Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K23: Elliptische Kurven über endlichen Körpern

Stichworte: Elliptische Kurven über endlichen Körpern, $N_r = \#E(\mathbb{F}_{p^r})$, Defekt, Satz von Hasse, Birch & Swinnerton-Dyer-Vermutung, komplexe Multiplikation (CM), gute/schlechte Reduktion, Spur des Frobenius, Text in elliptische Kurve einbetten

---

23.1. Einleitung: Wir behandeln Nötiges zu elliptischen Kurven über $\mathbb{F}_p$ und $\mathbb{F}_{p^r}$.

23.2. Elliptische Kurven über endlichen Körpern werden vielfältig eingesetzt, zum einen in der Kryptographie, zum anderen auch in technischen Systemen mit wenigen Ressourcen (eingebettete Systeme), z.B. Steuergerät in Automobilen (elektronische Wegfahrsperren, Tuning-Schutz, Car-to-Car-Kommunikation, etc.). Manche Hardware-Implementationen arbeiten über $\mathbb{F}_{2^r}$ der Charakteristik 2, bei denen die technische Umsetzung damit günstig ist.

23.3. Wesentlich ist dass wir auf diesen elliptischen Kurven Punkte zählen können, und die Frobenius-Abbildung kennen.
Wir studieren zunächst elliptische Kurven über $\mathbb{F}_p$, wo p prim, mit der "modularen Brille" mod p. Das Verhalten dieser Kurven kann ganz anders sein als über $\mathbb{Q}$: Die elliptische Kurve $E(\mathbb{Q})$: $y^2 = x^3 + x$ aus Bsp. 22.4 etwa enthält den einzigen rationalen Punkt $(0,0)$, über $\mathbb{F}_p$ hat sie aber viele Punkte:
Sei $N_p := \#E(\mathbb{F}_p)$ von $y^2 = x^3 + x$, d.h. N_p die Anzahl der Punkte der elliptischen Kurve $E(\mathbb{F}_p)$, ist die Anzahl der Lösungen von $y^2 = x^3 + x$ modulo p.

23.4. Numerische Daten ergeben folgende Tabelle:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	...
$N_p - 1$	2	3	3	7	11	19	15	19	23	19	31	35	31	43	47	...

Offenbar gilt $p = N_p - 1$, falls $p \equiv 3\ (4)$. Für $p \equiv 1\ (4)$ sieht der sogenannte Defekt $a_p := p + 1 - N_p$ aus:

p	5	13	17	29	37	41	53	61	73	89	...
$a_p/2$	1	-3	1	5	1	5	-7	5	-3	5	...

Beobachtung: $p - \left(\frac{a_p}{2}\right)^2$ ist stets Quadratzahl!

Wir halten fest:

23.5. Für $E(\mathbb{F}_p): y^2 = x^3 + x$ gilt:

(a) Ist $p \equiv 3\ (4)$, gilt $N_p = p + 1$.

(b) Ist $p \equiv 1\ (4)$, ist $N_p = p + 1 \pm 2A$, wobei $p = A^2 + B^2$ mit $2 \nmid A$.
Dabei gilt "+" falls $A \equiv 1\ (4)$ und "−" falls $A \equiv 3\ (4)$.

Zum Bew. benötigen wir:

23.6. **Satz**: Für $p > 2$ und $E(\mathbb{F}_p): y^2 = x^3 + ax + b$, mit $a, b \in \mathbb{F}_p$ gilt

$$N_p := \#E(\mathbb{F}_p) = p + 1 + \sum_{1 \le x < p} \left(\frac{x^3 + ax + b}{p}\right),$$

wobei $\left(\frac{u}{p}\right) := \begin{cases} +1, & \text{wenn } u \not\equiv 0\ (p) \text{ ein quadr. Rest mod } p, \text{ d.h. } \exists w \in \mathbb{Z}: u \equiv w^2\ (p), \\ -1, & \text{wenn } u \not\equiv 0\ (p) \text{ kein } " \quad " \quad , \text{ d.h. } \nexists w \in \mathbb{Z}: u \equiv w^2\ (p), \\ 0, & \text{wenn } u \equiv 0\ (p), \text{ d.h. } p \mid u, \end{cases}$

das **verallgemeinerte Legendresymbol** ist.

