Modulformen in Zahlentheorie und Geometrie

– vom Vierquadratesatz zum letzten Satz von Fermat –

Gabor Wiese

Universität Duisburg-Essen

Algebra und Zahlentheorie

Grundlegende Fragestellung:

Sei $\varphi(X) \in \mathbb{Z}[X]$ ein Polynom (irreduzibel und normiert).

Wie faktorisiert $\varphi(X)$ modulo Primzahlen?

Algebra und Zahlentheorie

Grundlegende Fragestellung:

Sei $\varphi(X) \in \mathbb{Z}[X]$ ein Polynom (irreduzibel und normiert).

Wie faktorisiert $\varphi(X)$ modulo Primzahlen?

- Erstes Beispiel: $\varphi(X) = X^2 + 1$.

Algebra und Zahlentheorie

Grundlegende Fragestellung:

Sei $\varphi(X) \in \mathbb{Z}[X]$ ein Polynom (irreduzibel und normiert).

Wie faktorisiert $\varphi(X)$ modulo Primzahlen?

- Erstes Beispiel: $\varphi(X) = X^2 + 1$.
- Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

Algebra und Zahlentheorie

Erstes Beispiel: $\varphi(X) = X^2 + 1$.

Algebra und Zahlentheorie

Erstes Beispiel: $\varphi(X) = X^2 + 1$.

p	Faktorisierung mod p
2	$(X+1)^2$
3	X^2+1
5	$(X+2)(X+3)$
7	X^2+1
11	X^2+1
13	$(X+5)(X+8)$
17	$(X+4)(X+13)$
19	X^2+1
23	X^2+1
29	$(X+12)(X+17)$
31	X^2+1

Algebra und Zahlentheorie

Erstes Beispiel: $\varphi(X) = X^2 + 1$.

p	Faktorisierung mod p
2	$(X+1)^2$
3	X^2+1
5	$(X+2)(X+3)$
7	X^2+1
11	X^2+1
13	$(X+5)(X+8)$
17	$(X+4)(X+13)$
19	X^2+1
23	X^2+1
29	$(X+12)(X+17)$
31	X^2+1

$p \equiv 1 \mod 4 \Leftrightarrow$ 2 Faktoren.

$p \equiv 3 \mod 4 \Leftrightarrow$ 1 Faktor.

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

p	Faktorisierung mod p
5	$(X^2+3)(X^2+X+1)(X^2+4X+1)$
13	$(X^3+10X+4)(X^3+10X+9)$
17	$(X^2+3)(X^2+2X+6)(X^2+15X+6)$
19	$(X^2+9)(X^2+X+12)(X^2+18X+12)$
31	$(X^3+28X+15)(X^3+28X+16)$
47	$(X^3+44X+20)(X^3+44X+27)$
53	$(X^2+22)(X^2+5X+25)(X^2+48X+25)$
59	$(X+9)(X+21)(X+29)(X+30)(X+38)(X+50)$
73	$(X^3+70X+14)(X^3+70X+59)$
97	$(X^2+39)(X^2+41X+42)(X^2+56X+42)$
101	$(X+4)(X+28)(X+32)(X+69)(X+73)(X+97)$

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

p	Faktorisierung mod p
5	$()()()$
13	$()()$
17	$()()()$
19	$()()()$
31	$()()$
47	$()()$
53	$()()()$
59	$()()()()()()$
73	$()()$
97	$()()()$
101	$()()()()()()$

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

Betrachte nun eine bestimmte Modulform

$$f(z) = e^{2\pi i z} + \sum_{n=2}^{\infty} a_n \, e^{2\pi i n z},$$

eine Hecke-Eigenspitzenform von Gewicht 7 und Stufe 23.

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

Betrachte nun eine bestimmte Modulform

$$f(z) = e^{2\pi i z} + \sum_{n=2}^{\infty} a_n \, e^{2\pi i n z},$$

eine Hecke-Eigenspitzenform von Gewicht 7 und Stufe 23.

Die a_n sind ganze algebraische Zahlen.

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

Betrachte nun eine bestimmte Modulform

$$f(z) = e^{2\pi iz} + \sum_{n=2}^{\infty} a_n \, e^{2\pi inz},$$

eine Hecke-Eigenspitzenform von Gewicht 7 und Stufe 23.

Die a_n sind ganze algebraische Zahlen.

