Der Satz von Hasse-Weil und Anwendungen

Philipp Heßler

Technische Universität Kaiserslautern

23. Mai 2011

Gliederung

Motivation

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_2)$?

Motivation

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_2)$?

x	$x^3 + 1$	$y^2 + xy$	y	Punkte

Motivation

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_2)$?

x	x^3+1	y^2+xy	y	Punkte
0	1	y^2	1	$(0,1)$

Motivation

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_2)$?

x	x^3+1	y^2+xy	y	Punkte
0	1	y^2	1	$(0,1)$
1	0	y^2+y	0	$(1,0)$

Motivation

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_2)$?

x	x^3+1	y^2+xy	y	Punkte
0	1	y^2	1	$(0,1)$
1	0	y^2+y	0	$(1,0)$
			1	$(1,1)$

Motivation

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_2)$?

x	x^3+1	y^2+xy	y	Punkte
0	1	y^2	1	$(0,1)$
1	0	y^2+y	0	$(1,0)$
			1	$(1,1)$
O			**O**	**O**

Motivation

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_2)$?

x	x^3+1	y^2+xy	y	Punkte
0	1	y^2	1	$(0,1)$
1	0	y^2+y	0	$(1,0)$
			1	$(1,1)$
O			**O**	**O**

$E(\mathbb{F}_2)$ hat also 4 Elemente.

Motivation

Beispiel

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_4)$?

Motivation

Beispiel

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_4)$?

x	x^3+1	y^2+xy	y	Punkte
0	1	y^2	1	$(0,1)$
1	0	y^2+y	0	$(1,0)$
			1	$(1,1)$
ω	0	$y^2+\omega y$	0	$(\omega,0)$
			ω	(ω,ω)
ω^2	0	$y^2+\omega^2 y$	0	$(\omega^2,0)$
			ω^2	(ω^2,ω^2)
$\mathbf{O}$			$\mathbf{O}$	$\mathbf{O}$

Motivation

Beispiel

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_4)$?

x	x^3+1	y^2+xy	y	Punkte
0	1	y^2	1	$(0,1)$
1	0	y^2+y	0	$(1,0)$
			1	$(1,1)$
ω	0	$y^2+\omega y$	0	$(\omega,0)$
			ω	(ω,ω)
ω^2	0	$y^2+\omega^2 y$	0	$(\omega^2,0)$
			ω^2	(ω^2,ω^2)
$\mathbf{O}$			$\mathbf{O}$	$\mathbf{O}$

$E(\mathbb{F}_2)$ hat also 8 Elemente.

Motivation

Beispiel

Wie viele Elemente hat die Gruppe $E(\mathbb{F}_{2^{101}})$?

Motivation

Satz von Hasse-Weil

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a := q + 1 - \#E(\mathbb{F}_q)$. Dann gilt:

$$|a| \leq 2\sqrt{q}$$

Motivation

Satz von Hasse-Weil

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a := q + 1 - \#E(\mathbb{F}_q)$. Dann gilt:

$$|a| \leq 2\sqrt{q}$$

Sei $x^2 - ax + q = (x - \alpha)(x - \beta)$. Dann gilt für alle $n \geq 1$:

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

Frobenius Endomorphismus

Definition

Sei $\mathbb{F}_q$ ein endlicher Körper mit algebraischem Abschluss $\overline{\mathbb{F}_q}$. Die Frobenius-Abbildung $\phi_q : \overline{\mathbb{F}_q} \longrightarrow \overline{\mathbb{F}_q}$ ist definiert durch $\phi_q(x) := x^q$.

Frobenius Endomorphismus

Definition

Sei $\mathbb{F}_q$ ein endlicher Körper mit algebraischem Abschluss $\overline{\mathbb{F}_q}$. Die Frobenius-Abbildung $\phi_q : \overline{\mathbb{F}_q} \longrightarrow \overline{\mathbb{F}_q}$ ist definiert durch $\phi_q(x) := x^q$.

Auf elliptischen Kurven gilt $\phi_q(x, y) = (x^q, y^q)$ und $\phi_q(\mathbf{O}) = \mathbf{O}$.

Frobenius Endomorphismus

Definition

Sei $\mathbb{F}_q$ ein endlicher Körper mit algebraischem Abschluss $\overline{\mathbb{F}_q}$. Die Frobenius-Abbildung $\phi_q : \overline{\mathbb{F}_q} \longrightarrow \overline{\mathbb{F}_q}$ ist definiert durch $\phi_q(x) := x^q$.

Auf elliptischen Kurven gilt $\phi_q(x, y) = (x^q, y^q)$ und $\phi_q(\mathbf{O}) = \mathbf{O}$.

