Zahlentheorie und Geometrie: alltäglich?!

Gabor Wiese

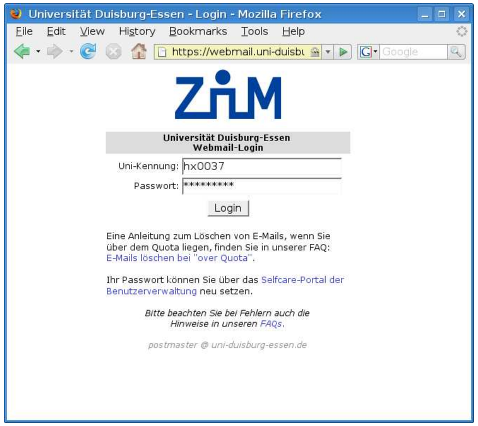
Institut für Experimentelle Mathematik

Universität Duisburg-Essen

Dinge aus dem Alltag

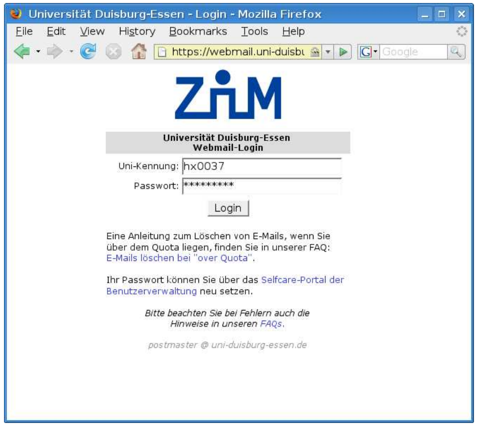
Dinge aus dem Alltag

- an der Uni Duisburg-Essen



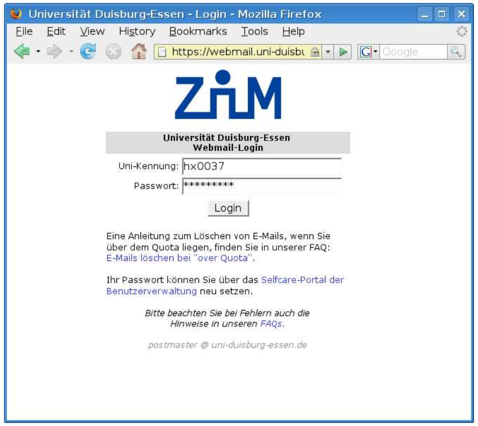
Dinge aus dem Alltag

- an der Uni Duisburg-Essen und in Deutschland



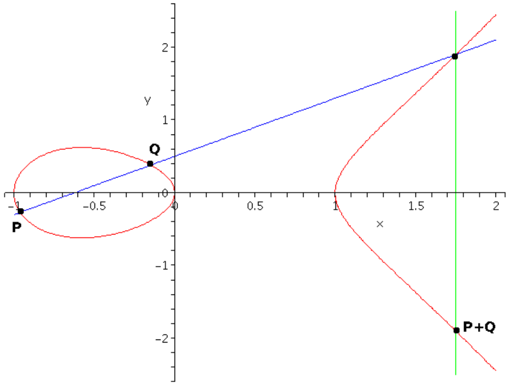
Dinge aus dem Alltag

- an der Uni Duisburg-Essen und in Deutschland



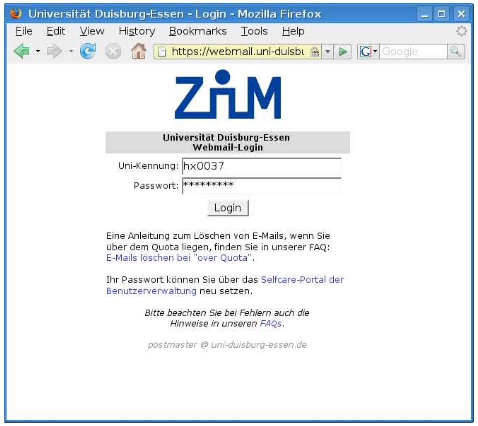
- von Zahlentheoretikern und Geometern

$$y^2 = x^3 + ax + b$$



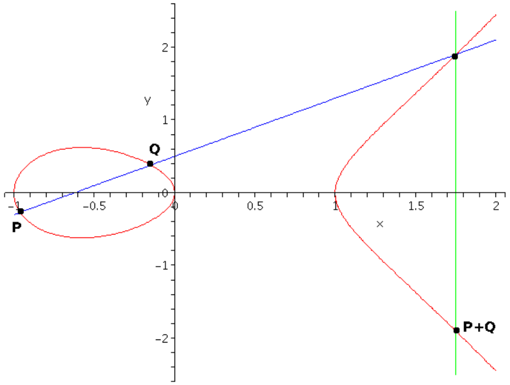
Dinge aus dem Alltag

- an der Uni Duisburg-Essen und in Deutschland



- von Zahlentheoretikern und Geometern

$$y^2 = x^3 + ax + b$$



- in Gallien

Alltag in Gallien

Caesar

Alltag in Gallien

Caesar

General

Alltag in Gallien

Caesar

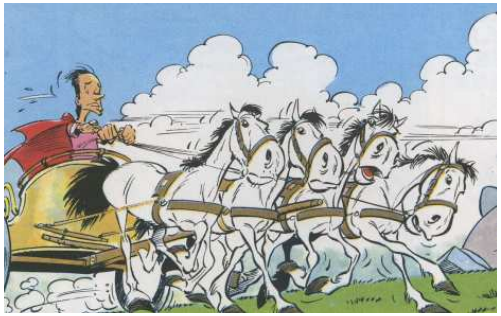
Befehle

General

Alltag in Gallien

Caesar

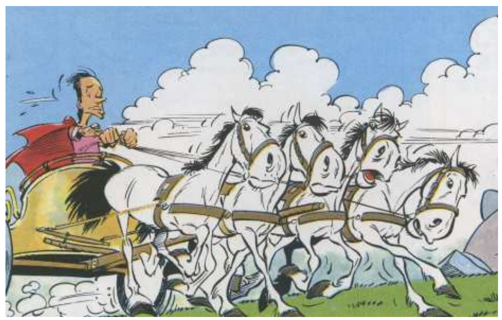
Befehle



General

Alltag in Gallien

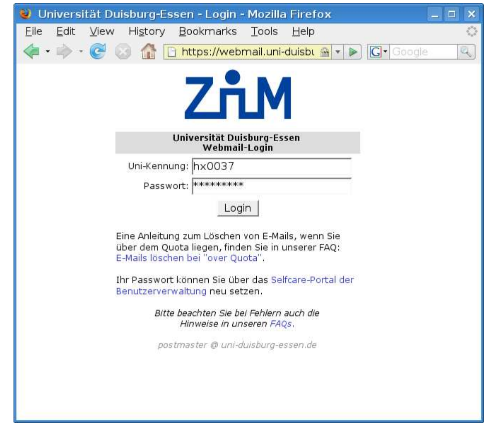
Caesar —Befehle→ General



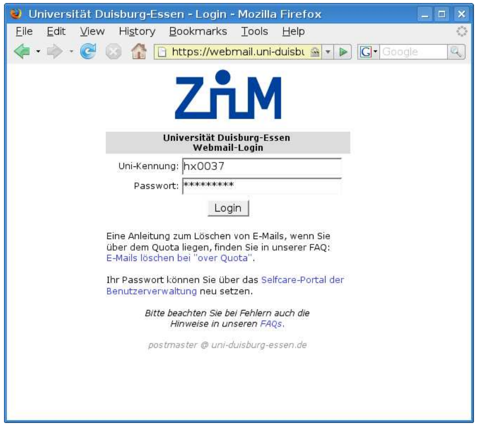
Problem!!

Alltag in Essen

- E-Mails lesen
  Niemand soll meine Mails lesen!

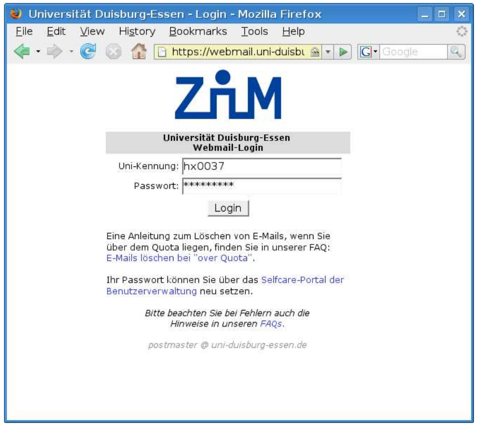


Alltag in Essen



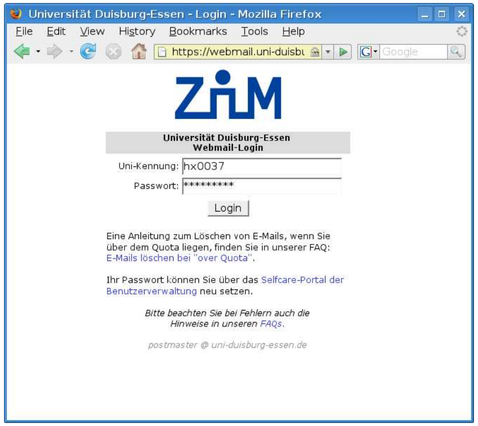
- E-Mails lesen
  Niemand soll meine Mails lesen!
- Bezahlen mit Mensa-Karte
  Aufladen ohne Geldscheine geht nicht.

