Die Vermutung von Birch und Swinnerton-Dyer

Michael Stoll

Universität Bayreuth

Bremen
22. November 2008

UNIVERSITÄT BAYREUTH

Die Vermutung von Birch und Swinnerton-Dyer

Swinnerton-Dyer
©MFO

Michael Stoll
Universität Bayreuth

Bremen
22. November 2008

Birch
©W.A. Stein

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 .

Elliptische Kurven

Eine Elliptische Kurve ist gegeben durch eine Gleichung

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

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

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 (Brüchen), 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 (Brüchen), 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 (Brüchen), die die Gleichung erfüllen.

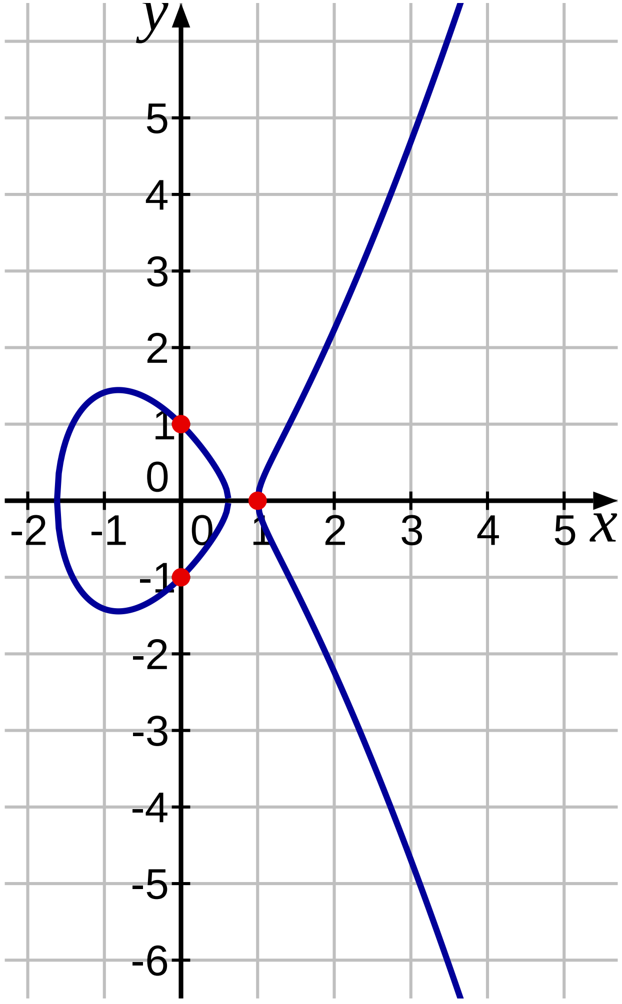
Es kann dabei entweder endlich viele (z.B. gar keine)
oder unendlich viele rationale Punkte geben.

Beispiele (siehe nächste Folie):

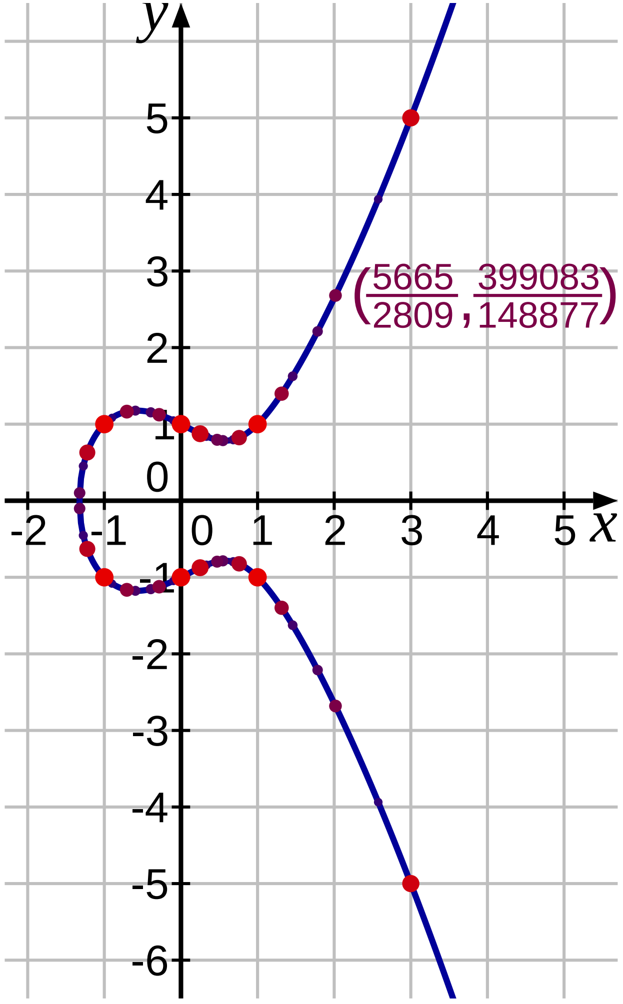
$E_0 : y^2 = x^3 - 2x + 1$ hat genau drei rationale Punkte;