Beweis: Vgl. Übungsblatt 12, Aufgabe A2 □

23.7. Bew. von 23.5(a): Für $p \equiv 3\ (4)$ ist $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$ nach 1. EG für das Legendresymbol, also $\left(\frac{(-x)^3 + (-x)}{p}\right) = -\left(\frac{x^3 + x}{p}\right)$ für $x \not\equiv 0\ (p)$ nach den Rechenregeln für das Legendresymbol, so dass $0 = \sum_{x \not\equiv 0\ (p)} \left(\left(\frac{x^3+x}{p}\right) + \left(\frac{(-x)^3+(-x)}{p}\right)\right) = 2 \sum_{x \not\equiv 0\ (p)} \left(\frac{x^3+x}{p}\right)$ folgt, denn mit x durchläuft auch $-x$ alle Restklassen $\not\equiv 0\ (p)$ mod p. Also ist $N_p = p + 1$. □

23.8. **Bem.:** den Bew. von 23.5(b) können wir hier nicht bringen.

23.9. **Bem.:** Für den Defekt $a_p = p+1-N_p$ gilt somit $a_p = -\sum_{1 \le x < p} \left(\frac{x^3+ax+b}{p} \right)$.
Im Absolutbetrag kann a_p nicht allzu groß werden, d.h. $N_p = \#E(\mathbb{F}_p)$ kann nicht allzu stark von p abweichen:

23.10. **Satz von Hasse (1933):** Für den Defekt a_p einer elliptischen Kurve $E(\mathbb{F}_p)$ gilt
$$|a_p| \le 2\sqrt{p}.$$
Der Satz gilt auch für $E(\mathbb{F}_{p^r})$, $r \ge 1$: Es ist $|p^r+1-N_{p^r}| \le 2\sqrt{p^r}$.

23.11. Diese Abschätzung für $|a_p|$ wurde 1920 von E. Artin vermutet. Eine Verallgemeinerung zeigte A. Weil in den 1940ern, und stark verallgemeinert wurde sie von P. Deligne in den 1970ern, wofür P. Deligne 1978 mit der Fieldsmedaille ausgezeichnet wurde.

23.12. **Bem.:** Im Bsp. $y^2 = x^3+x$ mit $p \equiv 1 \pmod 4$ folgt aus 23.5(b) die Hasseschranke, da
$$|a_p| = |p+1-N_p| = |p+1-p-1 \mp 2A| = |\mp 2A| = |\mp 2\sqrt{p-B^2}| \le 2\sqrt{p}.$$

23.13. **Bem.:** Fragen über die Größe von N_p führen zu offenen Problemen, z.B. die schwache Vermutung von Birch und Swinnerton-Dyer (1963/65): Für $E(\mathbb{Q})$ mit Koeff. aus $\mathbb{Z}$ sollte
$$\prod_{p \le x} \frac{N_p}{p} \sim C_E (\log x)^{r(E)}$$
gelten, wobei C_E eine Konstante >0 ist, die nur von $E(\mathbb{Q})$ abhängig ist.
Die Zahl $r(E)$ ist der Rang von $E(\mathbb{Q})$, vgl. K22.

Numerische Untersuchungen stützen diese Vermutung bislang.
Sie bedeutet: ist die Anzahl N_p der Punkte auf $E(\mathbb{F}_p)$ bei Reduktion mod p signifikant größer als der Erwartungswert, so sollte der Rang $r(E)$ positiv sein.
Sie stellt damit ein numerisch leicht testbares Kriterium für $r(E) > 0$ dar.

(Zur Schreibweise $\sim$: Die Aussage $f(x) \sim g(x)$ für zwei Funktionen $f,g : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ bedeutet, dass $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$, d.h. f,g sind asymptotisch gleich.)

23.14. Weitere numerische Beobachtungen in anderen Beispielen:
Für $E: y^2 = x^3 + 17$ gilt $a_p = 0$ genau für $p \equiv 2 \ (3)$, also auch $a_p = 0$ für "die Hälfte" aller Primzahlen. Das kommt für "wenige" elliptische Kurven mit Koeff. aus $\mathbb{Z}$ so heraus.
Für die Kurve $E: y^2 = x^3 - 4x^2 + 16$ etwa haben wir $a_p = 0$ nur selten:
Die einzigen $p < 2000$ mit $a_p = 0$ sind

$$p = 2, 19, 29, 199, 569, 809, 1289, 1439, \quad \text{usw.}$$

Welcher der Fälle eintritt, hängt davon ab, ob die elliptische Kurve "komplexe Multiplikation" (Kurz: CM für complex multiplication) hat.