Alltag in Essen



- E-Mails lesen
  Niemand soll meine Mails lesen!
- Bezahlen mit Mensa-Karte
  Aufladen ohne Geldscheine geht nicht.
- Geld abheben mit der EC-Karte
  ...

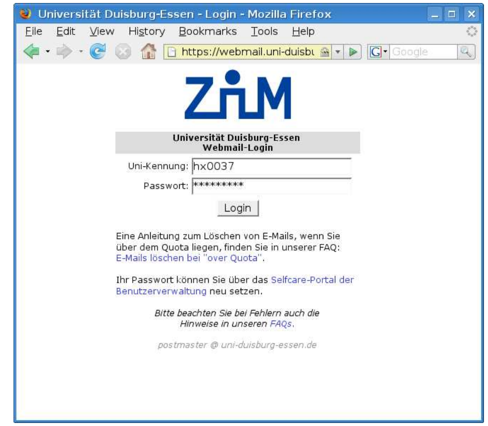
Alltag in Essen



- E-Mails lesen
  Niemand soll meine Mails lesen!
- Bezahlen mit Mensa-Karte
  Aufladen ohne Geldscheine geht nicht.
- Geld abheben mit der EC-Karte
  ...

- Telefonieren mit dem Handy
  Niemand soll auf meine Kosten telefonieren!

Alltag in Essen



- E-Mails lesen
  Niemand soll meine Mails lesen!
- Bezahlen mit Mensa-Karte
  Aufladen ohne Geldscheine geht nicht.

- Geld abheben mit der EC-Karte
  ...
- Telefonieren mit dem Handy
  Niemand soll auf meine Kosten telefonieren!

- etc.

Nun zu Zahlentheorie und Geometrie...

Die fabelhafte Welt der

elliptischen Kurven und Modulformen

From the front page of the
New York Times of 24 June 1993

At Last, Shout of 'Eureka!' In Age-Old Math Mystery

By GINA KOLATA

More than 350 years ago, a French mathematician wrote a deceptively simple theorem in the margins of a book, adding that he had discovered a marvelous proof of it but lacked space to include it in the margin. He died without ever offering his proof, and mathematicians have been trying ever since to supply it.

Now, after thousands of claims of success that proved untrue, mathematicians say the daunting challenge, perhaps the most famous of unsolved mathematical problems, has at last been surmounted.