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

Zwei Beispiele



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



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

Modulare Arithmetik

Modulare Arithmetik

Man kennt bisher kein Verfahren, mit dem man entscheiden kann, ob eine gegebene elliptische Kurve unendlich viele rationale Punkte hat.

Modulare Arithmetik

Man kennt bisher kein Verfahren, mit dem man entscheiden kann,
ob eine gegebene elliptische Kurve unendlich viele rationale Punkte hat.

(Es gibt aber Methoden, die meistens funktionieren.)

Modulare Arithmetik

Man kennt bisher kein Verfahren, mit dem man entscheiden kann,
ob eine gegebene elliptische Kurve unendlich viele rationale Punkte hat.

(Es gibt aber Methoden, die meistens funktionieren.)

Einfachere Aufgabe:

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

Modulare Arithmetik

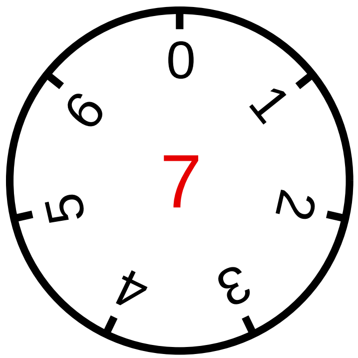
Man kennt bisher kein Verfahren, mit dem man entscheiden kann,
ob eine gegebene elliptische Kurve unendlich viele rationale Punkte hat.

(Es gibt aber Methoden, die meistens funktionieren.)

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

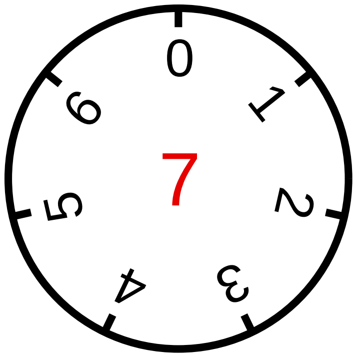
Man kennt bisher kein Verfahren, mit dem man entscheiden kann,
ob eine gegebene elliptische Kurve unendlich viele rationale Punkte hat.

(Es gibt aber Methoden, die meistens funktionieren.)

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

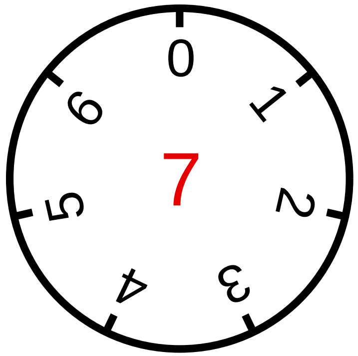
Man kennt bisher kein Verfahren, mit dem man entscheiden kann, ob eine gegebene elliptische Kurve unendlich viele rationale Punkte hat.

(Es gibt aber Methoden, die meistens funktionieren.)