Lemma

ϕ_q ist ein Endomorphismus von E vom Grad q und nicht separabel.

Frobenius Endomorphismus

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_4$ gegeben durch $y^2 + xy = x^3 + 1$.

(x, y)	$\Phi_q(x, y)$
$(0, 1)$	
$(1, 0)$	
$(1, 1)$	
$(\omega, 0)$	
(ω, ω)	
$(\omega^2, 0)$	
(ω^2, ω^2)	
$\mathbf{O}$	

Frobenius Endomorphismus

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_4$ gegeben durch $y^2 + xy = x^3 + 1$.

(x, y)	$\Phi_q(x, y)$
$(0, 1)$	$(0, 1)$
$(1, 0)$	$(1, 0)$
$(1, 1)$	$(1, 1)$
$(\omega, 0)$	$(\omega, 0)$
(ω, ω)	(ω, ω)
$(\omega^2, 0)$	$(\omega^2, 0)$
(ω^2, ω^2)	(ω^2, ω^2)
$\mathbf{O}$	$\mathbf{O}$

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Beweis

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Beweis

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

$$y^2 + a_1xy + a_3y \qquad = \qquad x^3 + a_2x^2 + a_4x + a_6$$

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Beweis

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

$$\begin{array}{rcc} & y^2 + a_1xy + a_3y & = & x^3 + a_2x^2 + a_4x + a_6 \\ \Longrightarrow & (y^2 + a_1xy + a_3y)^q & = & (x^3 + a_2x^2 + a_4x + a_6)^q \end{array}$$

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Beweis

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

$$\begin{array}{rcrcl} & & y^2 + a_1xy + a_3y & = & x^3 + a_2x^2 + a_4x + a_6 \\ \implies & & (y^2 + a_1xy + a_3y)^q & = & (x^3 + a_2x^2 + a_4x + a_6)^q \\ \implies & & (y^2)^q + (a_1xy)^q + (a_3y)^q & = & (x^3)^q + (a_2x^2)^q + (a_4x)^q + (a_6)^q \end{array}$$

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Beweis

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

$$
\begin{array}{rcrcl}
 & & y^2 + a_1xy + a_3y & = & x^3 + a_2x^2 + a_4x + a_6 \\
\implies & & (y^2 + a_1xy + a_3y)^q & = & (x^3 + a_2x^2 + a_4x + a_6)^q \\
\implies & & (y^2)^q + (a_1xy)^q + (a_3y)^q & = & (x^3)^q + (a_2x^2)^q + (a_4x)^q + (a_6)^q \\
\implies & & (y^q)^2 + a_1x^qy^q + a_3y^q & = & (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6
\end{array}
$$

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Beweis

$$(x, y) \in E(\mathbb{F}_q)$$

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Beweis

$$\begin{array}{ccc} & & (x, y) \in E(\mathbb{F}_q) \\ \iff & & x, y \in \mathbb{F}_q \end{array}$$

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Beweis

$$\begin{aligned} & (x, y) \in E(\mathbb{F}_q) \\ \iff \quad & x, y \in \mathbb{F}_q \\ \iff \quad & \Phi_q(x) = x, \Phi_q(y) = y \end{aligned}$$

Frobenius Endomorphismus

Lemma

Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:

1. $\Phi_q(x, y) \in E(\overline{\mathbb{F}_q})$
2. $(x, y) \in E(\mathbb{F}_q) \iff \Phi_q(x, y) = (x, y)$

Beweis

$$
\begin{aligned}
& (x, y) \in E(\mathbb{F}_q) \\
\iff \quad & x, y \in \mathbb{F}_q \\
\iff \quad & \Phi_q(x) = x, \Phi_q(y) = y \\
\iff \quad & \Phi_q(x, y) = (x, y)
\end{aligned}
$$

□

Frobenius Endomorphismus

Proposition

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $n \geq 1$. Dann gilt:

Frobenius Endomorphismus

Proposition

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $n \geq 1$. Dann gilt:

1. $\ker(\phi_q - 1) = E(\mathbb{F}_q)$

Frobenius Endomorphismus

Proposition

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $n \geq 1$. Dann gilt:

1. $\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$

Frobenius Endomorphismus

Proposition

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $n \geq 1$. Dann gilt:

1. $\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$
2. $\phi_q^n - 1$ ist ein separabler Endomorphismus, also gilt:

$$\deg(\phi_q^n - 1) = \#\ker(\phi_q^n - 1) = \#E(\mathbb{F}_{q^n})$$

Frobenius Endomorphismus

Proposition

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $n \geq 1$. Dann gilt:

1. $\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$
2. $\phi_q^n - 1$ ist ein separabler Endomorphismus, also gilt:

$$\deg(\phi_q^n - 1) = \#\ker(\phi_q^n - 1) = \#E(\mathbb{F}_{q^n})$$

Beweis

Mündlich.

