Kryptographisch verwendbare Kurven

Problem: $|E| \approx 2^{256}$

polynomieller Algorithmus zum Punktezählen

$O((\log p)^6)$ Schoof-Elkies-Atkin-Morain

Alternative: CM-Kurven

= elliptische Kurven mit komplexer Multiplikation

z.B. $E \leftrightarrow \mathbb{Z}[i]$

Hier Vorhersage der Punktezahl möglich.

Methode von Crandall/Pomerance.

1. Tabelle mit Diskriminanten und Parametern

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

2. Lösen einer quadratischen Gleichung abhängig von einem D-Wert und der Primzahl p

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

3. Quadratischen Nichtrest g mod p finden

[Spezialfall $D=-3$, g keine Kubikzahl]

$$g^{\frac{p-1}{2}} \equiv -1 \bmod p$$

[Spezialfall $D=-3$: $g^{\frac{p-1}{3}} \not\equiv 1 \bmod p$]

4. mögliche Werte für $|E|$ auflisten

$$p + 1 + u$$

$$p + 1 - u$$

5. falls $D = -3$:

6 Kurven bilden

$$y^2 \equiv x^3 - g^k \mod p$$

$$0 \leq k \leq 5$$

4 zusätzliche Werte für $|E|$

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

6. falls $D = -4$:

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

2 zusätzliche Werte für $|E|$

$$p + 1 + 2v$$

$$p + 1 - 2v$$

7. falls $D \notin \{-3, -4\}$

benutze r, s aus Tabelle von Schritt 1

bilde zwei Kurven für $k \in \{0, 1\}$

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

Beispiel: ① $D = -3$, $p = 13$

② $4p = u^2 + |-3| \cdot v^2$ $\quad u, v \in \mathbb{N}$

$4p = u^2 + 3v^2$

$4 \cdot 7 = 4^2 + 3 \cdot 2^2$

$4 \cdot 13 = 2^2 + 3 \cdot 4^2$

$= (-2)^2 + 3 \cdot 1^2$

$u = 7$
$v = 1$

③ g keine Kubikzahl mod 13

$1^{\frac{p-1}{3}} \equiv 1^4 \equiv 1 \bmod 13$ ist Kubikzahl?

$2^{\frac{p-1}{3}} \equiv 2^4 \equiv 16 \equiv 3 \neq 1 \bmod 13$

$\Rightarrow$ wähle $g = 2$

④ mögliche $|E|$-Werte

$p + 1 + u = 13 + 1 + 7 = 21$

$p + 1 - u = 13 + 1 - 7 = 7$

5. Kurven auflisten ($D=-3$)

$$y^2 \equiv x^3 - g^k \bmod p \qquad 0 \le k \le 5,\ g=2$$

(I) $y^2 \equiv x^3 - 1 \bmod 13$

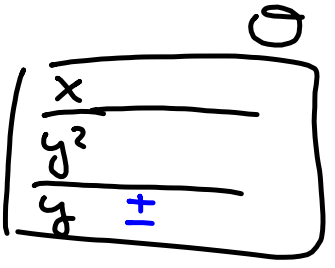
(II) $y^2 \equiv x^3 - 2 \bmod 13$

(III) $y^2 \equiv x^3 - 4 \bmod 13$

(IV) $y^2 \equiv x^3 - 8 \bmod 13$

(V) $y^2 \equiv x^3 - 3 \bmod 13$

(VI) $y^2 \equiv x^3 - 6 \bmod 13$



y	1	2	3	4	5	6
y^2	1	4	9	3	12	10

$u=7,\ v=1$

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

mögliche Werte für $|E|$

$\{7, 21, 19, 9, 12, 16\}$

VI S.O. III II V I IV