

Blatt 10, Aufg 2 : n -Torsionspunkte auf einer elliptischen Kurve

Ist G eine abelsche Gruppe und $n \in \mathbb{N}$, so bilden die Punkte endlicher Ordnung, also

$G_T := \{a \in G \mid \exists n \in \mathbb{N} : na = 0\}$ eine Untergruppe von G , die sogenannte Torsionsuntergruppe.

Für jedes $n \in \mathbb{N}$ sind die Mengen $G_n := \{a \in G \mid na = 0\}$ ihrerseits wieder Untergruppen von

G_T ; ein Element von G_n nennt man n -Torsionspunkt von G . Ist m ein Teiler von n , so ist

G_m Untergruppe von G_n . Für $G = \mathbb{Z}$ ist $T_G = \{0\}$, und insbesondere für endliche Gruppen

ist $T_G = G$. Für $G = \mathbb{R}^*$ ist $T_G = \{-1, 1\}$. Ist $\zeta_n = \exp\left(\frac{2\pi i}{n}\right)$ eine primitive n -te Einheits-

wurzel in \mathbb{C} , so gilt für $G = \mathbb{C}^*$: $G_n = \{\zeta_n^k \mid 0 \leq k < n\}$. Die Torsionsuntergruppen verraten viel über die Struktur einer abelschen Gruppe.

Es liegt daher nahe, die Torsionsuntergruppen einer elliptischen Kurve zu untersuchen.

Dazu gehen wir aus von einem Grundkörper K mit $\text{char } K \neq 2, 3$, denn in diesem Fall ist jede elliptische Kurve \mathcal{C} über K gegeben durch eine Gleichung $y^2 = x^3 + ax + b$, und wir kennen

Formeln für die Addition auf \mathcal{C} . Die Additionsformeln sind rationale Ausdrücke in den

Koordinaten der zu addierenden Punkte, daher ist auch nP ein rationaler Ausdruck in den

Koordinaten von P , falls nicht $nP = 0$. Konkreter: Ist $P = (x, y)$, $n \in \mathbb{N}$ und $nP \neq 0$, so gibt es

Polynome $\vartheta_n(x, y), \theta_n(x, y), \varphi_n(x, y), \psi_n(x, y) \in K[x, y]$ mit $nP = \left(\frac{\vartheta_n(x, y)}{\varphi_n(x, y)}, \frac{\theta_n(x, y)}{\psi_n(x, y)}\right)$.

Dies beweist man leicht durch Induktion über n , ohne dabei die konkrete Gestalt dieser Polynome bestimmen zu müssen.

Analysiert man die Situation genauer, so ergibt sich folgende Rekursion, deren Korrektheit man anschließend wieder induktiv durch konkretes Nachrechnen beweist:

Es gibt Polynome $\chi_n(x, y) \in K[x, y]$, so daß $\varphi_n = \chi_n^2, \psi_n = \chi_n^3$, wobei

$$\chi_0 = 0, \chi_1 = 1,$$

$$\chi_2(x, y) = 2y, \chi_3(x, y) = 3x^4 + 6ax^2 + 12bx - a^2,$$

$$\chi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),$$

$$\chi_{2m+1} = \chi_{m+2}\chi_m^3 - \chi_{m-1}\chi_{m+1}^3 \quad \text{für } m \geq 2,$$

$$\chi_{2m} = \frac{(\chi_{m+2}\chi_{m-1}^2 - \chi_{m-2}\chi_{m+1}^2)\chi_m}{2y} \quad \text{für } m > 2.$$

sowie

$$\vartheta_m = x\chi_m^2 - \chi_{m-1}\chi_{m+1} \quad \text{für } m \geq 1,$$

$$\theta_m = \frac{\chi_{2m}}{2\chi_m} \quad \text{für } m \geq 1.$$

Die in den Rekursionsformeln auftretenden Polynomdivisionen gehen immer auf.

Jetzt erwartet man, und zeigt auch leicht, daß ein Punkt $Q = (x, y)$ auf der Kurve genau dann ein n -Torsionspunkt ist, wenn $\chi_n(x, y) = 0$.

Es erweist sich als praktisch, eine entsprechende Aussage mit Hilfe eines Polynoms in nur einer Variablen treffen zu können. Es stellt sich heraus, daß für ungerades n die Polynome χ_n gar nicht

von y abhängen. Für gerades n hat man $\chi_2 | \chi_n$ und $\frac{\chi_n}{\chi_2}$ hängt ebenfalls nicht von y ab. Man setze

$$\text{also } f_n := \begin{cases} \chi_n & n \text{ ungerade} \\ \frac{\chi_n}{\chi_2} & n \text{ gerade} \end{cases} .$$

Damit gilt:

Für $n \geq 2$ ist ein Punkt $Q=(x, y)$ auf der Kurve genau dann ein n -Torsionspunkt, wenn $f_n(x)=0$ bzw. wenn n gerade und Q ein 2-Torsionspunkt ist, also $y=0$.