Beweis Satz von Hasse-Weil

Lemma

Seien $r, s \in \mathbb{Z}$ mit $\gcd(s, q) = 1$. Dann gilt:

$$\deg(r\phi_q - s) = r^2 q + s^2 - rsa$$

Beweis Satz von Hasse-Weil

Lemma

Seien $r, s \in \mathbb{Z}$ mit $\gcd(s, q) = 1$. Dann gilt:

$$\deg(r\phi_q - s) = r^2 q + s^2 - rsa$$

Beweis

Siehe Ausarbeitung.

Beweis Satz von Hasse-Weil

Lemma

Seien $r, s \in \mathbb{Z}$ mit $\gcd(s, q) = 1$. Dann gilt:

$$\deg(r\phi_q - s) = r^2 q + s^2 - rsa$$

Beweis

Siehe Ausarbeitung.

Satz von Hasse-Weil (1. Teil)

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a := q + 1 - \#E(\mathbb{F}_q)$. Dann gilt:

$$|a| \leq 2\sqrt{q}$$

Beweis Satz von Hasse-Weil

Lemma

Seien $r, s \in \mathbb{Z}$ mit $\gcd(s, q) = 1$. Dann gilt:

$$\deg(r\phi_q - s) = r^2 q + s^2 - rsa$$

Beweis

Siehe Ausarbeitung.

Satz von Hasse-Weil (1. Teil)

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a := q + 1 - \#E(\mathbb{F}_q)$. Dann gilt:

$$|a| \leq 2\sqrt{q}$$

Beweis

Siehe Tafel.

Beweis Satz von Hasse-Weil

Theorem

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a = q + 1 - \#E(\mathbb{F}_q)$. Dann ist $\phi_q^2 - a\phi_q + q = 0$ als Endomorphismus auf E und a ist die eindeutige ganze Zahl mit dieser Eigenschaft.

Außerdem gilt $a \equiv \mathrm{Trace}((\Phi_q)_m) \bmod m$ für $\gcd(m, q) = 1$.

Beweis Satz von Hasse-Weil

Theorem

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a = q + 1 - \#E(\mathbb{F}_q)$. Dann ist $\phi_q^2 - a\phi_q + q = 0$ als Endomorphismus auf E und a ist die eindeutige ganze Zahl mit dieser Eigenschaft.

Außerdem gilt $a \equiv \text{Trace}((\Phi_q)_m) \bmod m$ für $\gcd(m, q) = 1$.

Beweis

Siehe Tafel.

Beweis Satz von Hasse-Weil

Theorem

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a = q + 1 - \#E(\mathbb{F}_q)$. Dann ist $\phi_q^2 - a\phi_q + q = 0$ als Endomorphismus auf E und a ist die eindeutige ganze Zahl mit dieser Eigenschaft.

Außerdem gilt $a \equiv \text{Trace}((\Phi_q)_m) \bmod m$ für $\gcd(m, q) = 1$.

Beweis

Siehe Tafel.

Lemma

Sei $s_n = \alpha^n + \beta^n$. Dann ist $s_0 = 2$, $s_1 = a$ und $s_{n+1} = as_n - qs_{n-1}$.

Beweis Satz von Hasse-Weil

Theorem

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a = q + 1 - \#E(\mathbb{F}_q)$. Dann ist $\phi_q^2 - a\phi_q + q = 0$ als Endomorphismus auf E und a ist die eindeutige ganze Zahl mit dieser Eigenschaft.

Außerdem gilt $a \equiv \text{Trace}((\Phi_q)_m) \bmod m$ für $\gcd(m, q) = 1$.

Beweis

Siehe Tafel.

Lemma

Sei $s_n = \alpha^n + \beta^n$. Dann ist $s_0 = 2$, $s_1 = a$ und $s_{n+1} = as_n - qs_{n-1}$.

Beweis

Siehe Ausarbeitung.

Beweis Satz von Hasse-Weil

Satz von Hasse-Weil (2. Teil)

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a_1 := q + 1 - \#E(\mathbb{F}_q)$. Sei weiter $x^2 - a_1 x + q = (x - \alpha)(x - \beta)$. Dann gilt für alle $n \geq 1$:

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

Beweis Satz von Hasse-Weil

Satz von Hasse-Weil (2. Teil)

Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a_1 := q + 1 - \#E(\mathbb{F}_q)$. Sei weiter $x^2 - a_1 x + q = (x - \alpha)(x - \beta)$. Dann gilt für alle $n \geq 1$:

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

Beweis

Siehe Tafel.

