich um ein Vielfaches von p unterscheiden.
Dabei ist p eine Primzahl.



Beispiel ($p = 7$): $\quad (-2)^3 - (-2) + 1 = -5$ „=“ $9 = 3^2$,
also ist $(-2, 3)$ ein Punkt modulo 7 auf E_1.

Wie viele Punkte modulo p haben unsere Kurven?

Unsere Kurven „modulo p“



Mehr Daten

Mehr Daten

Die Anzahl N_p der Punkte (ohne O) modulo p ist nahe bei p; wir schreiben

$$N_p = p + A_p\,.$$

Mehr Daten

Die Anzahl N_p der Punkte (ohne O) modulo p ist nahe bei p; wir schreiben

$$N_p = p + A_p \, .$$

Man kann zeigen, dass $-2\sqrt{p} < A_p < 2\sqrt{p}$.

Mehr Daten

Die Anzahl N_p der Punkte (ohne O) modulo p ist nahe bei p; wir schreiben

$$N_p = p + A_p \, .$$

Man kann zeigen, dass $-2\sqrt{p} < A_p < 2\sqrt{p}$.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$N_p(E_0)$	2	3	4	11	7	15	15	15	19	31	39	31	47	51	43
$A_p(E_0)$	0	0	-1	4	-4	2	-2	-4	-4	2	8	-6	6	8	-4

Mehr Daten

Die Anzahl N_p der Punkte (ohne O) modulo p ist nahe bei p; wir schreiben

$$N_p = p + A_p\,.$$

Man kann zeigen, dass $-2\sqrt{p} < A_p < 2\sqrt{p}$.

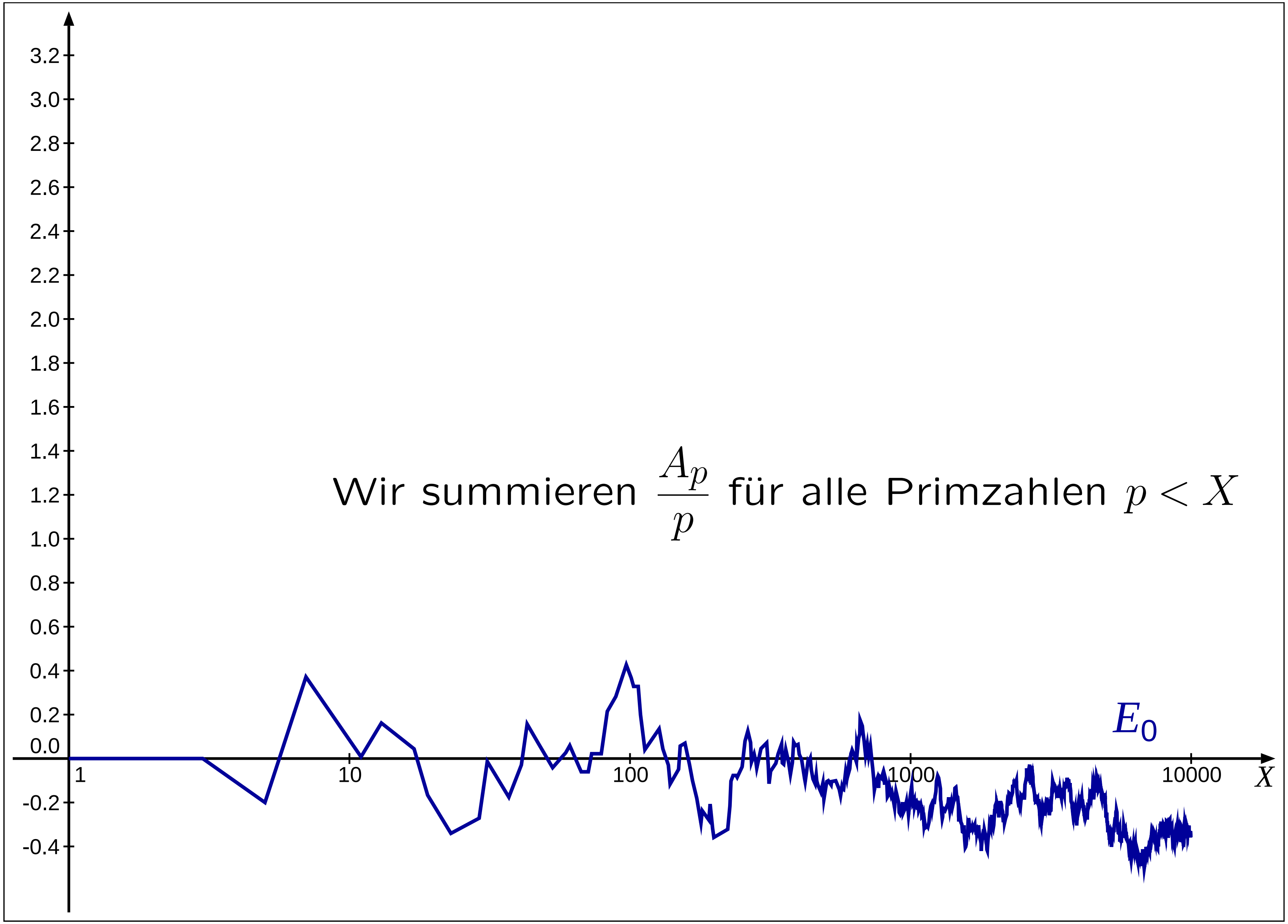
p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$N_p(E_0)$	2	3	4	11	7	15	15	15	19	31	39	31	47	51	43
$A_p(E_0)$	0	0	-1	4	-4	2	-2	-4	-4	2	8	-6	6	8	-4
$N_p(E_1)$	2	6	7	11	9	18	13	21	22	36	34	35	50	51	38
$A_p(E_1)$	0	3	2	4	-2	5	-4	2	-1	7	3	-2	9	8	-9