Einfachere Aufgabe:

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

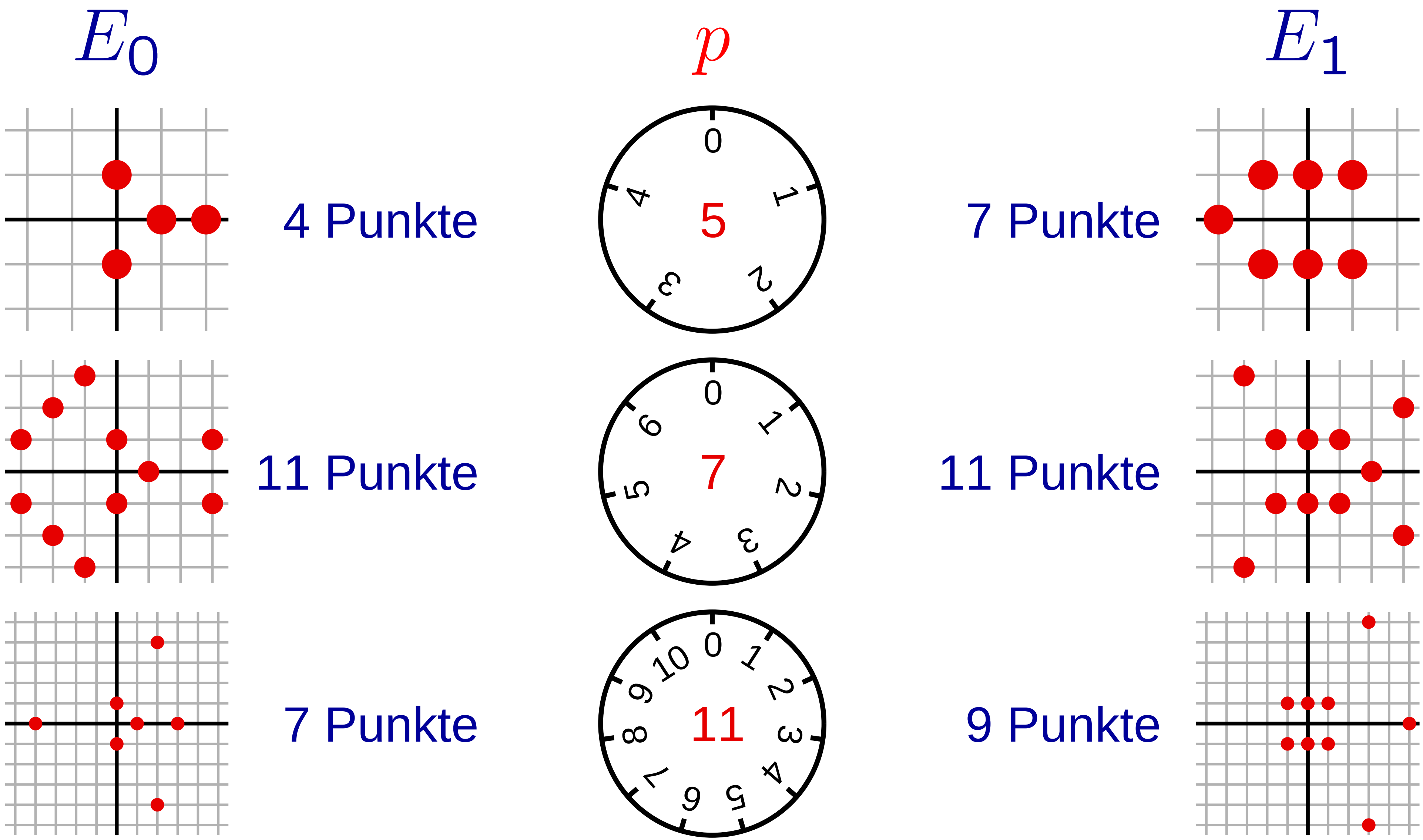
Wir betrachten zwei Zahlen als gleich, wenn sie sich um ein Vielfaches von p unterscheiden. Dabei ist p eine Primzahl.



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

Wie viele Punkte modulo p haben unsere Kurven?