23.15. **Def.:** Eine elliptische Kurve $E(k)$ hat komplexe Multiplikation (CM), falls sie neben den üblichen Endomorphismen $\psi_m : E(k) \to E(k)$, $P \mapsto m \cdot P$, wo $m \in \mathbb{Z}$, noch weitere hat.

Elliptische Kurven mit CM haben viele spezielle Eigenschaften, z.B.:
- Elliptische Kurven mit CM haben "ebensoviele" p mit $a_p = 0$ wie p mit $a_p \neq 0$.
- Elliptische Kurven ohne CM haben nur "wenige" p mit $a_p = 0$.

Dennoch konnte N. Elkies 1987 zeigen, dass jede elliptische Kurve $a_p = 0$ für unendlich viele p hat.

23.16. Beim Übergang von $E(\mathbb{Q})$ mit Koeffizienten $\in \mathbb{Z}$ zu $E(\mathbb{F}_p)$ zu einer Primzahl p reduzieren wir mod p. Nicht immer kommt dabei wieder eine elliptische Kurve heraus, nämlich dann nicht, wenn $\Delta(E(\mathbb{F}_p)) = 0$ in $\mathbb{F}_p$ gilt, d.h. $p \mid \Delta(E(\mathbb{Q})) \in \mathbb{Z}$.
Wir sprechen dann von schlechter Reduktion, engl.: bad prime,
ansonsten von guter Reduktion, engl.: good prime.

Die schlechte Reduktion kommt nur für alle Primteiler von $\Delta(E(\mathbb{Q})) \in \mathbb{Z}$ vor, also nur für endlich viele Primzahlen p. In diesen Ausnahmefällen verhält sich die kubische Kurve, die durch die Reduktion der Gleichung von $E(\mathbb{Q})$ mod p gegeben ist, oft anders; "+" gibt es dann nicht. Im Bsp. $E(\mathbb{Q})$: $y^2 = x^3 - 4x^2 + 16$ gilt etwa $N_p \equiv 4 \bmod 5$ für alle Primzahlen p außer $p=2$ und $p=11$. Tatsächlich sind $p=2$ und $p=11$ hier die Primzahlen mit schlechter Reduktion, da $\Delta(E(\mathbb{Q})) = -2^{12} \cdot 11$ ist.

23.17. Für eine elliptische Kurve $E(\mathbb{F}_{p^r})$, $r \geq 1$, wird der Defekt $a_{p^r} = p^r + 1 - N_{p^r}$ auch die "Spur des Frobenius" genannt. Wir erklären kurz diesen Begriff:

23.18. **Satz & Def.:** Der Frobeniusendomorphismus (kurz: Frobenius) einer elliptischen Kurve $E(\mathbb{F}_{p^r})$ ist der durch die Abb. $\phi: \mathbb{P}^2(\overline{\mathbb{F}_{p^r}}) \to \mathbb{P}^2(\overline{\mathbb{F}_{p^r}})$, $[x:y:z] \mapsto [x^{p^r} : y^{p^r} : z^{p^r}]$ vermittelte Gruppenhomomorphismus $\Phi: E(\overline{\mathbb{F}_{p^r}}) \to E(\overline{\mathbb{F}_{p^r}})$.

Beweisskizze:
- ϕ ist wirklich eine Abb. von $\mathbb{P}^2(\overline{\mathbb{F}_{p^r}})$ in sich. ✓
- ist $E(\mathbb{F}_{p^r})$ gegeben durch $F(x,y,z) = 0$, folgt auch $F(x^{p^r}, y^{p^r}, z^{p^r}) = 0$, weil in $\mathbb{F}_{p^r}$ die Gleichung $(c+d)^{p^r} = c^{p^r} + d^{p^r}$ für $c, d \in \overline{\mathbb{F}_{p^r}}$ richtig ist. Damit ist durch Φ eine Abb. von $E(\overline{\mathbb{F}_{p^r}})$ in sich definiert.
- die Verträglichkeit der Gruppenadd. auf $E(\overline{\mathbb{F}_{p^r}})$ mit Φ, d.h. die Eigenschaft $\Phi(P_1 + P_2) = \Phi(P_1) + \Phi(P_2)$, kann man nachrechnen. □

23.19. **Bem.:** Der Frobenius Φ lässt sich auf allgemeinere Strukturen (genau: dem Tatemodul) übertragen; dieser lässt eine Matrixdarstellung zu, wobei die Spur dieser Matrix genau a_{p^r} ergibt, daher der Name. Dieser Zusammenhang liefert weitere Möglichkeiten, den Defekt a_{p^r} bzw. N_{p^r} zu bestimmen.