The problem is Fermat's last theorem, and its apparent conqueror is Dr. Andrew Wiles, a 40-year-old English mathematician who works at Princeton University. Dr. Wiles announced the result yesterday at the last of three lectures given over three days at Cambridge University in England.

Within a few minutes of the conclusion of his final lecture, computer mail messages were winging around the world as mathematicians alerted each other to the startling and almost wholly unexpected result.

Dr. Leonard Adelman of the University of Southern California said he received a message about an hour after Dr. Wiles's announcement. The frenzy is justified, he said. "It's the most exciting thing that's happened in — geez — maybe ever, in mathematics."

Impossible Is Possible

Mathematicians present at the lecture said they felt "an elation," said Dr. Kenneth Ribet of the University of California at Berkeley, in a telephone interview from Cambridge.

The theorem, an overarching statement about what solutions are possible for certain simple equations, was stated in 1637 by Pierre de Fermat, a 17th-century French mathematician and physicist. Many of the brightest minds in mathematics have struggled to find the proof ever since, and many have concluded that Fermat, contrary to his tantalizing claim, had probably failed to develop one despite his considerable

Continued on Page D22, Column 1

Bettmann Archive

Pierre de Fermat, whose theorem may have been proved.

At Last, a 'Eureka!' in an Age-Old Math Mystery

Continued From Page A1

Remembering Pythagoras

Fermat's Last Theorem

Taking the World's 'Eureka'

Turning Point in Proof

Dr. Andrew Wiles explaining his proof of Fermat's last theorem yesterday at Cambridge University in England.

Die fabelhafte Welt der

elliptischen Kurven und Modulformen

From the front page of the
New York Times of 24 June 1993

At Last, Shout of 'Eureka!' In Age-Old Math Mystery

By GINA KOLATA

More than 350 years ago, a French mathematician wrote a deceptively simple theorem in the margins of a book, adding that he had discovered a marvelous proof of it but lacked space to include it in the margin. He died without ever offering his proof, and mathematicians have been trying ever since to supply it.

Now, after thousands of claims of success that proved untrue, mathematicians say the daunting challenge, perhaps the most famous of unsolved mathematical problems, has at last been surmounted.

The problem is Fermat's last theorem, and its apparent conqueror is Dr. Andrew Wiles, a 40-year-old English mathematician who works at Princeton University. Dr. Wiles announced the result yesterday at the last of three lectures given over three days at Cambridge University in England.

Within a few minutes of the conclusion of his final lecture, computer mail messages were winging around the world as mathematicians alerted each other to the startling and almost wholly unexpected result.

Dr. Leonard Adelman of the University of Southern California said he received a message about an hour after Dr. Wiles's announcement. The frenzy is justified, he said. "It's the most exciting thing that's happened in — geez — maybe ever, in mathematics."

Impossible Is Possible

Mathematicians present at the lecture said they felt "an elation," said Dr. Kenneth Ribet of the University of California at Berkeley, in a telephone interview from Cambridge.

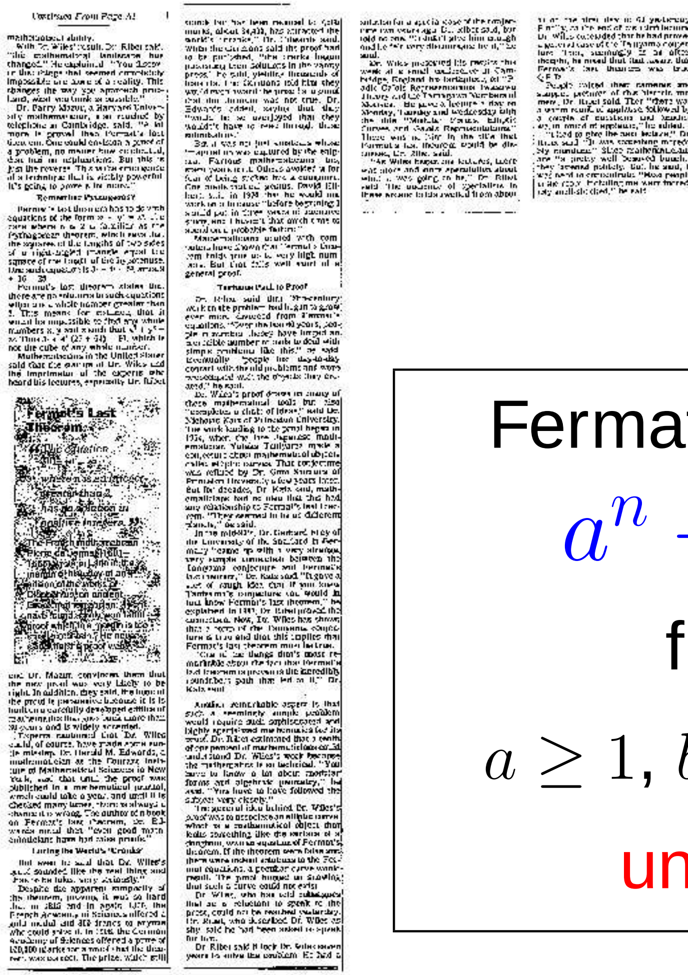
The theorem, an overarching statement about what solutions are possible for certain simple equations, was stated in 1637 by Pierre de Fermat, a 17th-century French mathematician and physicist. Many of the brightest minds in mathematics have struggled to find the proof ever since, and many have concluded that Fermat, contrary to his tantalizing claim, had probably failed to develop one despite his considerable

Continued on Page D22, Column 1

Bettmann Archive

Pierre de Fermat, whose theorem may have been proved.

At Last, a 'Eureka!' in an Age-Old Math Mystery



Dr. Andrew Wiles explaining his proof of Fermat's last theorem yesterday at Cambridge University in England.

Fermats letzter Satz:

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

für $n \geq 3$,

$a \geq 1$, $b \geq 1$ und $c \geq 1$

unmöglich!!!