Die Tendenz

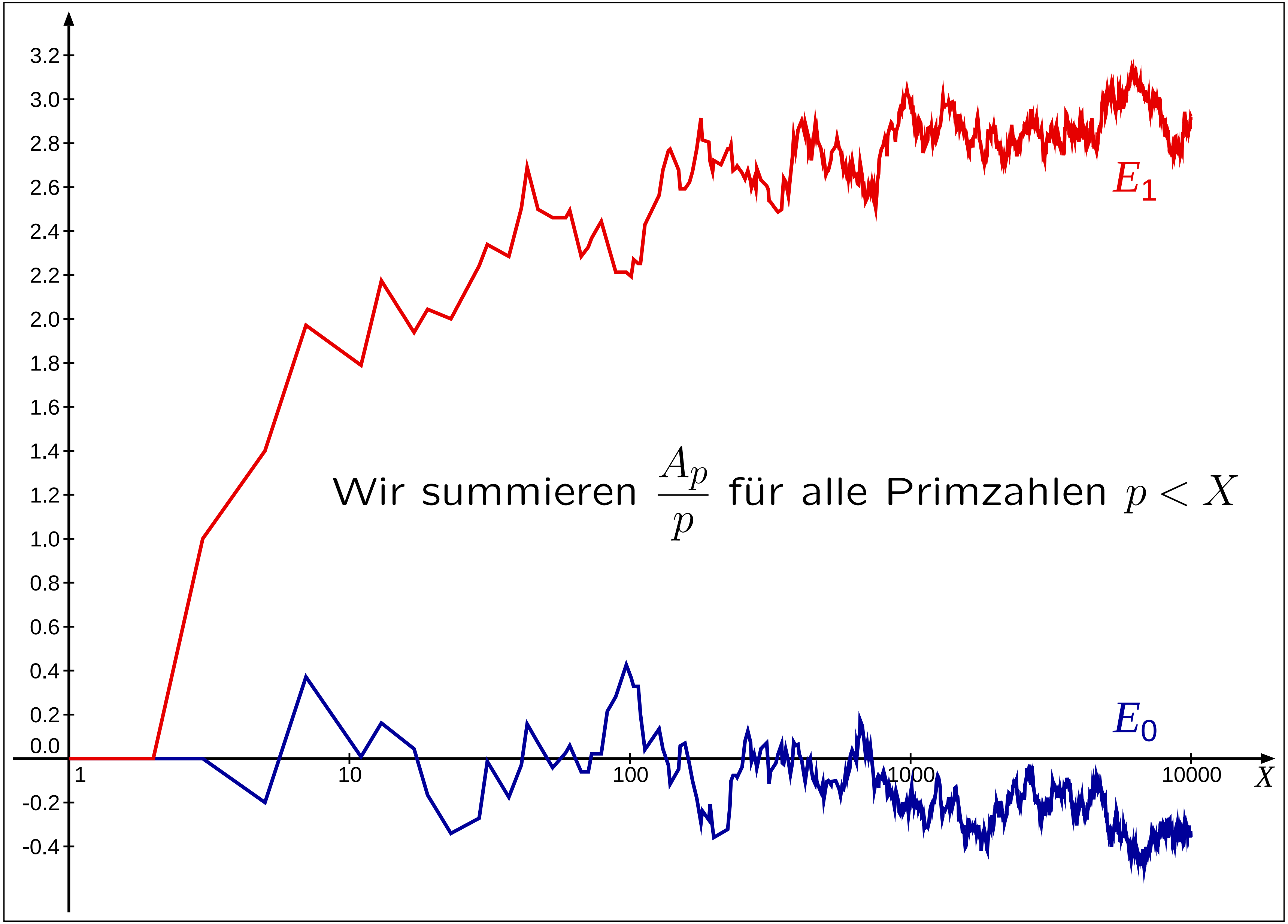
Die Tendenz

Wir summieren $\dfrac{A_p}{p}$ für alle Primzahlen $p < X$

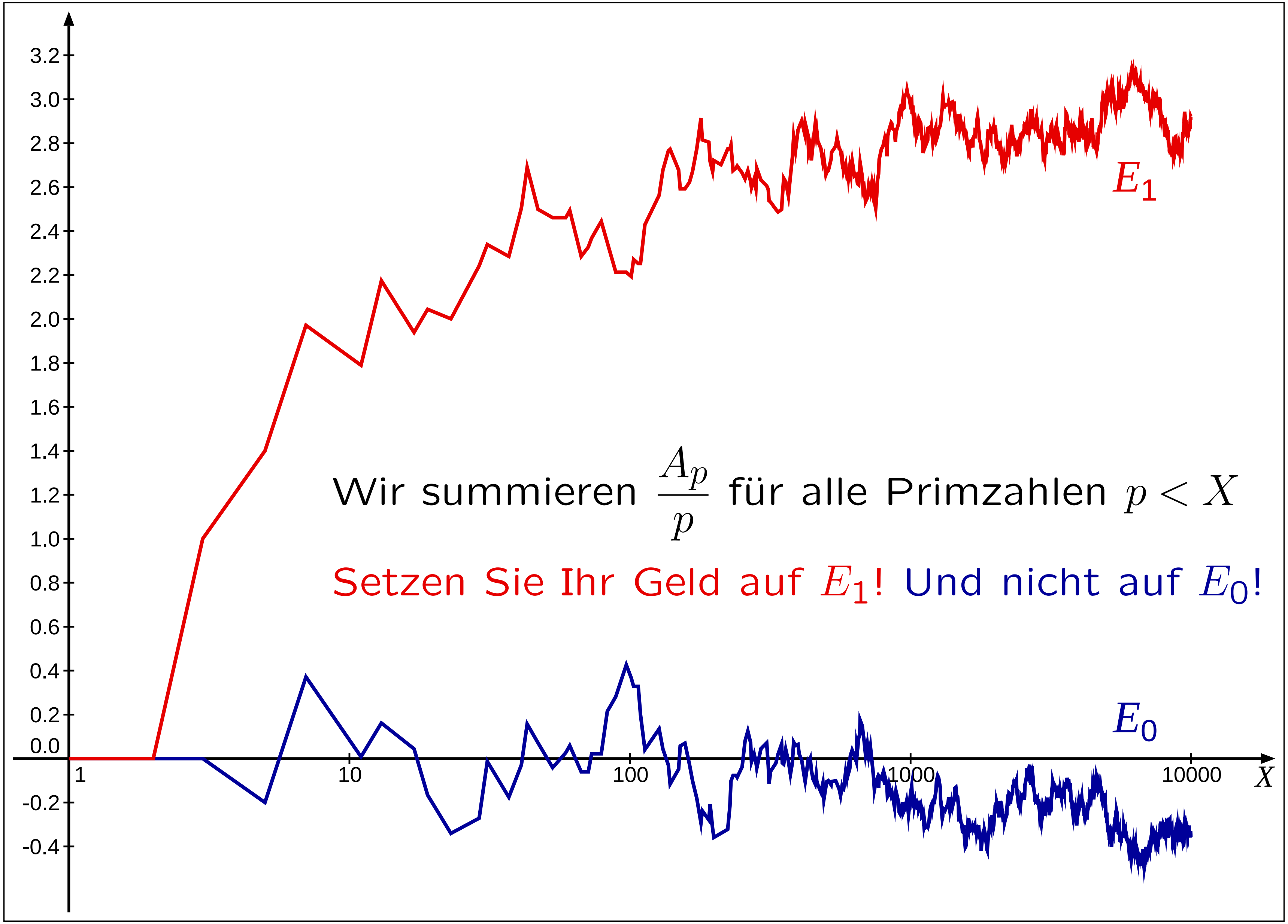
Die Tendenz


Wir summieren $\frac{A_p}{p}$ für alle Primzahlen $p < X$
3.2
3.0
2.8
2.6
2.4
2.2
2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
-0.2
-0.4
1
10
100
1000
10000
X
E_0

Die Tendenz


3.2
3.0
2.8
2.6
2.4
2.2
2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
-0.2
-0.4
1
10
100
1000
10000
X
E_1
E_0
Wir summieren $\dfrac{A_p}{p}$ für alle Primzahlen $p < X$

Die Tendenz



Wir summieren $\dfrac{A_p}{p}$ für alle Primzahlen $p < X$

Setzen Sie Ihr Geld auf E_1! Und nicht auf E_0!