23.20. **Text in eine elliptische Kurve einbetten**

Bei der Umsetzung des ElGamal-Verschlüsselungsverfahrens für eine elliptische Kurvengruppe $(G,+) = (E(\mathbb{F}_{p^r}),+)$, vgl. K5, ist erforderlich, dass sich die Kommunizierenden (A)lice und (B)ob darauf einigen, wie man Klartext in eine Folge von Punkten auf der elliptischen Kurve $E(\mathbb{F}_{p^r})$ übersetzt und wieder zurückerhält. Hier ein beispielhaftes Verfahren, wie dies praktisch durchgeführt werden kann:

23.21. **1. Schritt:** Man legt ein Alphabet mit N Buchstaben (identifiziert mit $0,1,\dots,N-1$) fest. Der Klartext (z.B ein Wort) habe die Blocklänge ℓ. Die Zuordnung

$$w = (a_0\, a_1 \dots a_\ell) \mapsto a_0 N^{\ell-1} + a_1 N^{\ell-2} + \dots + a_{\ell-2} N + a_{\ell-1} = x_w$$

liefert eine Bijektion zwischen den möglichen Klartextblöcken w und den Zahlen $0 \le x_w < N^\ell$. Eine Zahl x_w soll x-Koordinate eines Kurvenpunkts werden.

23.22. **2. Schritt:** Für eine gegebene elliptische Kurve $E(\mathbb{F}_{p^r})$ gibt es aber nicht zu jedem $x_0 \in \mathbb{F}_{p^r}$ einen Kurvenpunkt $(x_0, y_0) \in E(\mathbb{F}_{p^r})$. Für ein $k \in \mathbb{N}$ kann man aber die nächste x-Koordinate eines Kurvenpunkts $(x_1, y_1) \in E(\mathbb{F}_{p^r})$ mit $x_0 \le x_1 < x_0 + k$ schnell ermitteln; die Wahrscheinlichkeit, dass dies scheitert, d.h. dass ein solches x_1 nicht ex., beträgt schätzungsweise nur $\approx (\frac{1}{2})^k$. (Bsp.: $k = 50 \rightsquigarrow (\frac{1}{2})^{50} < 10^{-15}$)
Wähle so ein geeignetes k fest und eine elliptische Kurve $E(\mathbb{F}_{p^r})$ mit $p^r > k \cdot N^\ell$, d.h. es gibt wohl Kurvenpunkte mit genügend großen x-Koordinaten.

23.23. **3. Schritt:** Zu $x_w \in \{0,\dots,N^\ell - 1\}$ bestimme $P_w \in E(\mathbb{F}_{p^r})$ mit x-Koordinate $\ge k x_w$, etwa $P_w = (kx_w + j, y)$ mit $j \ge 0$ minimal.

23.24. **Beobachtung:** Hat das Verfahren funktioniert, ist dabei $j < k$, so dass durch Berechnung von $x_w = \lfloor \frac{x}{k} \rfloor$ für $P_w = (x,y) \in E(\mathbb{F}_{p^r})$ der Plaintext w aus P_w wieder zurückgewonnen werden kann.

23.25. **Bsp.:**

Für das Alphabet $\{A, B, \ldots, Z\} = \{0, 1, \ldots, 25\}$ ist $N = 26$, wähle z.B. $l = 2$, $k = 10$. Dann erfüllt $p = 6833$ die Bedingung $p > kN^2 = 6760$. Ist dazu $E(\mathbb{F}_p)$ gegeben durch $E(\mathbb{F}_p)$: $y^2 = x^3 + 5984x + 1180$, kann z.B. der Text "KRYPTO" wie folgt in eine Liste von 3 Punkten auf $E(\mathbb{F}_p)$ umgesetzt werden:

w	KR	YP	TO
x_w	$(10,17)_{26} = 277$	$(24,15)_{26} = 639$	$(19,14)_{26} = 508$
P_w	$(2771, 353)$	$(6390, 2797)$	$(5080, 238)$