Unsere Kurven „modulo p“



Mehr Daten

Mehr Daten

Die Anzahl N_p der Punkte modulo p ist nahe bei p; wir schreiben

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

Mehr Daten

Die Anzahl N_p der Punkte 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 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 modulo p ist nahe bei p; wir schreiben

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

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

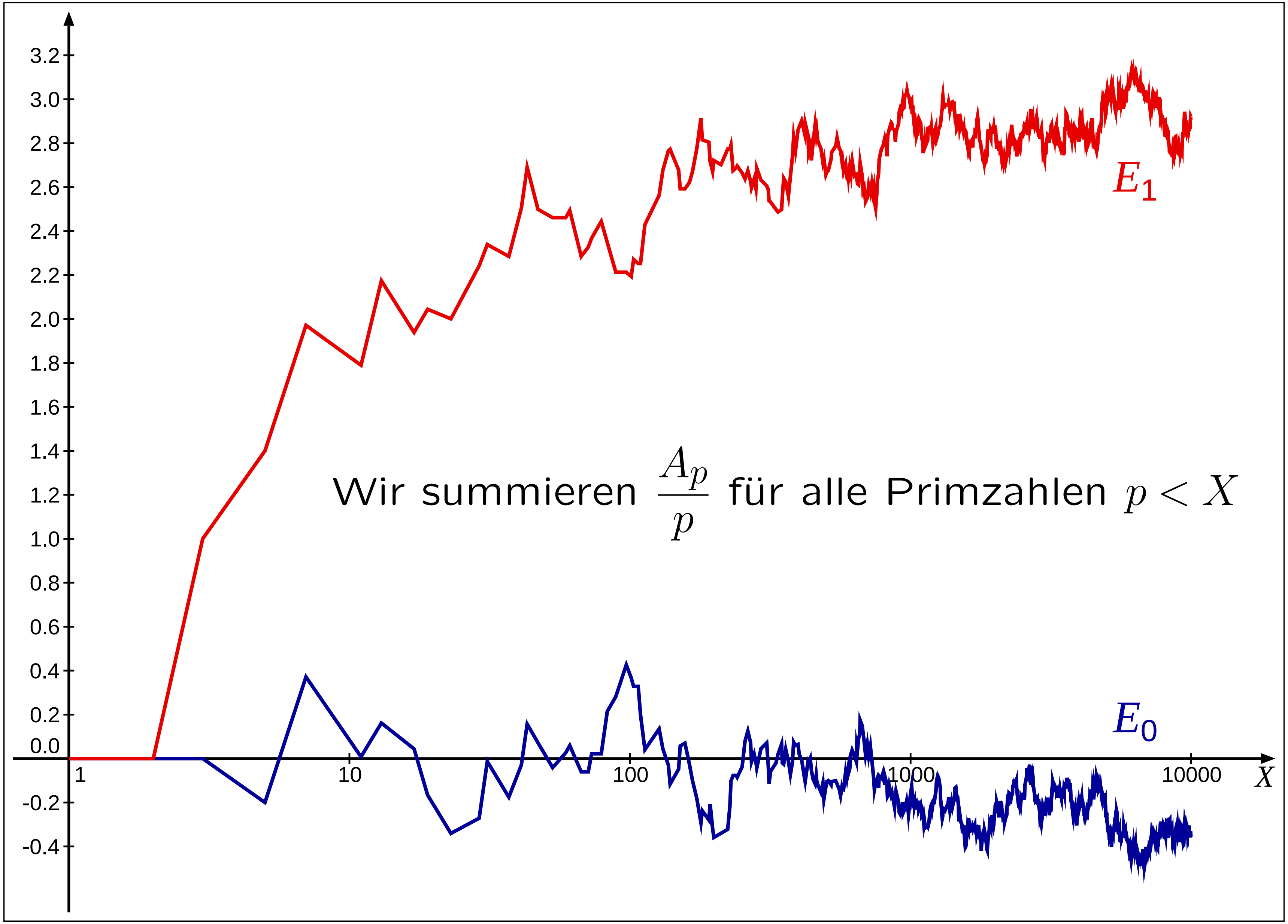
p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$N_p(E_0)$	2	3	4	11	7	15	15	15	19	31	39	31	47	51	43
$A_p(E_0)$	0	0	-1	4	-4	2	-2	-4	-4	2	8	-6	6	8	-4
$N_p(E_1)$	2	6	7	11	9	18	13	21	22	36	34	35	50	51	38
$A_p(E_1)$	0	3	2	4	-2	5	-4	2	-1	7	3	-2	9	8	-9