Die Vermutung

Die Vermutung

Die **Vermutung von Birch und Swinnerton-Dyer** sagt im wesentlichen:

Eine elliptische Kurve hat genau dann **unendlich viele** rationale Punkte, wenn die Summe über A_p/p für $p < X$ mit X **über alle Grenzen wächst**.

Die Vermutung

Die **Vermutung von Birch und Swinnerton-Dyer** sagt im wesentlichen:

Eine elliptische Kurve hat genau dann **unendlich viele** rationale Punkte, wenn die Summe über A_p/p für $p < X$ mit X **über alle Grenzen wächst**.

Die präzise Formulierung benutzt statt der Summe das Produkt

$$L(E,s) = \prod_p \frac{1}{1 + A_p p^{-s} + p^{1-2s}},$$

das zunächst nur für $s > \frac{3}{2}$ definiert ist,
aber beliebig weit „nach links“ fortgesetzt werden kann.

Die Vermutung

Die **Vermutung von Birch und Swinnerton-Dyer** sagt im wesentlichen:

Eine elliptische Kurve hat genau dann **unendlich viele** rationale Punkte, wenn die Summe über A_p/p für $p < X$ mit X **über alle Grenzen wächst**.

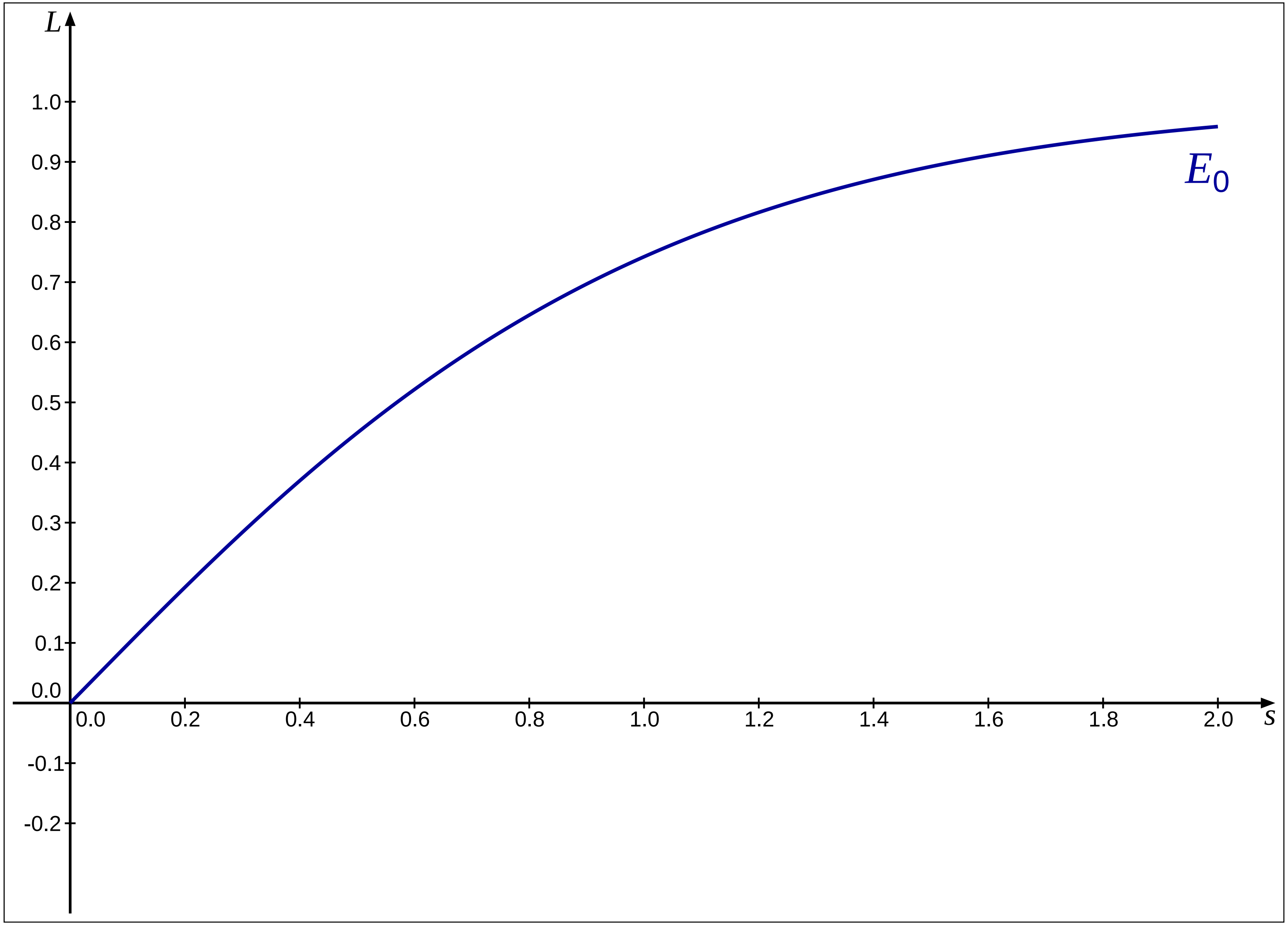
Die präzise Formulierung benutzt statt der Summe das Produkt

