Satz 1. *Sei $p \geq 3$ prim. Seien $k, s \in \mathbb{F}_p^*$. Dann ist die Anzahl der Paare $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ mit*

$$x^2 - ky^2 = s$$

gegeben durch

$$\begin{cases} p-1\,, & k \in (\mathbb{F}_p^*)^2\,, \\ p+1\,, & k \notin (\mathbb{F}_p^*)^2\,. \end{cases}$$

Korollar 2. *Sei $p \geq 5$ prim. Dann ist die Anzahl der Paare $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ mit*

$$a^2 + ab + b^2 = -1$$

gegeben durch

$$\begin{cases} p-1\,, & p \equiv 1 \pmod 6\,, \\ p+1\,, & p \equiv 5 \pmod 6\,. \end{cases}$$

Beweis. Dies folgt aus Satz 1, indem wir $k = -3$ und $s = -1$ setzen, denn es gilt

$$a^2 + ab + b^2 = \left(a + \tfrac{1}{2}b\right)^2 + 3\left(\tfrac{1}{2}b\right)^2\,,$$

und

$$(a, b) \mapsto \left(a + \tfrac{1}{2}b, \tfrac{1}{2}b\right)$$

ist ein linearer Endomorphismus mit Determinante

$$\det \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} = \tfrac{1}{2} \neq 0$$

und daher bijektiv. Zudem ist -3 bekanntlich genau für $p \equiv 1 \pmod 6$ ein quadratischer Rest modulo p (das folgt zum Beispiel aus dem quadratischen Reziprozitätsgesetz). □

Beweis von Satz 1. Wir beginnen mit dem Fall $k \in (\mathbb{F}_p^*)^2$. Es gilt

$$x^2 - ky^2 = \left(x - \sqrt{k} \cdot y\right)\left(x + \sqrt{k} \cdot y\right)\,,$$

und

$$(x, y) \mapsto \left(x - \sqrt{k} \cdot y, x + \sqrt{k} \cdot y\right)$$

ist ein linearer Endomorphismus mit Determinante

$$\det \begin{pmatrix} 1 & -\sqrt{k} \\ 1 & +\sqrt{k} \end{pmatrix} = 2\sqrt{k} \neq 0$$

und daher bijektiv. Wir können also stattdessen die Anzahl der Paare $(u, v) \in \mathbb{F}_p \times \mathbb{F}_p$ mit

$$uv = s$$

betrachten. Diese beträgt offensichtlich $p - 1$.

Wir kommen nun zu dem Fall $k \notin (\mathbb{F}_p^*)^2$. Dann gilt $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{k}]$. In $\mathbb{F}_{p^2}$ gilt erneut

$$x^2 - ky^2 = \left(x + \sqrt{k} \cdot y\right)\left(x - \sqrt{k} \cdot y\right) \ .$$

Die Umkehrabbildung zu

$$\begin{aligned} \mathbb{F}_{p^2} \times \mathbb{F}_{p^2} &\to \mathbb{F}_{p^2} \times \mathbb{F}_{p^2} \\ (x, y) &\mapsto \left(x + \sqrt{k} \cdot y, x - \sqrt{k} \cdot y\right) \end{aligned}$$

lautet

$$(u, v) \mapsto \left(\frac{u+v}{2}, \frac{u-v}{2\sqrt{k}}\right) \ .$$

Wir suchen also die Anzahl der Paare $(u, v) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$ mit

$$uv = s \ ,$$

für die $\frac{u+v}{2}$ und $\frac{u-v}{2\sqrt{k}}$ in $\mathbb{F}_p$ liegen. Bekanntlich ist $\mathbb{F}_p \subset \mathbb{F}_{p^2}$ durch die Fixpunkte des Frobenius-Automorphismus $t \mapsto t^p$ gegeben. Wegen $2^{p-1} = 1$ und

$$\left(\sqrt{k}\right)^{p-1} = k^{\frac{p-1}{2}} = \left(\frac{k}{p}\right) = -1$$

ist die Bedingung daher äquivalent zu

$$uv = s \qquad \text{und} \qquad (u+v)^p = u + v \qquad \text{und} \qquad (u-v)^p = v - u \ .$$

Wir beweisen jetzt folgendes Lemma:

Lemma 3. *Für $u \in \mathbb{F}_{p^2}^*$ und $s \in \mathbb{F}_p^*$ ist die Bedingung*

$$\left(u + \frac{s}{u}\right)^p = u + \frac{s}{u} \qquad \textit{und} \qquad \left(u - \frac{s}{u}\right)^p = \frac{s}{u} - u \tag{1}$$

äquivalent zu $u^{p+1} = s$.

Beweis. Aus $u^{p+1} = s$ folgt

$$\left(u + \frac{s}{u}\right)^p = (u + u^p)^p = u^p + u^{p^2} = u^p + u = u + \frac{s}{u}$$

sowie

$$\left(u - \frac{s}{u}\right)^p = (u - u^p)^p = u^p - u^{p^2} = u^p - u = \frac{s}{u} - u \ .$$

Umgekehrt impliziert (1) durch Multiplikation mit u^p und Verwendung von $s^p = s$, dass

$$0 = u^{2p} + s^p - u^{p+1} - su^{p-1} = (u^{p+1} - s)(u^{p-1} - 1)$$

und

$$0 = u^{2p} - s^p - su^{p-1} + u^{p+1} = (u^{p+1} - s)(u^{p-1} + 1)$$

gelten. Da nicht gleichzeitig $u^{p-1} = 1$ und $u^{p-1} = -1$ sein kann, folgt $u^{p+1} = s$. □

Somit suchen wir für ein gegebenes $s \in \mathbb{F}_p^*$ einfach die Anzahl aller $u \in \mathbb{F}_{p^2}^*$ mit $u^{p+1} = s$. Diese beträgt $p + 1$, da $\mathbb{F}_{p^2}^*$ zyklisch ist und $\mathbb{F}_p^*$ eine Untergruppe von Index $p + 1$ ist. □