Beispiel: a_{11} ist Nullstelle des Polynoms

$$x^8 + 11694708x^6 + 43659862073820x^4$$
$$+55081049334486544800x^2 + 17925962078516662247616000.$$

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

Betrachte nun eine bestimmte Modulform

$$f(z) = e^{2\pi i z} + \sum_{n=2}^{\infty} a_n \, e^{2\pi i n z},$$

eine Hecke-Eigenspitzenform von Gewicht 7 und Stufe 23.

Die a_n sind ganze algebraische Zahlen.

Beispiel: a_{11} ist Nullstelle des Polynoms

$$x^8 + 11694708x^6 + 43659862073820x^4$$
$$+55081049334486544800x^2 + 179259620785166622476160000.$$

7 ist total verzweigt in dem Koeffizientenkörper.

Sei $\overline{a_n}$ die Reduktion von a_n modulo (Ideal über) 7.

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

p	Faktoris. mod p
5	$()()()$
13	$()()$
17	$()()()$
19	$()()()$
31	$()()$
47	$()()$
53	$()()()$
59	$()()()()()()$
73	$()()$
97	$()()()$
101	$()()()()()()$

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

p	Faktoris. mod p	$\overline{a_p}$
5	$()()()$	0
13	$()()$	-1
17	$()()()$	0
19	$()()()$	0
31	$()()$	-1
47	$()()$	-1
53	$()()()$	0
59	$()()()()()()$	2
73	$()()$	-1
97	$()()()$	0
101	$()()()()()()$	2

INSTITUT FÜR EXPERIMENTELLE MATHEMATIK

Algebra und Zahlentheorie

Zweites Beispiel: $\varphi(X) = X^6 - 6X^4 + 9X^2 + 23$.

p	Faktoris. mod p	$\overline{a_p}$
5	()()()	0
13	()()	-1
17	()()()	0
19	()()()	0
31	()()	-1
47	()()	-1
53	()()()	0
59	()()()()()()	2
73	()()	-1
97	()()()	0
101	()()()()()()	2

$\overline{a_p} = 0 \quad \Leftrightarrow$ 3 Faktoren.

$\overline{a_p} = -1 \quad \Leftrightarrow$ 2 Faktoren.

$\overline{a_p} = 2 \quad \Leftrightarrow$ 6 Faktoren.

Zurück an die Tafel...

Elliptische Kurven

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

$$y^2 = x^3 + ax^2 + bx + c$$

(ohne Selbstdurchschneidungen u. Ä.)