$$L(E,s) = \prod_p \frac{1}{1 + A_p p^{-s} + p^{1-2s}},$$

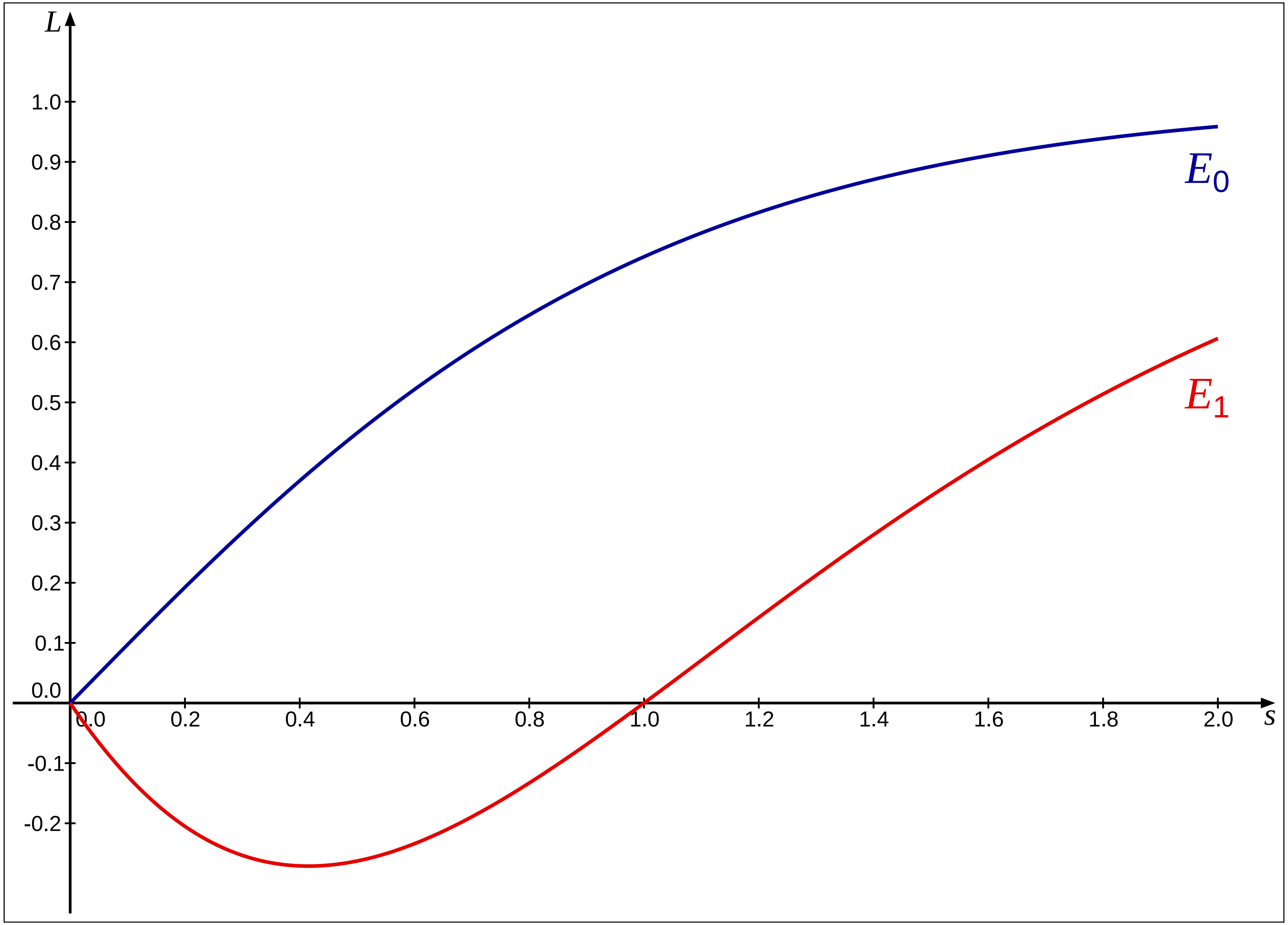
das zunächst nur für $s > \frac{3}{2}$ definiert ist,
aber beliebig weit „nach links" fortgesetzt werden kann.

Vermutung: E hat unendlich viele rationale Punkte $\iff L(E,1) = 0$.

