Elliptische Kurven über endlichen Körpern

Jonathan Pirnay (MN 1740960)

Vortrag im Seminar über Kryptographie und elliptische Kurven am 21.12.2016

Im Folgenden sei q immer eine Primzahlpotenz $q = p^r$ und $F = \mathbb{F}_q$ der endliche Körper mit q Elementen. Unser Ziel ist es, die Gruppenordnung einer elliptischen Kurve $E(F)$ über einem endlichen Körper genauer zu verstehen, sowie mit Hilfe des Legendre-Symbols im zweiten Abschnitt eine explizite Formel für die Gruppenordnung anzugeben, wenn $q = p > 3$ prim ist.

Ist bspw. $E(F)$ elliptische Kurve mit $P \in E(F)$, sowie $Q \in \langle P \rangle$, dann ist $Q = mP$ für $m \in \mathbb{N}$. Für große $\#E(F)$ ist dies ein schwieriges DL-Problem.

Somit liefern elliptische Kurven mit kleiner Ordnung keine kryptographische Sicherheit.

1. Punkte zählen

1.1. **Bemerkung.** Sei $E(F)$ mit $F = \mathbb{F}_q = \mathbb{F}_{p^r}$ gegeben durch Weierstraßgleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

i.) Habe $E(F) \subseteq i(\mathbb{A}^2(F)) \cup \{O = [0:1:0]\}$ mit kanonischer Einbettung

$$i : \mathbb{A}^2(F) \to \mathbb{P}^2(F),\ (a,b) \mapsto [a:b:1]$$

Es gilt also

$$\#E(F) = 1 + \#\{(x,y) \in \mathbb{A}^2(F) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\ \} \tag{1}$$

Sei $x \in F$. Dann erhalten wir in (1) eine quadratische Gleichung in y mit höchstens zwei Lösungen in F. Dies liefert natürliche Schranke

$$\#E(F) \leq 2q + 1$$

ii.) Im Folgenden gelte $\mathrm{char}(F) \neq 2$. Nach [W, 2.3.2] können wir in (1) übergehen zu vereinfachter Weierstraßgleichung (mit neuen Koeffizienten a_i!)

$$y^2 = x^3 + a_2x^2 + a_3x + a_6 \tag{2}$$

Setze $h(x) := x^3 + a_2x^2 + a_3x + a_6$ und sei $x \in F$. Gilt $h(x) = 0$, so hat $y^2 = h(x)$ nur die Lösung $y = 0$. Ist $h(x) \neq 0$, und ist $h(x)$ ein Quadrat in F, so hat die Gleichung die Lösungen $(x,y), (x,-y) \in F \times F$. Ist $h(x)$ kein Quadrat in F, so existiert keine Lösung in $F \times F$.

iii.) Sei ζ Erzeuger der zyklischen Einheitengruppe $\mathbb{F}_q^{\times}$. Definiere Abbildung

$$\chi : \mathbb{F}_q^{\times} \to \{+1, -1\},\ \zeta^k \mapsto \begin{cases} +1 & \text{für } k \text{ gerade} \\ -1 & \text{für } k \text{ ungerade} \end{cases} \tag{3}$$

Da p ungerade, ist $n := \#\mathbb{F}_q^{\times} = p^r - 1$ gerade. Insbesondere ist für $l \in \mathbb{Z}$ $k + ln$ gerade genau dann wenn k gerade ist, und es folgt Wohldefiniertheit in (3). Zeige, dass χ unabhängig von der Wahl von ζ ist. Sei dazu $a \in \mathbb{F}_q^{\times}$ und α weiterer Erzeuger, d.h. $\alpha^m = a = \zeta^k$ und $\alpha = \zeta^l$ für $0 < k, l, m \leq n$. Dann $\zeta^k = \alpha^m = (\zeta^l)^m = \zeta^{lm}$, also $lm = k + sn$ für $s \in \mathbb{N}_{\geq 0}$ und erhalte

$$m \text{ gerade} \implies lm \text{ gerade} \overset{n \text{ gerade}}{\implies} k \text{ gerade}$$

