Elliptische Kurven

Inhalt

1. Beispiele
2. PARI/GP Befehle
3. Vergleich: $\mathbb{Z}_p^*$ vs ellitpische Kurven

Recap

Formeln für Addition

Für Punkte $P = (x_1; y_1)$ und $Q = (x_2; y_2)$ auf der Kurve gilt:

a) Falls $x_1 \neq x_2$:

$m := \frac{y_2 - y_1}{x_2 - x_1}$, $\quad x_3 := m^2 - x_1 - x_2$, $\quad y_3 := -m(x_3 - x_1) - y_1$ und

$P + Q := (x_3; y_3)$

b) Falls $x_1 = x_2$ und $y_1 = y_2 \neq 0$:

$m := \frac{3x_1^2 + a}{2y_1}$, $\quad x_3 := m^2 - 2x_1$, $\quad y_3 := -m(x_3 - x_1) - y_1$ und

$P + Q := (x_3; y_3)$

c) Falls $x_1 = x_2$ und $y_1 = -y_2$ setzen wir $P + Q := O$.

d) $P + O = O + P = P$.

Bem: $2P = P + P$

Beispiele

Notation: $E_{a,b}$ bezeichnet die Elemente der elliptischen Kurve der Form $y^2 = x^3 + ax + b$.

Erinnerung Euler-Kriterium:

$a \in \mathbb{Z}_p$ hat eine Quadratwurzel $\Leftrightarrow a^{\frac{p-1}{2}} = 1 \pmod{p}$

Aufgaben:

- Wir betrachten die elliptische Kurve $y^2 = x^3 + x + 6$ über GF(11). Bestimme $E_{1,6}$.

Beispiele

Aufgaben (Fortsetzung)

- Wir betrachten wieder die Kurve $y^2 = x^3 + x + 6$ über GF(11). Bestimme
  - (i) $(2, 4) + (5, 9)$,
  - (ii) $(2, 4) + (2, 7)$,
  - (iii) $(2, 4) + (2, 4)$

PARI/GP Befehle

Recap:

- Allgemeine Form: $y^2 = x^3 + ax + b$ über $\mathbb{Z}_p$.
- Beispiel: $y^2 = x^3 + x + 6$ über $\mathbb{Z}_{11}$.

Befehle

- **ellinit**
  Aufruf: $E = \text{ellinit}([a,b],p)$ im Bsp: $E = \text{ellinit}([1,6],11)$
- **elladd**
  Aufruf: $\text{elladd}(E,[x_1, y_1], [x_2, y_2])$ z.B.: $\text{elladd}(E,[2,7],[3,6])$
- **ellpow**
  Aufruf: $\text{ellpow}(E,[x, y],n)$ z.B.: $\text{ellpow}(E, [2,4], 2)$

Vergleich: $\mathbb{Z}_p^*$ vs elliptische Kurve

Muliplikative Gruppe vs Additive Gruppe

	$\mathbb{Z}_p^*$	ell. Kurve
Potenz	g^x	$x \cdot P$
Ordnung	kleinstes n so dass $g^n = 1$	kleinstes n so dass $n \cdot P = 0$
Logarithmus	$g^x = a$	$x \cdot P = a$

Bem: $n \cdot P = P + P + \ldots + P$ (n Summanden)