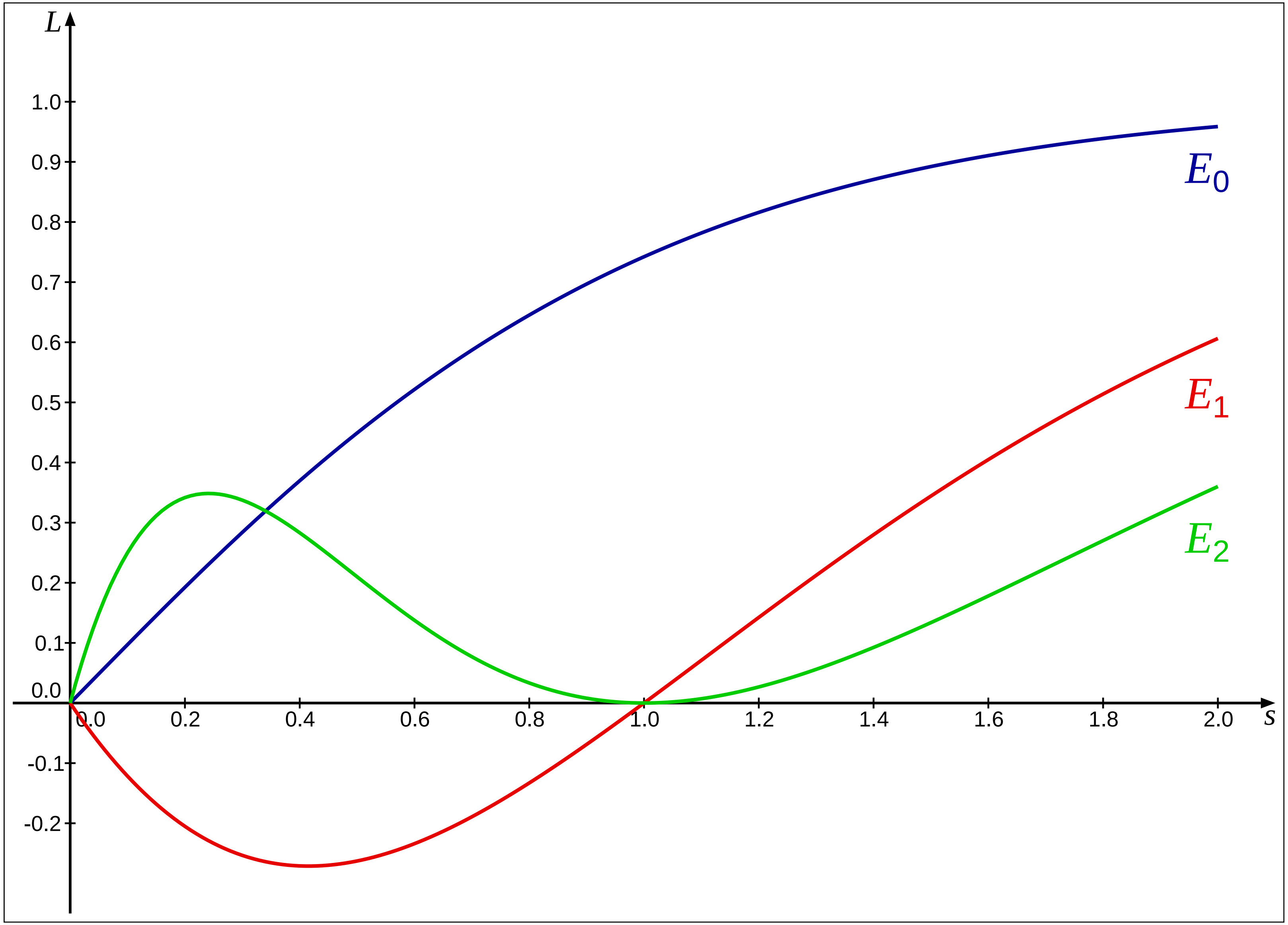
Einige L-Funktionen



Einige L-Funktionen



Einige L-Funktionen



Genauere Formulierung

Genauere Formulierung

Man kann messen, „wie unendlich" die Anzahl der rationalen Punkte ist.
Das wird ausgedrückt durch den Rang $r \geq 0$ von $E(\mathbb{Q})$.

Genauere Formulierung

Man kann messen, „wie unendlich“ die Anzahl der rationalen Punkte ist.
Das wird ausgedrückt durch den Rang $r \geq 0$ von $E(\mathbb{Q})$.

$$\text{endlich viele rationale Punkte} \iff r = 0$$

Genauere Formulierung

Man kann messen, „wie unendlich“ die Anzahl der rationalen Punkte ist. Das wird ausgedrückt durch den Rang $r \geq 0$ von $E(\mathbb{Q})$.

$$\text{endlich viele rationale Punkte} \iff r = 0$$

Vermutung:

Die Funktion $L(E, s)$ hat bei $s = 1$ genau eine r-fache Nullstelle.

Genauere Formulierung

Man kann messen, „wie unendlich“ die Anzahl der rationalen Punkte ist. Das wird ausgedrückt durch den Rang $r \geq 0$ von $E(\mathbb{Q})$.

$$\text{endlich viele rationale Punkte} \iff r = 0$$

Vermutung:

Die Funktion $L(E, s)$ hat bei $s = 1$ genau eine r-fache Nullstelle.

Was man weiß:

Genauere Formulierung

Man kann messen, „wie unendlich“ die Anzahl der rationalen Punkte ist.
Das wird ausgedrückt durch den Rang $r \geq 0$ von $E(\mathbb{Q})$.

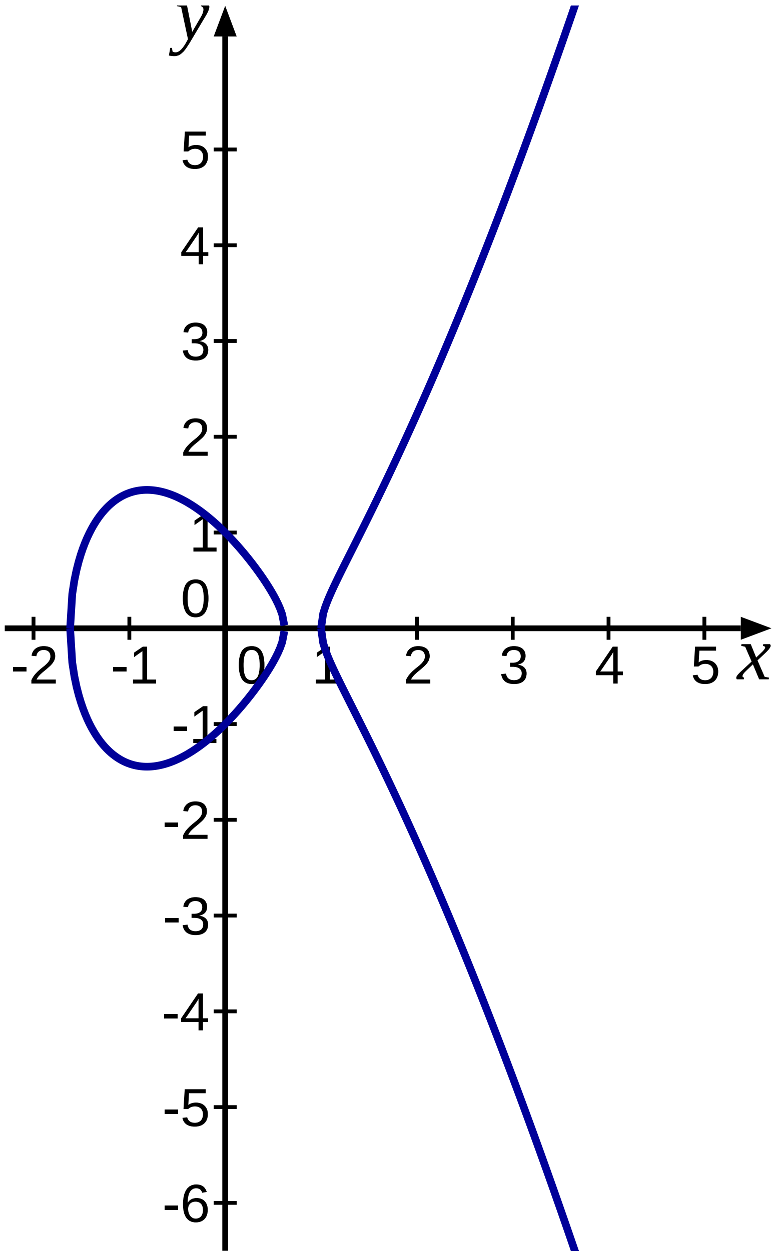
$$\text{endlich viele rationale Punkte} \iff r = 0$$

Vermutung:

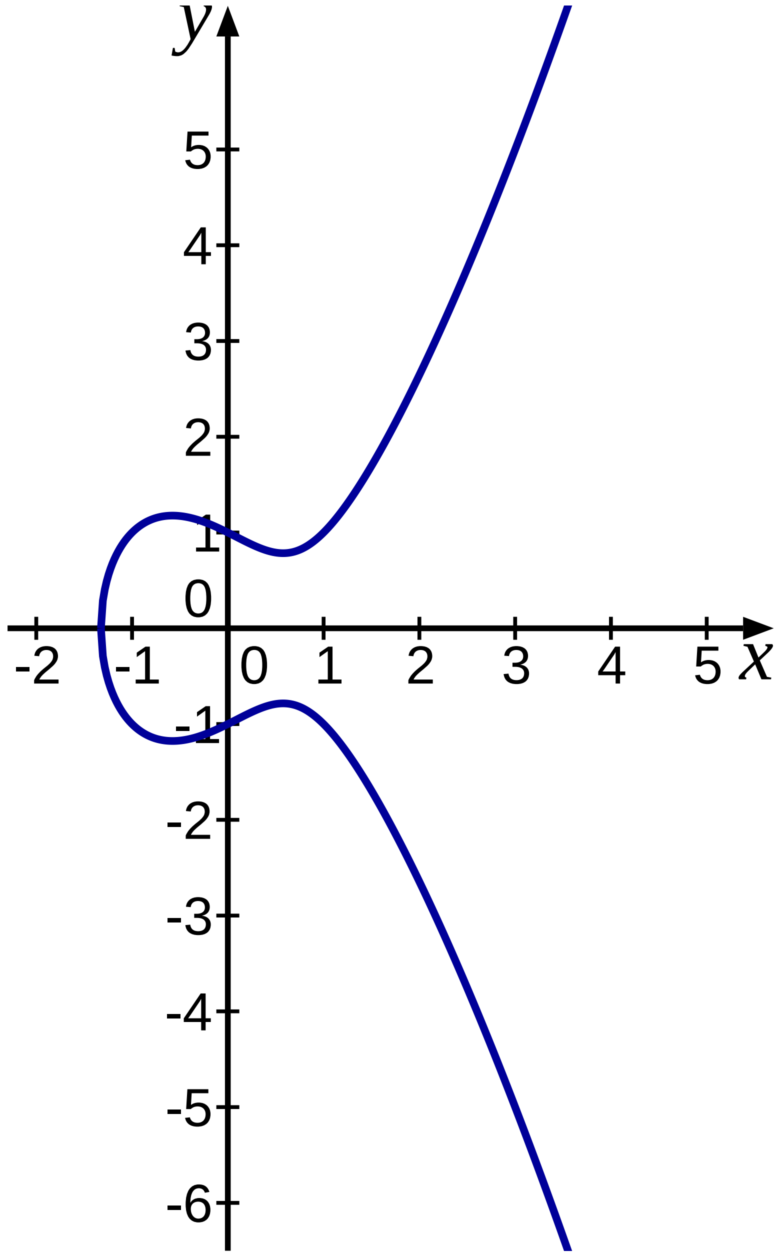
Die Funktion $L(E, s)$ hat bei $s = 1$ genau eine r-fache Nullstelle.

Was man weiß:

Die Vermutung ist richtig,
wenn $L(E, s)$ bei $s = 1$ keine oder eine einfache Nullstelle hat.
(Dies gilt zum Beispiel für E_0 und E_1.)



PAUSE!



Der Rang

Wir wissen: $E(\mathbb{Q})$ ist eine endlich erzeugte abelsche Gruppe.

Also ist $$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$$

mit einer endlichen abelschen Gruppe T.

Die Zahl $r \geq 0$ heißt der Rang von $E(\mathbb{Q})$.

Der Rang

Wir wissen: $E(\mathbb{Q})$ ist eine endlich erzeugte abelsche Gruppe.

Also ist
$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$$
mit einer endlichen abelschen Gruppe T.

Die Zahl $r \geq 0$ heißt der Rang von $E(\mathbb{Q})$.

Satz (Mazur 1977/78):

$$T \cong \mathbb{Z}/n\mathbb{Z} \quad \text{mit } n \in \{1, 2, 3, \ldots, 9, 10, 12\}$$

oder
$$T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \quad \text{mit } n \in \{1, 2, 3, 4\}.$$

T ist leicht zu bestimmen;
die Berechnung von r ist ein offenes Problem.

Die L-Reihe

Sei $\quad E: y^2 = x^3 + Ax + B \quad$ und $\quad \Delta = 4A^3 + 27B^2$.

Für Primzahlen p setzen wir

$$L_p(E,s) = (1 - a_p p^{-s} + \varepsilon_p p^{1-2s})^{-1}\,;$$

für $p \nmid \Delta$ ist dabei $\varepsilon_p = 1$ und $a_p = -A_p$.
(Für $p \mid \Delta$ kann $\varepsilon_p = 0$ sein; dann ist $a_p \in \{-1, 0, 1\}$.)

Dann ist

$$L(E,s) = \prod_p L_p(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}\,.$$

Für $\operatorname{Re} s > 3/2$ konvergieren Produkt und Reihe absolut
und lokal gleichmäßig
und definieren eine holomorphe Funktion von s.

Die L-Reihe

In Analogie etwa zur Riemannschen Zetafunktion erwartet man, dass

- $L(E,s)$ eine holomorphe Fortsetzung auf ganz $\mathbb{C}$ hat und
- eine Funktionalgleichung erfüllt:

Mit $$\Lambda(E,s) = (2\pi)^{-s}\Gamma(s)N^{s/2}L(E,s)$$

(N ist der „Führer“ von E) sollte gelten

$$\Lambda(E,2-s) = \pm\Lambda(E,s)\,.$$

Die L-Reihe

In Analogie etwa zur Riemannschen Zetafunktion erwartet man, dass

- $L(E, s)$ eine holomorphe Fortsetzung auf ganz $\mathbb{C}$ hat und
- eine Funktionalgleichung erfüllt:

Mit $$\Lambda(E, s) = (2\pi)^{-s}\Gamma(s)N^{s/2}L(E, s)$$

(N ist der „Führer“ von E) sollte gelten

$$\Lambda(E, 2 - s) = \pm\Lambda(E, s)\,.$$

Für beides gibt es keinen direkten Beweis.

Für elliptische Kurven über $\mathbb{Q}$ folgt es aus der Modularitätsvermutung (die inzwischen ein Satz ist).

Man kann also von der Vielfachheit der Nullstelle von $L(E, s)$ bei $s = 1$ sprechen.

Die Höhe

Für $x = \frac{p}{q} \in \mathbb{Q}$ definieren wir die Höhe als

$$h(x) = \log \max\{|p|, q\}\,.$$

Für $P \in E(\mathbb{Q})$ definieren wir die Höhe von P durch

$$h(O) = 0 \quad \text{und} \quad h((x,y)) = h(x)\,.$$

Es gilt dann (für $B \to \infty$)

$$\#\{P \in E(\mathbb{Q}) \mid h(P) \le B\} \sim c\,B^{r/2}\,.$$

mit einer (von E abhängigen) Konstanten $c > 0$.

Verfeinerung der Vermutung

Es gibt eine präzisere Form der B-SD-Vermutung, die zu folgender Aussage äquivalent ist:

$$\lim_{B\to\infty}\Big(\#\{P\in E(\mathbb{Q}) \mid h(P)\le B\}\Big)^2 L(E,1+B^{-1}) = \lambda_r^2 c(E)\#\text{Ш}(E)$$

Hierbei ist $\lambda_r = \frac{\pi^{r/2}}{(r/2)!}$ das Volumen der r-dimensionalen Einheitskugel, und $c(E)$ ist eine einfach zu bestimmende Konstante.