Gleiches Argument mit Rollentausch liefert schließlich Äquivalenz

$$k \text{ gerade} \iff m \text{ gerade}$$

und χ ist unabhängig von der Wahl des Erzeugers. Man sieht leicht ein, dass χ Gruppenhomomorphismus ist, und nenne χ **quadratischen Quarakter**.

iv.) Setze $N := \{a \in F \mid \exists b \in F : \ a = b^2\}$. Offenbar is $N \subseteq \mathbb{F}_q^{\times}$ Untergruppe und wir können χ auch beschreiben durch

$$\mathbb{F}_q^{\times} \to \{+1, -1\}, \ a \mapsto \begin{cases} +1 & \text{für } a \in N \\ -1 & \text{für } a \notin N \end{cases} \tag{4}$$

und Homomorphiesatz liefert ${}^{\mathbb{F}_q^{\times}}\!/_N \cong \{\pm 1\}$, insbesondere $\#\mathbb{F}_q^{\times} = 2 \cdot \#N$. Es gibt in F also genau so viele Quadrate wie Nicht-Quadrate.

v.) Erweitere χ auf ganz $\mathbb{F}_q$ durch $\chi(0) := 0$. Ist $x \in F$, dann folgt aus ii.), dass die Gleichung $y^2 = h(x)$ genau $\chi(h(x)) + 1$ Lösungen in F besitzt.

Wir fassen diese Diskussion in folgendem Satz zusammen.

1.2. **Satz.** Sei $F := F_q$ der endlicher Körper mit $q = p^r$ und $\mathrm{char}(F) = p > 2$, sowie $E(F)$ elliptische Kurve mit Weierstraßgleichung der Form

$$Y^2Z = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

und

$$h(x) := x^3 + a_2x^2 + a_4x + a_6$$

Dann gilt

$$\#E(F) = \underbrace{1}_{[0:1:0]} + \sum_{x \in \mathbb{F}_q} (\chi(h(x)) + 1) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(h(x)) \tag{5}$$

Beweis: Klar nach 1.1. □

1.3. **Bemerkung.** Nach 1.1, i.) haben wir $\#E(F) \leq 2q + 1$. Wir haben aber gesehen, dass die Anzahl der Nicht-Quadrate in F gerade $\dfrac{\#F^{\times}}{2}$ beträgt. Man erwartet somit eher eine viel kleinere obere Schranke. Der folgende Satz zeigt, dass diese Annahme korrekt ist. Er war eine Vermutung von Emil Artin und wird in [S, Ch. V, Thm. 1.1] bewiesen.

1.4. **Satz von Hasse.** Sei $E(\mathbb{F}_q)$ eine elliptische Kurve über endlichem Körper. Dann gilt

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

1.5. **Korollar.** In der Situation von 1.2 gilt

$$|\sum_{x\in\mathbb{F}_q} \chi(h(x))| \leq 2\sqrt{q}$$

Beweis: Klar nach 1.2 und Satz von Hasse. □

2. Gruppenordnung über $\mathbb{Z}/p\mathbb{Z}$

Später werden wir den Schoof-Algorithmus kennenlernen, der eine effiziente Methode für die Bestimmung der Gruppenordnung liefert. Mit unserer allgemeinen Formel (5) ist es für gegebenes $h(x)$ noch unklar, wie man $\chi(h(x))$ berechnen kann. Im Folgenden betrachten wir elliptische Kurven über $\mathbb{F}_p$ mit p prim.

2.1. **Definition.** Sei $p > 2$ Primzahl und $a \in \mathbb{Z}$. Definiere das **Legendre-Symbol** durch

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{falls } b \in \mathbb{Z} \text{ existiert mit } a \equiv b^2 \bmod p \text{ und } (a,p) = 1 \\ -1 & \text{falls kein } b \in \mathbb{Z} \text{ existiert mit } a \equiv b^2 \bmod p \\ 0 & \text{falls } a \equiv 0 \bmod p \end{cases} \tag{6}$$

Ist $\left(\frac{a}{p}\right) = 1$ (bzw. -1), so nennt man a einen **quadratischen Rest (bzw. Nichtrest) modulo** p.

