Punktezahl für spezielle E

Kurven mit CM = complex mult.

man wählt eine Diskriminante D

⟶ Primzahl p

⟶ 2, 4 oder 6 Kurven E

und 2, 4 oder 6 Punktzahlen $|E|$

Beispiel:

(a_1, b_1) (a_2, b_2)

$|E_1|$ $|E_2|$

bekannt $\{|E_1|, |E_2|\}$

⟶ Zuordnungsproblem

dieses lösen mit der Eigenschaft

$$|E| \cdot P = \mathcal{O}$$

Methode von Crandall/Pomerance

1. Tabelle mit Diskriminanten

D	r	s
-3	—	—
-4	—	—
-7	125	189
-8	125	98
-11	512	539
-19	512	513

2. Primzahl p aus D bestimmen

$$4p = u^2 + |D| \cdot v^2$$

D	u	v	p
-3	1	3	7
-4	4	1	5
-7	4	2	11
-8	2	1	3
-11	4	6	103
-19	4	2	23

Beispiel

3. Quadratischen Nichtrest g mod p finden

Bedeutung: es darf kein y geben mit

$$y^2 \equiv g \bmod p$$

Kriterium: $\frac{p-1}{2}$

$$g \equiv -1 \bmod p$$

Fortführung des Beispiels:

$p = 11,\ u = 4,\ v = 2,\ D = -7$

Quadratischer Nichtrest, probiere $g = 2$

$$g^{\frac{11-1}{2}} \equiv 2^5 \equiv 10 \equiv -1 \bmod 11$$

$\rightarrow g = 2$ auswählen

Ergänzung:

falls $D = -3$ darf g auch kein kubischer Rest sein, d.h. g muss

$\frac{p-1}{3}$

$$g \not\equiv 1 \bmod p$$

erfüllen

4. mögliche Werte für $|E|$

$$p+1+u$$

$$p+1-u$$

im Beispiel

$p = 11$, $u = 4$

$p+1+u = 16$

$p+1-u = 8$

5. Fallunterscheidung nach D

$D = -3$:

$$y^2 \equiv x^3 - g^k \mod p, \quad 0 \le k \le 5$$

6 Kurven

$\Rightarrow$ 4 weitere $|E|$-Werte

$$p+1 \pm (u \pm 3v)/2$$

$D = -4$:

$$y^2 \equiv x^3 - g^k \cdot x \mod p, \quad 0 \le k \le 3$$

4 Kurven

$\Rightarrow$ 2 weitere $|E|$-Werte

$$p+1 \pm 2v$$

$D \notin \{-3, -4\}$:

benutze r, s aus Tabelle (Schritt 1)

$$y^2 \equiv x^3 - 3rs^3 g^{2k} x + 2rs^5 g^{3k} \mod p$$

für $k \in \{0, 1\}$