$\text{Ш}(E)$ ist die Shafarevich-Tate-Gruppe von E, eine E zugeordnete abelsche Gruppe, von der vermutet wird, dass sie stets endlich ist.

Diese Endlichkeitsvermutung ist aber nicht allgemein bewiesen.

Zitat von John Tate

„This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group $Ш$ which is not known to be finite!“

Zitat von John Tate

„This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group Ш which is not known to be finite!“

Inzwischen wissen wir, dass $L(E, s)$ für alle $s \in \mathbb{C}$ definiert ist.

Es wird erwartet, dass ein allgemeiner Beweis der B-SD-Vermutung einen Beweis der Endlichkeit von $\text{Ш}(E)$ mitliefern wird.

Zitat von John Tate

„This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group $Ш$ which is not known to be finite!“

Inzwischen wissen wir, dass $L(E,s)$ für alle $s \in \mathbb{C}$ definiert ist.

Es wird erwartet, dass ein allgemeiner Beweis der B-SD-Vermutung einen Beweis der Endlichkeit von $Ш(E)$ mitliefern wird.

Was bekannt ist (Kolyvagin 1989):

Ist $\mathrm{ord}_{s=1} L(E,s) \leq 1$, dann gilt

$$r = \mathrm{ord}_{s=1} L(E,s)\,, \qquad Ш(E) \text{ ist endlich},$$

und die verfeinerte Vermutung gilt bis auf einen rationalen Faktor $\neq 0$.

Parität

Sei $w(E) = \pm 1$ das Vorzeichen in der Funktionalgleichung:

$$\Lambda(E, 2-s) = w(E)\Lambda(E, s)\,.$$

Dann ist $(-1)^{\mathrm{ord}_{s=1} L(E,s)} = w(E)$.

Das erwartete Vorzeichen $w(E)$ kann einfach bestimmt werden, auch wenn die analytische Fortsetzbarkeit von $L(E, s)$ nicht bekannt ist.

Es sollte also gelten:

$$(-1)^r = w(E)\,.$$

Parität

Sei $w(E) = \pm 1$ das Vorzeichen in der Funktionalgleichung:

$$\Lambda(E, 2-s) = w(E)\Lambda(E, s)\,.$$

Dann ist $(-1)^{\mathrm{ord}_{s=1} L(E,s)} = w(E)$.

Das erwartete Vorzeichen $w(E)$ kann einfach bestimmt werden, auch wenn die analytische Fortsetzbarkeit von $L(E, s)$ nicht bekannt ist.

Es sollte also gelten:

$$(-1)^r = w(E)\,.$$

Dies („B-SD modulo 2“) ist bewiesen (z.B. Dokchitser&Dokchitser 2008) unter der Voraussetzung $Ш(E)$ endlich.

Modularität

Auf der oberen Halbebene $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$
operiert die Gruppe $\mathrm{SL}(2, \mathbb{Z})$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}$$

Für $N > 1$ betrachten wir $\quad \Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N \right\}$.

Der Quotient $\Gamma_0(N) \backslash \mathbb{H}$, vervollständigt durch endlich viele Punkte,
ist eine kompakte Riemannsche Fläche;
die zugehörige algebraische Kurve $X_0(N)$ ist über $\mathbb{Q}$ definiert.

Modularität

Auf der oberen Halbebene $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$
operiert die Gruppe $\mathrm{SL}(2,\mathbb{Z})$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

Für $N > 1$ betrachten wir $\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N \right\}$.

Der Quotient $\Gamma_0(N)\backslash\mathbb{H}$, vervollständigt durch endlich viele Punkte,
ist eine kompakte Riemannsche Fläche;
die zugehörige algebraische Kurve $X_0(N)$ ist über $\mathbb{Q}$ definiert.

Eine elliptische Kurve E vom Führer N heißt modular,
wenn es einen nicht-konstanten Morphismus $\phi : X_0(N) \to E$ gibt.

Modularität

Eine elliptische Kurve E vom Führer N heißt modular,
wenn es einen nicht-konstanten Morphismus $\phi : X_0(N) \to E$ gibt.

Modularität

Eine elliptische Kurve E vom Führer N heißt modular,
wenn es einen nicht-konstanten Morphismus $\phi : X_0(N) \to E$ gibt.

Sei $\omega = dx/2y$ (eine 1-Form auf E) und $\psi : \mathbb{H}^* \to X_0(N)$.
Dann ist $\psi^*\phi^*\omega = f(z)\,dz$ unter $\Gamma_0(N)$ invariant:
f ist eine Modulform vom Gewicht 2 (sogar eine Spitzenform).

Modularität

Eine elliptische Kurve E vom Führer N heißt modular,
wenn es einen nicht-konstanten Morphismus $\phi : X_0(N) \to E$ gibt.

Sei $\omega = dx/2y$ (eine 1-Form auf E) und $\psi : \mathbb{H}^* \to X_0(N)$.
Dann ist $\psi^*\phi^*\omega = f(z)\,dz$ unter $\Gamma_0(N)$ invariant:
f ist eine Modulform vom Gewicht 2 (sogar eine Spitzenform).

Insbesondere gilt $f(z+1) = f(z)$, also hat f eine Fourierentwicklung:

$$f(z) = c(q + a_2q^2 + a_3q^3 + a_4q^4 + \dots) \qquad \text{mit } q = e^{2\pi iz}$$

Dann ist

$$L(E,s) = 1 + a_2 2^{-s} + a_3 3^{-s} + a_4 4^{-s} + \dots\,;$$

$L(E,s)$ hat eine holomorphe Fortsetzung auf $\mathbb{C}$
und erfüllt die erwartete Funktionalgleichung.

Modularität

Satz (Wiles, Breuil, Conrad, Diamond, Taylor 1995–2001):

Jede elliptische Kurve E über $\mathbb{Q}$ ist modular.

Folgerung:

$\mathrm{ord}_{s=1} L(E, s)$ ist definiert.

Modularität

Satz (Wiles, Breuil, Conrad, Diamond, Taylor 1995–2001):

Jede elliptische Kurve E über $\mathbb{Q}$ ist modular.

Folgerung:

$\mathrm{ord}_{s=1} L(E,s)$ ist definiert.

Satz (Gross-Zagier 1986):

Ist E modular und $\mathrm{ord}_{s=1} L(E,s) = 1$, dann ist $E(\mathbb{Q})$ unendlich.

Kolyvagins Resultat basiert darauf.

Modularität

Satz (Wiles, Breuil, Conrad, Diamond, Taylor 1995–2001):

Jede elliptische Kurve E über $\mathbb{Q}$ ist modular.