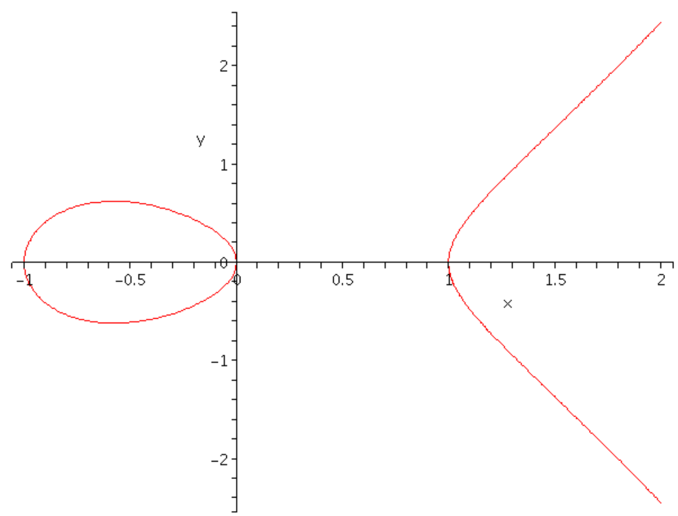
Elliptische Kurven

Eine elliptische Kurve ist eine Punktmenge in der x-y-Ebene der Form

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

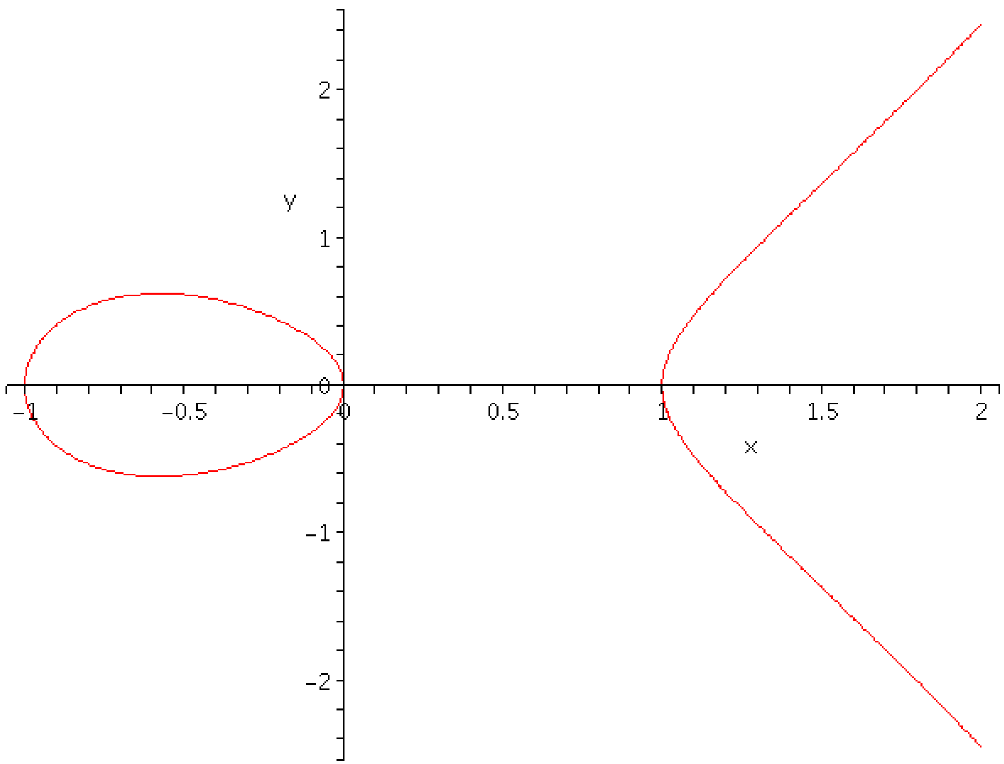
(ohne Selbstdurchschneidungen u. Ä.)

Beispiel: Die (reelle) elliptische Kurve $y^2 = x^3 - x$.



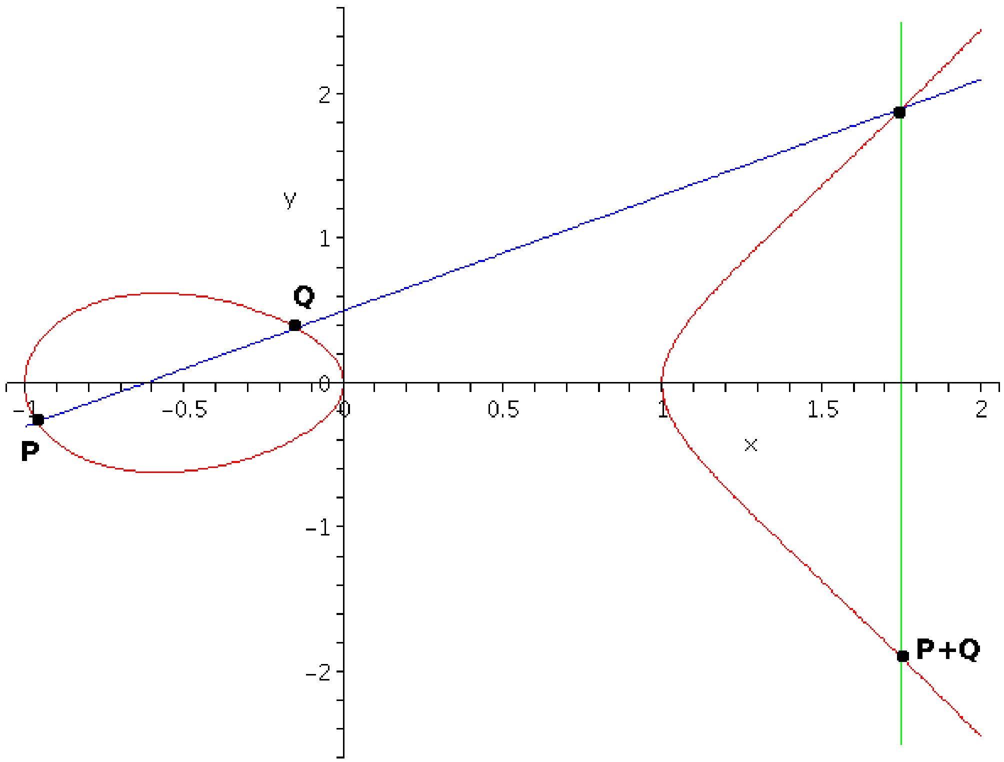
Elliptische Kurven - Addition

Elliptische Kurven haben etwas Besonderes: eine Addition!