2.2. **Satz.** Für das Legendre-Symbol gilt:

i.) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

ii.) $\#\{a^2 \in \mathbb{F}_p^{\times} : \ a \in \mathbb{F}_p^{\times}\} = \frac{p-1}{2}$

iii.) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$

Beweis: Aus der Definition von $\left(\frac{a}{p}\right)$ folgt sofort, dass wir das Legendre-Symbol auch als Gruppenhomomorphismus $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p \to \pm 1, \ \left(\frac{a}{p}\right) = \chi(a)$ auffassen können. Mit 1.1 folgt sofort i.) und ii.) ($\#\mathbb{F}_p^{\times} = p - 1$). Für iii.) sei ζ Erzeuger von $\mathbb{F}_p^{\times}$ und $a = \zeta^k, \ k > 0$. Es gilt

$$a \text{ ist Quadrat in } \mathbb{F}_p^{\times} \iff k \text{ gerade} \iff \zeta^{\frac{k(p-1)}{2}} = 1 \iff a^{\frac{p-1}{2}} = 1$$

Angenommen $a^{\frac{p-1}{2}} \not\equiv 1 \bmod p$. Dann kann $(a^{\frac{p-1}{2}})^2 \equiv 1 \bmod p$ nur gelten für $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ und es folgt die Behauptung. □

2.3. **Bemerkung.** Mit der square-and-multiply Methode (siehe Vortrag über schnelle zahlentheoretische Algorithmen) können wir also schnell testen, ob $a \in \mathbb{Z}$ ein Quadrat in $\mathbb{F}_p^{\times}$ ist.

Folgender Satz über das Legendre-Symbol ist ein wichtiger Satz der Zahlentheorie und vereinfacht in vielen Fällen die Berechnung des Legendre-Symbols.

2.4. **Satz (Quadratisches Reziprozitätsgesetz).**

i.) Für Primzahlen $p, q > 2$ gilt:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{, falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\ -\left(\frac{q}{p}\right) & \text{, falls } p \equiv q \equiv 3 \bmod 4 \end{cases}$$

In geschlossener Form schreibt sich dies als

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \tag{7}$$

ii.) (Ergänzungssatz zum quadratischen Reziprozitätsgesetz)

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{, falls } p \equiv 1 \bmod 4 \\ -1 & \text{, falls } p \equiv 3 \bmod 4 \end{cases}, \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{, falls } p \equiv 1, 7 \bmod 8 \\ -1 & \text{, falls } p \equiv 3, 5 \bmod 8 \end{cases}$$

In geschlossener Form schreibt sich dies als

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{8}$$

2.5. **Beispiel.** Setze $q := 1009$, $p := 10^{1000} + 453$. q is prim, p ist wahrscheinlich prim (kleiner Fermatscher Satz). Habe $p \equiv q \equiv 1 \bmod 4$. Berechne $p \equiv 417 \bmod 1009$. Es folgt:

$$\left(\frac{1009}{p}\right) = \left(\frac{p}{1009}\right) = \left(\frac{p \bmod 1009}{1009}\right) = \left(\frac{417}{1009}\right) = \left(\frac{3 \cdot 139}{1009}\right) =$$
$$= \left(\frac{3}{1009}\right) \cdot \left(\frac{139}{1009}\right) = \left(\frac{1009}{3}\right) \cdot \left(\frac{1009}{139}\right) = \left(\frac{1009 \bmod 3}{3}\right) \cdot \left(\frac{1009 \bmod 139}{139}\right) =$$
$$= \left(\frac{1}{3}\right) \cdot \left(\frac{36}{139}\right) = 1 \cdot 1 = 1$$

Also ist q quadratischer Rest modulo p.

2.6. **Bemerkung.** Sei $p > 3$ prim, $F := \mathbb{F}_p$, sowie elliptische Kurve $E(F)$. Insbesondere ist $\mathrm{char}(F) \neq 2, 3$, und wir können nach [W, 2.3.2] zu affiner Weierstraßgleichung

$$y^2 = x^3 + ax + b$$

übergehen. Satz 1.2 vereinfacht sich somit mit Hilfe des Legendre-Symbols zu

$$\#E(F) = p + 1 + \sum_{x \in F} \left(\frac{x^3 + ax + b}{p} \right) \tag{9}$$

2.7. **Beispiel.** Sei $p \equiv 3 \bmod 4$ Primzahl und $F := \mathbb{F}_p$, sowie die elliptische Kurve $E(F)$ gegeben durch die affine Weierstraßgleichung

$$y^2 = x^3 + ax =: h(x)$$

für $a \neq 0$ in F. Quadratisches Reziprozitätsgesetz liefert $\chi(-1) = \left(\frac{-1}{p} \right) = -1$. Es folgt für alle $x \in F$ mit $h(x) \neq 0$:

$$\chi(h(-x)) = \chi((-x)^3 + a(-x)) = \chi((-1) \cdot (x^3 + ax)) = \chi(-1) \cdot \chi(h(x)) = -\chi(h(x))$$