Die Tendenz

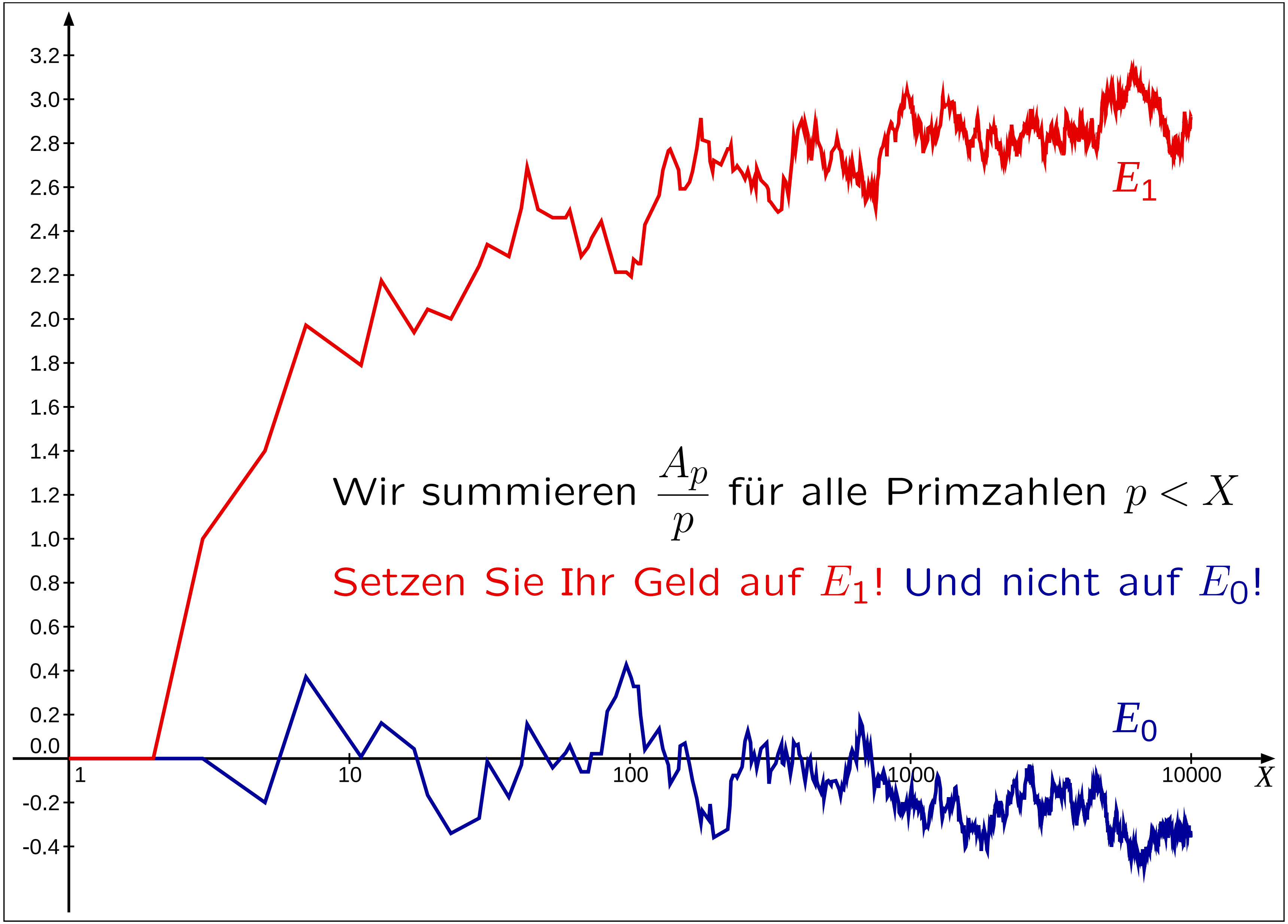
Die Tendenz

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

Die Tendenz


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 $\frac{A_p}{p}$ 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**.