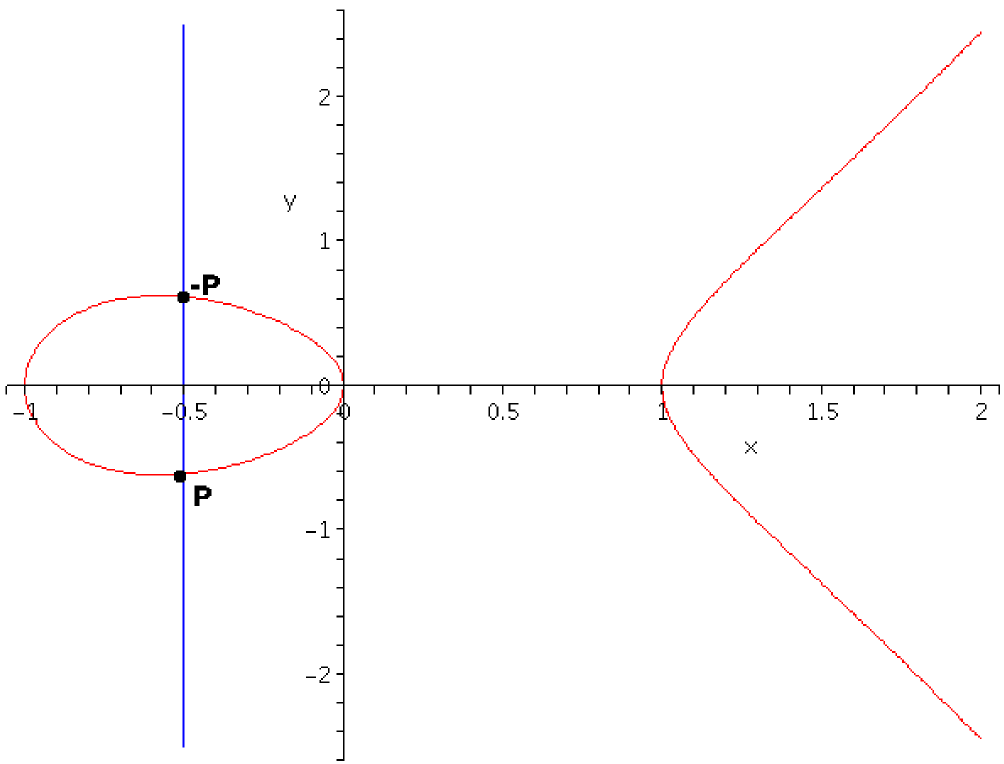
Elliptische Kurven - Addition

Elliptische Kurven haben etwas Besonderes: eine Addition!



Elliptische Kurven - Addition

Elliptische Kurven haben etwas Besonderes: eine Addition!



Elliptische Kurven sind Gruppen

Elliptische Kurven sind abelsche Gruppen!

D.h., die Addition ist genauso wie die Addition ganzer Zahlen

- assoziativ: $P + (Q + R) = (P + Q) + R$,
- kommutativ: $P + Q = Q + P$,
- es gibt ein neutrales Element 0, also $P + 0 = P$,
- man kann auch subtrahieren: $P + (-P) = 0$.

Elliptische Kurven sind Gruppen

Elliptische Kurven sind abelsche Gruppen!

D.h., die Addition ist genauso wie die Addition ganzer Zahlen

- assoziativ: $P + (Q + R) = (P + Q) + R$,
- kommutativ: $P + Q = Q + P$,
- es gibt ein neutrales Element 0, also $P + 0 = P$,
- man kann auch subtrahieren: $P + (-P) = 0$.

Ist n eine natürliche Zahl, dann schreibt man

$$n \cdot P = \underbrace{P + P + \cdots + P}_{n-\text{mal}}.$$

Elliptische Kurven

Sei p Primzahl: Zahl > 1, teilbar nur durch 1 und sich selbst,

z.B. 2, 3, 5, 7, $11, \ldots$.

Elliptische Kurven

Sei p Primzahl: Zahl > 1, teilbar nur durch 1 und sich selbst,

z.B. 2, 3, 5, 7, $11, \ldots$.

Elliptische Kurve, zum Beispiel:

$$E: \; y^2 - x^3 + x + 1 = 0.$$

Elliptische Kurven

Sei p Primzahl: Zahl > 1, teilbar nur durch 1 und sich selbst,

z.B. 2, 3, 5, 7, $11, \ldots$.

Elliptische Kurve, zum Beispiel:

$$E: \; y^2 - x^3 + x + 1 = 0.$$

Betrachte Paare ganzer Zahlen (x, y) mit $0 \leq x < p$ und $0 \leq y < p$, so dass

$$y^2 - x^3 + x + 1$$

durch p teilbar ist.

Elliptische Kurven

Sei p Primzahl: Zahl > 1, teilbar nur durch 1 und sich selbst,

z.B. 2, 3, 5, 7, $11, \ldots$.

Elliptische Kurve, zum Beispiel:

$$E: \; y^2 - x^3 + x + 1 = 0.$$

Betrachte Paare ganzer Zahlen (x, y) mit $0 \leq x < p$ und $0 \leq y < p$, so dass

$$y^2 - x^3 + x + 1$$

durch p teilbar ist.

Diese Paare (x, y) (zusammen mit 0) nennt man $E(\mathbb{F}_p)$,
Punkte der elliptischen Kurve im Körper mit p Elementen.