Offenbar ist $h(x) = 0$ nur für $x = 0$ und (sofern $\left(\frac{-a}{p} \right) = 1$) für $b, -b \in F$ mit $b^2 = -a$. In jedem Fall muss also gelten

$$\sum_{x \in F} \chi(h(x)) = 0$$

und damit

$$\#E(F) = 1 + p + \sum_{x \in F} \chi(h(x)) = p + 1$$

3. Beweis des quadratischen Reziprozitätsgesetzes

In diesem Zusatzkapitel wollen wir das quadratische Reziprozitätsgesetz beweisen. Gauß selbst lieferte acht verschiedene Beweise, mittlerweile gibt es über hundert, von denen sich viele natürlich nur in Details unterscheiden. Wir werden einen Beweis nachvollziehen, der auf Eisenstein zurückgeht, und den Ergänzungssatz weglassen.

3.1. **Satz (Quadratisches Reziprozitätsgesetz).** Für Primzahlen $p, q > 2$ gilt:

$$\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

3.2. **Definition und Beispiel.** Sei $p > 2$ Primzahl und $a \in \mathbb{Z}$ mit $(a, p) = 1$. Betrachte Menge

$$S := \{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}\}$$

Für $k \in \{1, \ldots, \frac{p-1}{2}\}$ ist ka kongruent zu genau einem Element in S (mod p) Setze somit:

$$\mu := \#\{c \in S \mid c < 0 \ \wedge \ \exists k \in \{1, \ldots, \frac{p-1}{2}\} : \ ak \equiv c \bmod p\}$$

Beispiel: Sei $p = 7$ und $a = 4$. Dann ist $\frac{p-1}{2} = 3$ und $1 \cdot 4, 2 \cdot 4, 3 \cdot 4$ sind kongruent zu $-3, 1, -2$ in S. Davon sind 2 Zahlen negativ, also in diesem Fall $\mu = 2$.

3.3. **Gaußsches Lemma.** In der Situation von 3.2 gilt

$$\left(\frac{a}{p}\right) = (-1)^{\mu}$$

Beweis: Für beliebiges l habe $\pm m_l \equiv l \cdot a \bmod p$, wobei $m_l > 0$ und $\pm m_l \in S$. Läuft l über $1, \ldots, \frac{p-1}{2}$, so ist μ offenbar genau gleich der Anzahl der Minuszeichen, die vor den m_l's auftreten. Zeige dass für $1 \leq k, l \leq \frac{p-1}{2}$ mit $l \neq k$ gilt, dass $m_l \neq m_k$. Angenommen $m_k = m_l$, dann ist $la \equiv \pm ka \ (p)$, und aus $p \nmid a$ folgt $l \pm k \equiv 0 \ (p)$. Dies ist aber unmöglich, denn $l \neq k$ und $|l \pm k| \leq |l| + |k| = l + k \leq p - 1$. Also $m_l \neq m_k$ und somit

$$\{1, \ldots, \frac{p-1}{2}\} = \{m_1, \ldots, m_{\frac{p-1}{2}}\} \tag{10}$$

Durch Multiplikation der Kongruenzen

$$1 \cdot a \equiv \pm m_1 \ (p), 2 \cdot a \equiv \pm m_2 \ (p), \ldots, \frac{p-1}{2} \cdot a \equiv \pm m_{\frac{p-1}{2}} \ (p)$$

erhalten wir schließlich

$$(\frac{p-1}{2})! \ a^{\frac{p-1}{2}} \equiv (-1)^{\mu} (\frac{p-1}{2})! \bmod p$$

Aus $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$ folgt die Behauptung. □