Anwendung

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Anwendung

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wir wissen $q = 2$, $\#E(\mathbb{F}_2) = 4$, also $a = q + 1 - \#E(\mathbb{F}_q) = -1$.

Anwendung

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wir wissen $q = 2$, $\#E(\mathbb{F}_2) = 4$, also $a = q + 1 - \#E(\mathbb{F}_q) = -1$.

$$x^2 + x + 2 = \left(x - \frac{-1 + \sqrt{-7}}{2}\right)\left(x - \frac{-1 - \sqrt{-7}}{2}\right)$$

Anwendung

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wir wissen $q = 2$, $\#E(\mathbb{F}_2) = 4$, also $a = q + 1 - \#E(\mathbb{F}_q) = -1$.

$$x^2 + x + 2 = \left(x - \frac{-1 + \sqrt{-7}}{2}\right)\left(x - \frac{-1 - \sqrt{-7}}{2}\right)$$

Wieviele Elemente hat $E(\mathbb{F}_4)$?

Anwendung

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wir wissen $q = 2$, $\#E(\mathbb{F}_2) = 4$, also $a = q + 1 - \#E(\mathbb{F}_q) = -1$.

$$x^2 + x + 2 = \left(x - \frac{-1 + \sqrt{-7}}{2}\right)\left(x - \frac{-1 - \sqrt{-7}}{2}\right)$$

Wieviele Elemente hat $E(\mathbb{F}_4)$?

$$\#E(\mathbb{F}_4) = 4 + 1 - \left(\frac{-1 + \sqrt{-7}}{2}\right)^2 - \left(\frac{-1 - \sqrt{-7}}{2}\right)^2 = 8$$

Anwendung

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wir wissen $q = 2$, $\#E(\mathbb{F}_2) = 4$, also $a = q + 1 - \#E(\mathbb{F}_q) = -1$.

$$x^2 + x + 2 = \left(x - \frac{-1 + \sqrt{-7}}{2}\right)\left(x - \frac{-1 - \sqrt{-7}}{2}\right)$$

Anwendung

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wir wissen $q = 2$, $\#E(\mathbb{F}_2) = 4$, also $a = q + 1 - \#E(\mathbb{F}_q) = -1$.

$$x^2 + x + 2 = \left(x - \frac{-1 + \sqrt{-7}}{2}\right)\left(x - \frac{-1 - \sqrt{-7}}{2}\right)$$

Wieviele Elemente hat $E(\mathbb{F}_{2^{101}})$?

Anwendung

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wir wissen $q = 2$, $\#E(\mathbb{F}_2) = 4$, also $a = q + 1 - \#E(\mathbb{F}_q) = -1$.

$$x^2 + x + 2 = \left(x - \frac{-1 + \sqrt{-7}}{2}\right)\left(x - \frac{-1 - \sqrt{-7}}{2}\right)$$

Wieviele Elemente hat $E(\mathbb{F}_{2^{101}})$?

$$\#E(\mathbb{F}_{2^{101}}) \;=\; 2^{101} + 1 - \left(\frac{-1 + \sqrt{-7}}{2}\right)^{101} - \left(\frac{-1 - \sqrt{-7}}{2}\right)^{101}$$

Anwendung

Beispiel

Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2 + xy = x^3 + 1$.

Wir wissen $q = 2$, $\#E(\mathbb{F}_2) = 4$, also $a = q + 1 - \#E(\mathbb{F}_q) = -1$.

$$x^2 + x + 2 = \left(x - \frac{-1 + \sqrt{-7}}{2}\right)\left(x - \frac{-1 - \sqrt{-7}}{2}\right)$$

Wieviele Elemente hat $E(\mathbb{F}_{2^{101}})$?

$$\begin{aligned} \#E(\mathbb{F}_{2^{101}}) &= 2^{101} + 1 - \left(\frac{-1 + \sqrt{-7}}{2}\right)^{101} - \left(\frac{-1 - \sqrt{-7}}{2}\right)^{101} \\ &= 2535301200456455833701195805484 \end{aligned}$$

Fazit

- $\#E(\mathbb{F}_q)$ lässt sich abschätzen.

Fazit

- $\#E(\mathbb{F}_q)$ lässt sich abschätzen.
- $\#E(\mathbb{F}_{q^n})$ lässt sich berechnen, falls $\#E(\mathbb{F}_q)$ bekannt ist und E über $\mathbb{F}_q$ definiert ist.

Fazit

- $\#E(\mathbb{F}_q)$ lässt sich abschätzen.
- $\#E(\mathbb{F}_{q^n})$ lässt sich berechnen, falls $\#E(\mathbb{F}_q)$ bekannt ist und E über $\mathbb{F}_q$ definiert ist.

Vielen Dank für eure Aufmerksamkeit