Eine Gruppe!

Elliptische Kurven

Beispiel:

Sei $p = 2$, die kleinste Primzahl. Wie viele Paare (x, y) mit $0 \leq x < 2$ und $0 \leq y < 2$ gibt es, so dass

$$y^2 - x^3 + x + 1$$

durch 2 teilbar ist?

Elliptische Kurven

Beispiel:

Sei $p = 2$, die kleinste Primzahl. Wie viele Paare (x, y) mit $0 \leq x < 2$ und $0 \leq y < 2$ gibt es, so dass

$$y^2 - x^3 + x + 1$$

durch 2 teilbar ist?

Zwei: $(0, 1)$ und $(1, 1)$.

Elliptische Kurven

Beispiel:

Sei $p = 2$, die kleinste Primzahl. Wie viele Paare (x, y) mit $0 \leq x < 2$ und $0 \leq y < 2$ gibt es, so dass

$$y^2 - x^3 + x + 1$$

durch 2 teilbar ist?

Zwei: $(0, 1)$ und $(1, 1)$.

$E(\mathbb{F}_2)$ ist also eine Gruppe mit 3 Elementen (auch 0!).

UNIVERSITÄT DUISBURG ESSEN

Modulformen

Modulformen sind Funktionen, die *zahlentheoretische Informationen* speichern.

Modulformen

Modulformen sind Funktionen, die *zahlentheoretische Informationen* speichern.

Beispiel:

Weiterhin elliptische Kurve $E:\ y^2 - x^3 + x + 1 = 0.$

Es gibt eine Modulform, die für jede Primzahl p speichert, wie viele Elemente die Gruppe $E(\mathbb{F}_p)$ hat.

Modulformen

Modulformen sind Funktionen, die *zahlentheoretische Informationen* speichern.

Beispiel:

Weiterhin elliptische Kurve $E: \ y^2 - x^3 + x + 1 = 0.$

Es gibt eine Modulform, die für jede Primzahl p speichert, wie viele Elemente die Gruppe $E(\mathbb{F}_p)$ hat.

Mehr zu Modulformen und dem neuesten Durchbruch, die Serre-Vermutung, im Heft der Essener Unikate zum Jahr der Mathematik.

Zurück nach Gallien

UNIVERSITÄT DUISBURG ESSEN

Zurück nach Gallien

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

Zurück nach Gallien

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

A $\mapsto$ D,

Zurück nach Gallien

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

$\mathrm{A} \longmapsto \mathrm{D}, \;\; \mathrm{B} \longmapsto \mathrm{E},$

Zurück nach Gallien

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

$$\mathsf{A} \mapsto \mathsf{D},\ \ \mathsf{B} \mapsto \mathsf{E},\ \ \mathsf{C} \mapsto \mathsf{F}, \ldots, \mathsf{X} \mapsto \mathsf{A}, \mathsf{Y} \mapsto \mathsf{B}, \mathsf{Z} \mapsto \mathsf{C}.$$

Zurück nach Gallien

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

$$\mathrm{A} \mapsto \mathrm{D},\ \ \mathrm{B} \mapsto \mathrm{E},\ \ \mathrm{C} \mapsto \mathrm{F}, \ldots, \mathrm{X} \mapsto \mathrm{A}, \mathrm{Y} \mapsto \mathrm{B}, \mathrm{Z} \mapsto \mathrm{C}.$$

$$\mathrm{ANGRIFF} \mapsto \mathrm{DQJULII}$$

Zurück nach Gallien

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

$$\mathrm{A} \mapsto \mathrm{D},\ \ \mathrm{B} \mapsto \mathrm{E},\ \ \mathrm{C} \mapsto \mathrm{F}, \ldots, \mathrm{X} \mapsto \mathrm{A}, \mathrm{Y} \mapsto \mathrm{B}, \mathrm{Z} \mapsto \mathrm{C}.$$

$$\mathrm{ANGRIFF} \mapsto \mathrm{DQJULII}$$

Kein Problem für Miraculix!

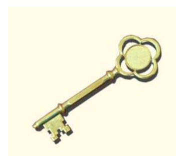
Lösungen (ca. 2030 Jahre nach Caesars Tod)

Fakt: Haben   u.   ein gemeinsames Geheimnis,

einen Schlüssel  (z. B. eine sehr große Zahl),
dann können sie Nachrichten so verschlüsseln,
dass sie nur füreinander lesbar sind.

Lösungen (ca. 2030 Jahre nach Caesars Tod)

Fakt: Haben   u.   ein gemeinsames Geheimnis,

einen Schlüssel  (z. B. eine sehr große Zahl),
dann können sie Nachrichten so verschlüsseln,
dass sie nur füreinander lesbar sind.

Aber:

Caesar ist in Rom,	der General in Gallien.
Ich bin zu Hause,	der Mailserver im Serverraum in Du/E.
Ich bin hier,	meine Bank ist in Nürnberg.
Ich bin hier,	der Handy-Sendemast 1 km von hier.

Lösungen (ca. 2030 Jahre nach Caesars Tod)

Transportiert ein Bote den Schlüssel, dann gibt es Gefahr:

Kopie oder Fälschung des Schlüssels erlauben es, Nachrichten zu lesen oder gar zu fälschen!

Lösungen (ca. 2030 Jahre nach Caesars Tod)

Transportiert ein Bote den Schlüssel, dann gibt es Gefahr:

Kopie oder Fälschung des Schlüssels erlauben es, Nachrichten zu lesen oder gar zu fälschen!

Muss ein Bote den Schlüssel transportieren????

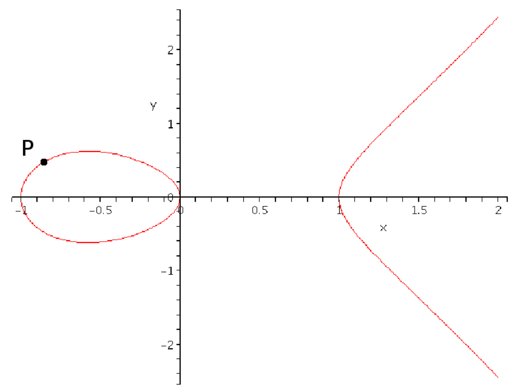
Muss man den Schlüssel verschicken????