Folgerung:

$\mathrm{ord}_{s=1} L(E,s)$ ist definiert.

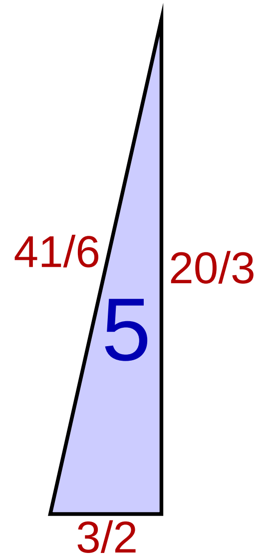
Satz (Gross-Zagier 1986):

Ist E modular und $\mathrm{ord}_{s=1} L(E,s) = 1$, dann ist $E(\mathbb{Q})$ unendlich.

Kolyvagins Resultat basiert darauf.

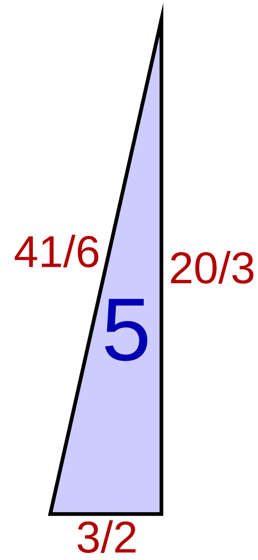
William Stein hat mit einer Reihe von Studenten
die verfeinerte Version der Vermutung für viele Kurven verifiziert.

Kongruenzzahlen



Eine natürliche Zahl n heißt Kongruenzzahl,
wenn n der Flächeninhalt eines rechtwinkligen Dreiecks
mit rationalen Seitenlängen ist.

Kongruenzzahlen

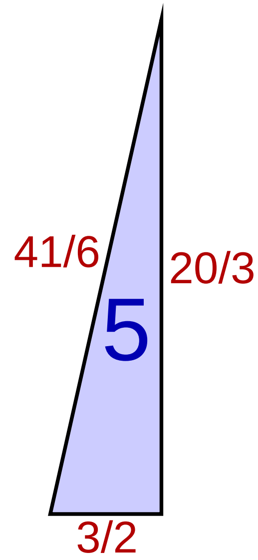


Eine natürliche Zahl n heißt Kongruenzzahl,
wenn n der Flächeninhalt eines rechtwinkligen Dreiecks
mit rationalen Seitenlängen ist.

Tatsache:

$$n \text{ ist Kongruenzzahl} \iff E_n(\mathbb{Q}) \text{ unendlich für } E_n : y^2 = x^3 - n^2 x$$

Kongruenzzahlen



Eine natürliche Zahl n heißt Kongruenzzahl,
wenn n der Flächeninhalt eines rechtwinkligen Dreiecks
mit rationalen Seitenlängen ist.

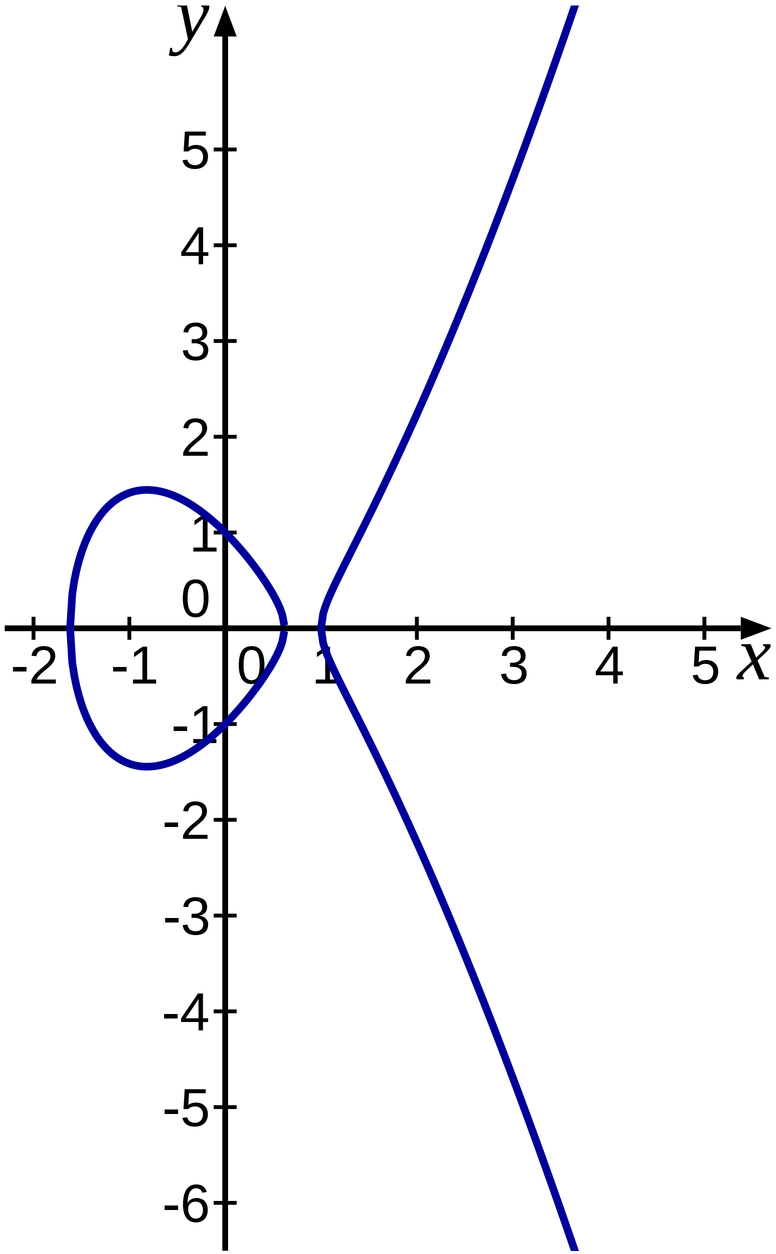
Tatsache:

$$n \text{ ist Kongruenzzahl } \iff E_n(\mathbb{Q}) \text{ unendlich für } E_n : y^2 = x^3 - n^2 x$$

Sei n ungerade und quadratfrei (für n gerade gilt ähnliches).

Satz (Tunnell 1983):
Wenn n Kongruenzzahl ist, dann hat $x^2 + 2y^2 + 8z^2 = n$
gleich viele Lösungen in $\mathbb{Z}$ mit z gerade wie mit z ungerade.

Die B-SD-Vermutung impliziert die Umkehrung.
Zum Beispiel folgt, dass n Kongruenzzahl ist für $n \equiv 5$ oder $7 \bmod 8$.



ENDE