3.4. **Lemma.** Betrachte Funktion

$$f : \mathbb{R} \to \mathbb{C}, \ z \mapsto e^{2\pi \mathrm{i} z} - e^{-2\pi \mathrm{i} z} \tag{11}$$

f erfüllt folgende Eigenschaften $\forall z \in \mathbb{R}$:

i.) $f(z) = 2\mathrm{i} \sin(2\pi z)$
ii.) $f(z + 1) = f(z)$
iii.) $f(-z) = -f(z)$
iv.) $2z \notin \mathbb{Z} \implies f(z) \neq 0$

Beweis: i.) folgt aus

$$\begin{aligned} e^{2\pi \mathrm{i} z} - e^{-2\pi \mathrm{i} z} &= \cos(2\pi z) + \mathrm{i}\sin(2\pi z) - (\cos(-2\pi z) + \mathrm{i}\sin(-2\pi z)) = \\ &= \cos(2\pi z) + \mathrm{i}\sin(2\pi z) - \cos(2\pi z) - (-\mathrm{i}\sin(2\pi z)) = 2\mathrm{i}\sin(2\pi z) \end{aligned}$$

Der Rest ist klar mit i.). □

Wir möchten nun zwei wichtige Identitäten von f nachrechnen. Dafür benötigen wir noch folgendes Lemma.

3.5. **Lemma.** Sei $n > 0$ ungerade und $\zeta = e^{\frac{2\pi \mathrm{i}}{n}}$ n-te primitive Einheitswurzel, sowie $x, y \in \mathbb{C}$. Es gilt:

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) \tag{12}$$

Beweis: Die Behauptung ist offenbar wahr für $y = 0$. Gelte also $y \neq 0$. Bekanntlich zerfällt das Polynom $X^n - 1$ über $\mathbb{C}$ in $X^n - 1 = \prod_{k=0}^{n-1} (X - \zeta^k)$. Insbesondere folgt

$$\left(\frac{x}{y}\right)^n - 1 = \prod_{k=0}^{n-1} \left(\frac{x}{y} - \zeta^k\right) \overset{\cdot y^n}{\Longrightarrow} x^n - y^n = \prod_{k=0}^{n-1} (x - \zeta^k y)$$

Da n ungerade ist, gilt: Läuft k über alle Restklassen mod n, so auch $-2k$. Es folgt also:

$$\begin{aligned} x^n - y^n &= \prod_{k=0}^{n-1} (x - \zeta^{-2k} y) \\ &= \zeta^{-(1+2+\cdots+(n-1))} \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) \\ &= \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) \end{aligned}$$

Der letzte Schritt folgt aus n ungerade, also

$$n \mid (1 + 2 + \cdots + (n-1)) = \frac{n \cdot (n-1)}{2}$$

□

3.6. **Proposition.** Sei $n > 0$ ungerade. Dann gilt in (11):

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} f(z + \frac{k}{n}) f(z - \frac{k}{n})$$

Beweis: Benutze 3.5 für $x = e^{2\pi \mathrm{i} z}$ und $y = e^{-2\pi \mathrm{i} z}$. Dann ist

$$\begin{aligned} f(nz) = x^n - y^n &= \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) \\ &= \prod_{k=0}^{n-1} (e^{\frac{2\pi \mathrm{i} k}{n}} \cdot e^{2\pi \mathrm{i} z} - e^{\frac{-2\pi \mathrm{i} k}{n}} e^{-2\pi \mathrm{i} z}) \\ &= \prod_{k=0}^{n-1} f(z + \frac{k}{n}) \end{aligned}$$

Mit 3.4 gilt $f(z + \frac{k}{n}) = f(z + \frac{k}{n} - 1) = f(z - \frac{n-k}{n})$. Läuft k von $\frac{n+1}{2}$ nach $n-1$, so läuft $n - k$ von $\frac{n-1}{2}$ nach 1. Somit folgt

$$\begin{aligned} \frac{f(nz)}{f(z)} &= \prod_{k=1}^{\frac{n-1}{2}} f(z + \frac{k}{n}) \cdot \prod_{k=\frac{n+1}{2}}^{n-1} f(z + \frac{k}{n}) \\ &= \prod_{k=1}^{\frac{n-1}{2}} f(z + \frac{k}{n}) \cdot \prod_{k=\frac{n+1}{2}}^{n-1} f(z - \frac{n-k}{n}) \\ &= \prod_{k=1}^{\frac{n-1}{2}} f(z + \frac{k}{n}) f(z - \frac{k}{n}) \end{aligned}$$