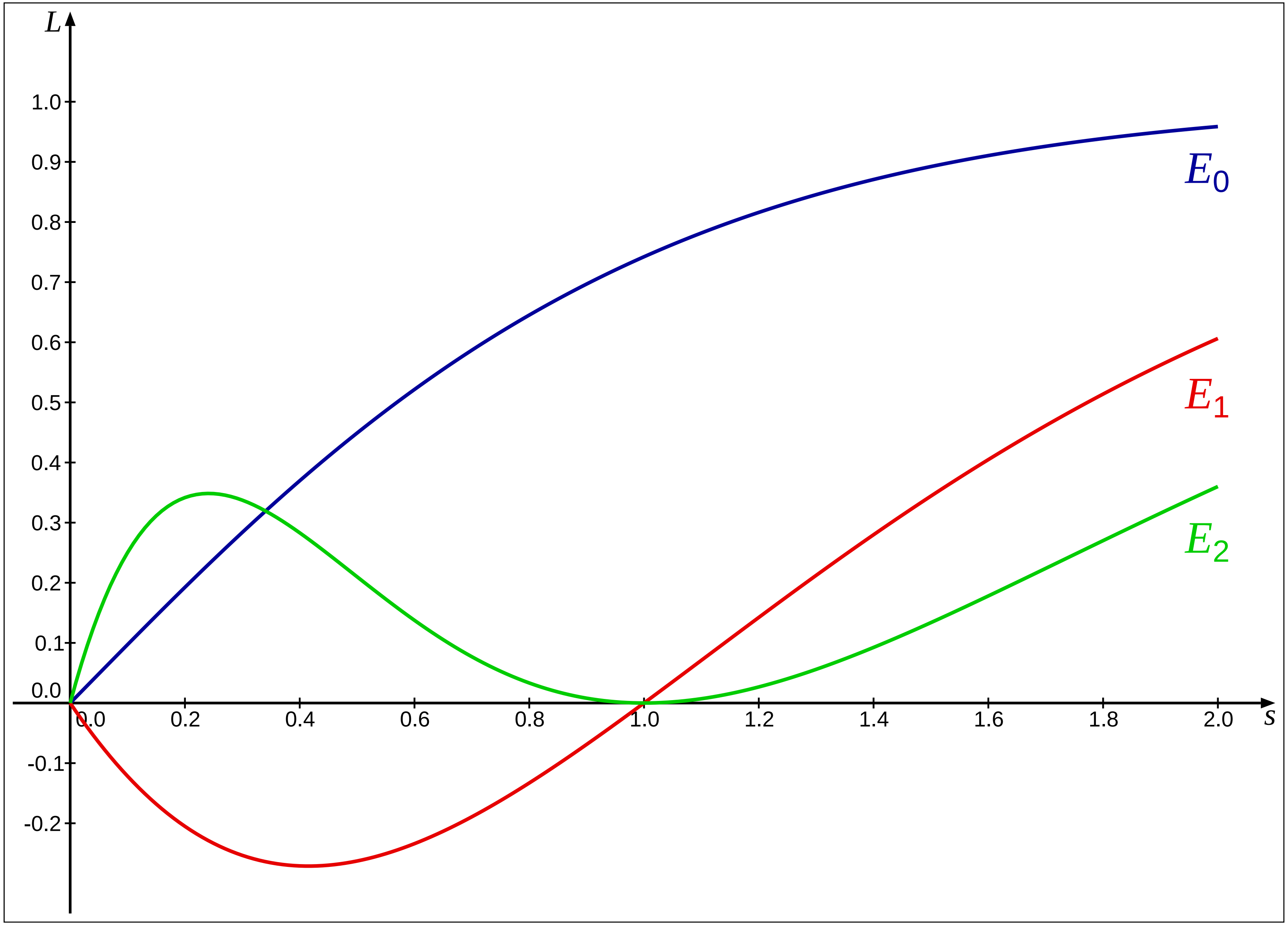
Die präzise Formulierung benutzt statt der Summe das Produkt

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

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



Genauere Formulierung

Genauere Formulierung

Man kann messen, „wie unendlich“ die Anzahl der rationalen Punkte ist.
Das wird ausgedrückt durch den Rang $r \geq 0$.

Genauere Formulierung

Man kann messen, „wie unendlich“ die Anzahl der rationalen Punkte ist. Das wird ausgedrückt durch den Rang $r \geq 0$.

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

Genauere Formulierung

Man kann messen, „wie unendlich“ die Anzahl der rationalen Punkte ist. Das wird ausgedrückt durch den Rang $r \geq 0$.

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

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 $r \geq 0$.

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

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 $r \geq 0$.

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

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.)