Lösungen (ca. 2030 Jahre nach Caesars Tod)

Römisches Amtsblatt

(zu verteilen im ganzen Römischen Reich):

Zur Kommunikation verwende man die elliptische Kurve E



und den Punkt P über einem endlichen Körper,

also z. B. $E(\mathbb{F}_p)$.

(Jeder kennt sie und jeder darf sie auch kennen.)

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.


1. Wählt $a \in \mathbb{N}$.


1. Wählt $b \in \mathbb{N}$.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.


1. Wählt $a \in \mathbb{N}$.
2. Berechnet $a \cdot P$.

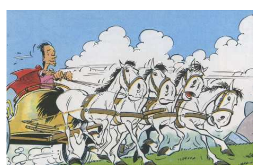

1. Wählt $b \in \mathbb{N}$.
2. Berechnet $b \cdot P$.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.

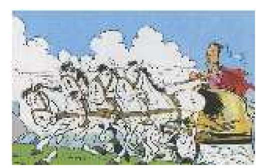
1. Wählt $a \in \mathbb{N}$.
2. Berechnet $a \cdot P$.
3. Verschickt $a \cdot P$.



4. Empfängt $b \cdot P$.

1. Wählt $b \in \mathbb{N}$.
2. Berechnet $b \cdot P$.
3. Verschickt $b \cdot P$.

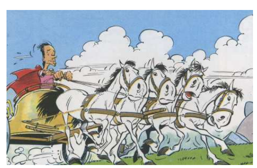


4. Empfängt $a \cdot P$.

Diffie-Hellman-Schlüsselaustausch

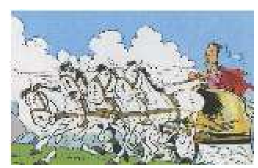
Allen bekannt: elliptische Kurve und ein Punkt P darauf.


1. Wählt $a \in \mathbb{N}$.
2. Berechnet $a \cdot P$.
3. Verschickt $a \cdot P$.



4. Empfängt $b \cdot P$.
5. Berechnet $a \cdot (b \cdot P)$.


1. Wählt $b \in \mathbb{N}$.
2. Berechnet $b \cdot P$.
3. Verschickt $b \cdot P$.

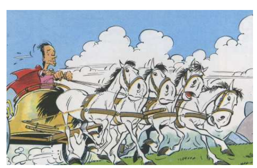


4. Empfängt $a \cdot P$.
5. Berechnet $b \cdot (a \cdot P)$.

Diffie-Hellman-Schlüsselaustausch

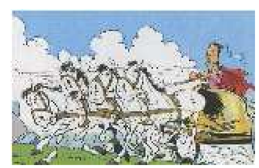
Allen bekannt: elliptische Kurve und ein Punkt P darauf.


1. Wählt $a \in \mathbb{N}$.
2. Berechnet $a \cdot P$.
3. Verschickt $a \cdot P$.

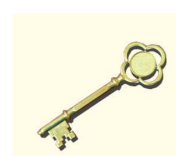


4. Empfängt $b \cdot P$.
5. Berechnet $a \cdot (b \cdot P)$.


1. Wählt $b \in \mathbb{N}$.
2. Berechnet $b \cdot P$.
3. Verschickt $b \cdot P$.



4. Empfängt $a \cdot P$.
5. Berechnet $b \cdot (a \cdot P)$.

Gemeinsames Geheimnis:  $= (a \cdot b) \cdot P$.

Diffie-Hellman-Schlüsselaustausch

Warum ist  $= (a \cdot b) \cdot P$ ein Geheimnis?

Diffie-Hellman-Schlüsselaustausch

Warum ist  $= (a \cdot b) \cdot P$ ein Geheimnis?

Elliptische Kurve ist über endl. Körper mit p Elementen definiert, wobei p

in Binärschreibweise 224 Ziffern haben sollte,

im Dezimalsystem 68 Ziffern haben sollte.

Diffie-Hellman-Schlüsselaustausch

Warum ist  $= (a \cdot b) \cdot P$ ein Geheimnis?

Elliptische Kurve ist über endl. Körper mit p Elementen definiert, wobei p

in Binärschreibweise 224 Ziffern haben sollte,
im Dezimalsystem 68 Ziffern haben sollte.

Die kleinste Primzahl größer 2^{224} ist:
26959946667150639794667015087019630673637144422540572481103610249951

Diffie-Hellman-Schlüsselaustausch

Warum ist  $= (a \cdot b) \cdot P$ ein Geheimnis?

Elliptische Kurve ist über endl. Körper mit p Elementen definiert, wobei p

in Binärschreibweise 224 Ziffern haben sollte,
im Dezimalsystem 68 Ziffern haben sollte.

Die kleinste Primzahl größer 2^{224} ist:
26959946667150639794667015087019630673637144422540572481103610249951

Die Zahlen a, b und die Koordinaten von P, $a \cdot P$, $a \cdot b \cdot P$ etc. sind genauso groß!!

Diffie-Hellman-Schlüsselaustausch

Warum ist  $= (a \cdot b) \cdot P$ ein Geheimnis?

Elliptische Kurve ist über endl. Körper mit p Elementen definiert, wobei p

in Binärschreibweise 224 Ziffern haben sollte,
im Dezimalsystem 68 Ziffern haben sollte.

Die kleinste Primzahl größer 2^{224} ist:
26959946667150639794667015087019630673637144422540572481103610249951

Die Zahlen a, b und die Koordinaten von P, $a \cdot P$, $a \cdot b \cdot P$ etc. sind genauso groß!!

Kann man damit überhaupt noch rechnen?