Jetzt erhält man durch Induktion die folgenden Rekursionsformeln für f_n

$$f_0=0, f_1=1, f_2=1, f_3=3x^4+6ax^2+12bx-a^3, \\ f_4=2(x^6+5ax^4+20bx^3-5a^2x^2-4abx-8b^2-a^3) ;$$

mit $F(x):=4(x^3+ax+b)$ ist

$$f_{2m+1} = \begin{cases} f_{m+2}f_m^3 - F^2 f_{m-1}f_{m+1}^3 & \text{für } m \text{ ungerade } m \geq 3 \\ F^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3 & \text{für } m \text{ gerade } m \geq 2 \end{cases}$$

$$f_{2m} = (f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2) f_m \quad \text{für } m > 2 .$$

Welchen Grad f_n besitzt, hängt von der Charakteristik von K ab. Rechnet man in Charakteristik 0, so besitzt z.B. f_5 den Grad 12 und der Leitkoeffizient ist 5, wie man sich mittels des unten stehenden Pari-Programms überzeugt. Offenbar hat dann in Charakteristik 5 f_5 einen kleineren Grad. Außerdem besitzt f_n keine mehrfachen Nullstellen. Dies ist im Folgenden wichtig, wir zeigen es aber leider nicht.

Damit kommen wir zu Blatt 10, Aufgabe 2:

Dort gehen wir vom algebraisch vollständigen Körper \mathbb{C} der Charakteristik 0 aus. Man beweist mittels der Rekursionsformeln für f_n leicht durch Induktion, daß für ungerades $n \geq 3$ f_n den Grad $\frac{n^2-1}{2}$ und daher ebensoviele Nullstellen besitzt. Da für jeden n -Torsionspunkt $P=(x, y)$

$y \neq 0$ gilt und daher die $-P=(x, -y)$ weitere n -Torsionspunkte sind, gibt es insgesamt n^2 n -Torsionspunkte, denn man muß ja zusätzlich den 0-Punkt mitzählen.

Für gerades n besitzt f_n den Grad $\frac{n^2-4}{2}$ und daher ebensoviele Nullstellen. Für n -Torsionspunkte $P=(x, y)$, welche keine 2-Torsionspunkte sind, ist $y \neq 0$ und daher auch $-P=(x, -y)$ ein n -Torsionspunkt. Genau die x -Komponenten dieser n -Torsionspunkte ergeben sich als Nullstellen von f_n . Zählen wir jetzt 0 und die drei weiteren 2-Torsionspunkte hinzu, so haben wir auch in diesem Fall insgesamt n^2 n -Torsionspunkte.

Zusammenfassung: Eine elliptische Kurve über \mathbb{C} besitzt n^2 n -Torsionspunkte.

Bemerkungen:

a) Mittels obiger Rekursionsformeln läßt sich leicht ein Pari-Programm schreiben, welches die f_n auch für große n berechnet:

$$F=4*x^3 + 4*a*x + 4*b;$$

```
f(n) =
{
  local(m=n\2);
  if(n==0,return(0));
  if(n==1,return(1));
  if(n==2,return(1));
  if(n==3,return(3*x^4+6*a*x^2+12*b*x-a^2));
  if(n==4,return(2*(x^6+5*a*x^4+20*b*x^3-5*a^2*x^2-4*a*b*x-8*b^2-a^3)));

  if(n%2,
    if(m%2,return(f(m+2)*f(m)^3-F^2*f(m-1)*f(m+1)^3),
      return(F^2*f(m+2)*f(m)^3-f(m-1)*f(m+1)^3);
    ),
    return((f(m+2)*f(m-1)^2-f(m-2)*f(m+1)^2)*f(m));
  );
}
```

Nachdem f_n berechnet ist, kann man das Ergebnis etwas übersichtlicher gestalten und konkrete Werte für a, b einsetzen, indem man z.B. $y^2=(x-1)x(x+1)=x^3-x$, also $a=-1$ und $b=0$ wählt.

b) Eigentlich ist die konkrete Gestalt der f_n , die mit den Rekursionsformeln hergeleitet wird, für die Gradbestimmung am Schluß gar nicht nötig. Man könnte also probieren, nur die Grade der f_n rekursiv zu bestimmen.

c) Ein ganz anderer Beweis dafür, daß die n -Torsionsgruppe einer elliptischen Kurve über \mathbb{C} die Ordnung n^2 besitzt, wäre vielleicht schöner.

d) Die obigen Überlegungen stützen sich auf das Kapitel „Divisionspolynome“ im Buch von Blake, Seroussi, Smart „Elliptic Curves in Cryptography“.