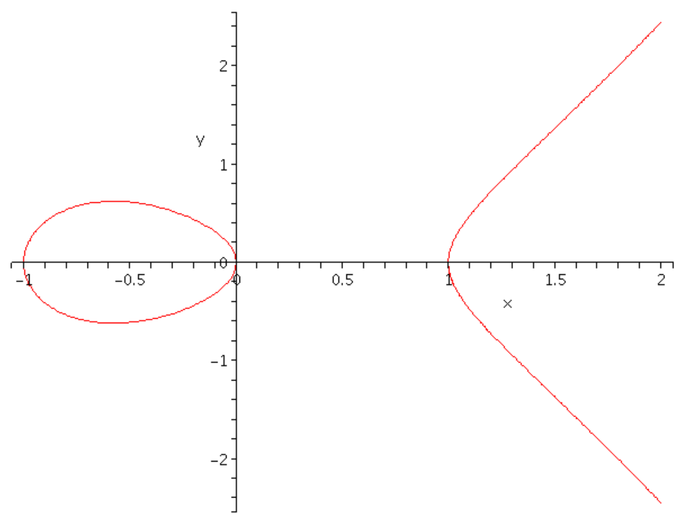
Elliptische Kurven

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

$$y^2 = x^3 + ax^2 + bx + c$$

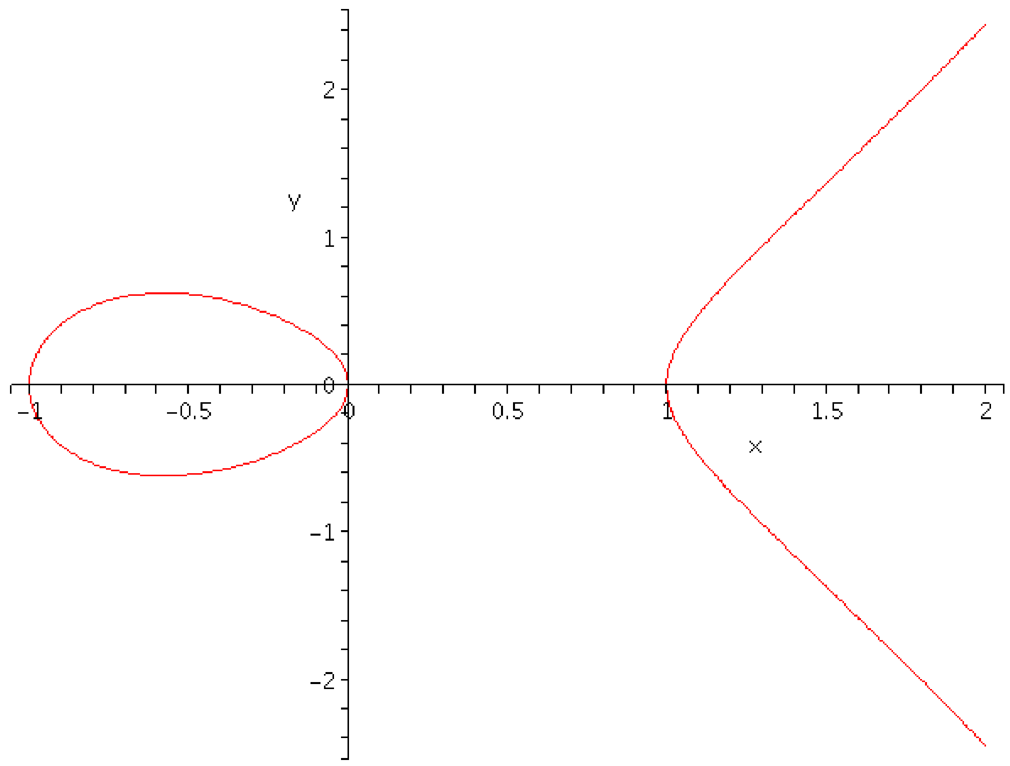
(ohne Selbstdurchschneidungen u. Ä.)

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



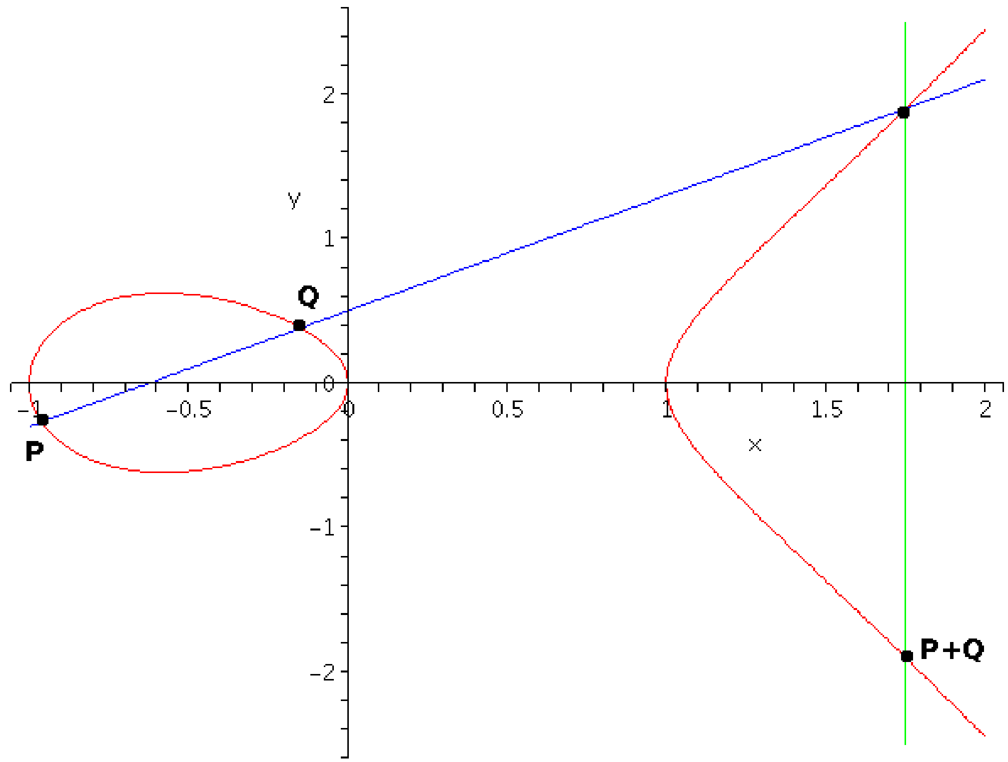
Elliptische Kurven - Addition

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!