Diffie-Hellman-Schlüsselaustausch

Kann man mit so großen Zahlen überhaupt noch rechnen?

Diffie-Hellman-Schlüsselaustausch

Kann man mit so großen Zahlen überhaupt noch rechnen?

Antwort: ja und nein!

Diffie-Hellman-Schlüsselaustausch

Kann man mit so großen Zahlen überhaupt noch rechnen?

Antwort: ja und nein!

Ja: Ist a eine große Zahl und P ein Punkt auf der Kurve, dann kann man $a \cdot P$ sehr schnell ausrechnen.

Diffie-Hellman-Schlüsselaustausch

Kann man mit so großen Zahlen überhaupt noch rechnen?

Antwort: ja und nein!

Ja: Ist a eine große Zahl und P ein Punkt auf der Kurve, dann kann man $a \cdot P$ sehr schnell ausrechnen.

Beispiel: $103 = (1100111)_2 = 2^0 + 2^1 + 2^2 + 2^5 + 2^6$

$103 \cdot P = P + 2 \cdot P + 2 \cdot (2 \cdot P) + 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot P)))) + 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot P)))))$

Diffie-Hellman-Schlüsselaustausch

Kann man mit so großen Zahlen überhaupt noch rechnen?

Antwort: ja und nein!

Ja: Ist a eine große Zahl und P ein Punkt auf der Kurve, dann kann man $a \cdot P$ sehr schnell ausrechnen.

Beispiel: $103 = (1100111)_2 = 2^0 + 2^1 + 2^2 + 2^5 + 2^6$

$103 \cdot P = P + 2 \cdot P + 2 \cdot (2 \cdot P) + 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot P)))) + 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot P)))))$

Das sind maximal 2 Rechenoperationen pro Binärstelle, also nicht mehr als $2 \cdot 224 = 448$.

Diffie-Hellman-Schlüsselaustausch

Kann man mit so großen Zahlen überhaupt noch rechnen?

Antwort: ja und nein!

Ja: Ist a eine große Zahl und P ein Punkt auf der Kurve, dann kann man $a \cdot P$ sehr schnell ausrechnen.

Beispiel: $103 = (1100111)_2 = 2^0 + 2^1 + 2^2 + 2^5 + 2^6$
$103 \cdot P = P + 2 \cdot P + 2 \cdot (2 \cdot P) + 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot P)))) + 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot P)))))$

Das sind maximal 2 Rechenoperationen pro Binärstelle, also nicht mehr als $2 \cdot 224 = 448$.

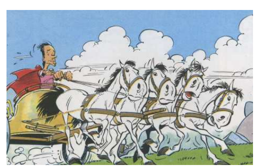
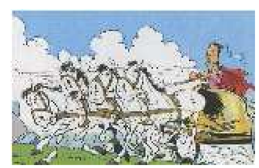
Nein: Kennt man nur P und $a \cdot P$, dann kann man a nicht ausrechnen (alle Computer der Welt bräuchten Jahre dafür)!!

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.

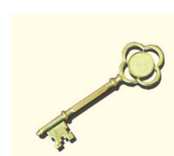

1. Wählt $a \in \mathbb{N}$.
2. Berechnet $a \cdot P$.
3. Verschickt $a \cdot P$.


1. Wählt $b \in \mathbb{N}$.
2. Berechnet $b \cdot P$.
3. Verschickt $b \cdot P$.

4. Empfängt $b \cdot P$.
5. Berechnet $a \cdot (b \cdot P)$.

4. Empfängt $a \cdot P$.
5. Berechnet $b \cdot (a \cdot P)$.

Gemeinsames Geheimnis:  $= (a \cdot b) \cdot P$.

Diffie-Hellman-Schlüsselaustausch

Also: Auch wenn der Bote mit $a \cdot P$ und/oder $b \cdot P$ abgefangen wird, kann man weder a noch b wissen.

Diffie-Hellman-Schlüsselaustausch

Also: Auch wenn der Bote mit $a \cdot P$ und/oder $b \cdot P$ abgefangen wird, kann man weder a noch b wissen.

Also: Niemand anderes kann $(a \cdot b) \cdot P$ herausfinden!!

Diffie-Hellman-Schlüsselaustausch

Also: Auch wenn der Bote mit $a \cdot P$ und/oder $b \cdot P$ abgefangen wird, kann man weder a noch b wissen.

Also: Niemand anderes kann $(a \cdot b) \cdot P$ herausfinden!!

Also ist  $= (a \cdot b) \cdot P$ ein gemeinsames Geheimnis!

Da hilft nur noch eins...

Kryptographie

Im neuen deutschen Reisepass werden elliptische Kurven benutzt.

Kryptographie

Im neuen deutschen Reisepass
werden elliptische Kurven benutzt.

Verwendung:

- Signieren der Daten (Echtheitsgarantie).
- Sichere Kommunikation mit dem Lesegerät.

Kryptographie

Verschlüsselungsverfahren:

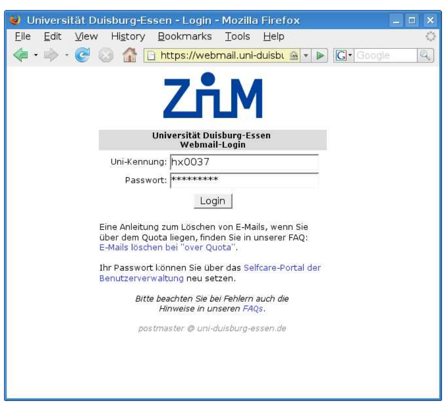
- Elliptische Kurven
- Abelsche Varietäten
- RSA
- Diskrete Logarithmen in endlichen Körpern (Diffie-Hellman)

Kryptographie

Verschlüsselungsverfahren:

- Elliptische Kurven
- Abelsche Varietäten
- RSA
- Diskrete Logarithmen in endlichen Körpern (Diffie-Hellman)

Anwendungen:



. . .

Zahlentheorie und Geometrie:

alltäglich und etwas Besonderes!!