□

3.7. **Proposition.** Sei $p > 2$ prim, $a \in \mathbb{Z}$ mit $(a, p) = 1$. Dann gilt

$$\prod_{l=1}^{\frac{p-1}{2}} f(\frac{la}{p}) = \left(\frac{a}{p}\right) \cdot \prod_{l=1}^{\frac{p-1}{2}} f(\frac{l}{p})$$

Beweis: Sei wie im Beweis von 3.3 $la \equiv \pm m_l \ (p)$, wobei $1 \leq m_l \leq \frac{p-1}{2}$. Somit gilt

$$la = kp \pm m_l \text{ für ein } k \in \mathbb{Z} \implies f(\frac{la}{p}) = f(k \pm \frac{m_l}{p}) \overset{3.4}{\implies} f(\frac{la}{p}) = f(\pm \frac{m_l}{p})$$

Insgesamt folgt also

$$\begin{aligned}\prod_{l=1}^{\frac{p-1}{2}} f(\frac{la}{p}) &= \prod_{l=1}^{\frac{p-1}{2}} f(\pm\frac{m_l}{p}) = \prod_{l=1}^{\frac{p-1}{2}} \pm f(\frac{m_l}{p}) \\ &= (-1)^{\mu} \prod_{l=1}^{\frac{p-1}{2}} f(\frac{m_l}{p}) \overset{3.3}{=} \left(\frac{a}{p}\right) \cdot \prod_{l=1}^{\frac{p-1}{2}} f(\frac{m_l}{p}) \\ &\overset{(10)}{=} \left(\frac{a}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f(\frac{l}{p})\end{aligned}$$

□

Wir können nun das quadratische Reziprozitätsgesetz beweisen.

3.8. **Beweis von 3.1.** Seien $p, q > 2$ Primzahlen. Mit 3.7 gilt

$$\prod_{l=1}^{\frac{p-1}{2}} f(\frac{lq}{p}) = \left(\frac{q}{p}\right) \cdot \prod_{l=1}^{\frac{p-1}{2}} f(\frac{l}{p})$$

Nach 3.6 habe

$$\frac{f(q \cdot \frac{l}{p})}{f(\frac{l}{p})} = \prod_{m=1}^{\frac{q-1}{2}} f(\frac{l}{p} + \frac{m}{q}) f(\frac{l}{p} - \frac{m}{q})$$

Zusammen erhalten wir also:

$$\left(\frac{q}{p}\right) = \prod_{l=1}^{\frac{p-1}{2}} \prod_{m=1}^{\frac{q-1}{2}} f(\frac{l}{p} + \frac{m}{q}) f(\frac{l}{p} - \frac{m}{q})$$

Tauschen wir die Rollen von p und q, so bekommen wir auf die gleiche Weise:

$$\left(\frac{p}{q}\right) = \prod_{l=1}^{\frac{p-1}{2}} \prod_{m=1}^{\frac{q-1}{2}} f(\frac{m}{q} + \frac{l}{p}) f(\frac{m}{q} - \frac{l}{p})$$

Wegen $f(\frac{m}{q} - \frac{l}{p}) = -f(\frac{l}{p} - \frac{m}{q})$ gilt

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{l=1}^{\frac{p-1}{2}} \prod_{m=1}^{\frac{q-1}{2}} (-1) f(\frac{l}{p} + \frac{m}{q}) f(\frac{m}{q} - \frac{l}{p}) \\ &= (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})} \left(\frac{p}{q}\right)\end{aligned}$$

also

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

□

Literatur

[I] Ireland, K. (et al.). *A Classical Introduction to Modern Number Theory*. Springer.

[R] W. Ruppert. *Elliptische Kurven und Kryptographie*. Skript einer Vorlesung im Sommer 2003 an der Universität Erlangen.

[S] Silverman, J.H. *The Arithmetic of Elliptic Curves*. Springer.

[W] Werner, A. *Elliptische Kurven in der Kryptographie*. Springer 2002.