Wurzelziehen in einem endlichen Körper *K*

Es sei char $K = p > 2$.
K kann in natürlicher Weise als endlichdimensionaler Vektorraum über $\mathbb{Z}_p$ aufgefaßt werden.
Ist $r \in \mathbb{N}$ dessen Dimension, so hat man offenbar $|K| = q$ mit $q = p^r$.

Die Abbildung $\sigma: K \to K$, gegeben durch $x \mapsto x^p$, ist ein Körperautomorphismus, wie man leicht überlegt bzw. nachrechnet. Es ergibt sich auch, daß $\sigma^r = \underbrace{\sigma \circ \ldots \circ \sigma}_{r-\text{mal}}$ die Identität ist, denn es gilt für $x \in K$: $\sigma^r(x) = x^{p^r} = x^q = x^{q-1} x = x$: die Ordnung der multiplikativen Gruppe K^* ist ja q-1.

Ein irreduzibles Polynom $f \in K[X]$ vom Grad 2 führt zum Körper $E := K[X]/<f>$. Dessen Elemente lassen sich repräsentieren durch Polynome vom Grad kleinergleich 1. Es ist $|E| = q^2$.
K läßt sich als Unterkörper von *E* auffassen, indem man die Elemente von *K* mit den konstanten Polynomen in *E* identifiziert. Die kanonische Projektion $\pi: K[X] \to E$ ist ein surjektiver Ringhomomorphismus, sein Kern gerade das Ideal $<f>$. Wir schreiben $\overline{g} := \pi(g)$ und $x := \overline{X}$, sowie einfach 0 für das Nullelement $\overline{0}$ und 1 für das 1-Element $\overline{1}$ von *E*.

E besitzt wie *K* die Charakteristik p ; der Frobenius-Automorphismus ist auf *E* wie auf *K* definiert. Setzen wir $\tau = \sigma^r$, so ist τ^2 die Identität auf E, wärend *K* gerade der "Fixkörper" von τ ist, d.h. *K* besteht gerade aus den Elementen von *E*, die durch τ auf sich selbst abgebildet werden.

Als irreduzibles Polynom in *K*[*X*] besitzt *f* natürlich keine Nullstelle in *K*.
f besitzt wohl aber eine Nullstelle in *E*, denn es ist $f(x) = f(\overline{X}) = \overline{f(X)} = \overline{f} = \overline{0} = 0$.
Die zweite Nullstelle finden wir durch Division:
$(X^2 + aX + b) : (X - x) = X + (x + a)$. Dabei nutzen wir die Gleichung $x^2 + ax + b = 0$.
Der Witz ist jetzt, daß diese zweite Nullstelle -(x+a)auch gleich $\tau(x) = x^q$ ist!

Denn die Automorphismuseigenschaft bewirkt, daß $f(x^q) = f(\tau(x)) = \tau(f(x)) = \tau(0) = 0$. Die Koeffizienten von *f* liegen ja in *K* und werden daher durch τ auf sich selbst abgebildet. Da $x \notin K$, ist auch $\tau(x) \neq x$.

Zusammenfassend: $X^2 + aX + b = (X - x)(X - x^q) = X^2 - (x + x^q) X + x \cdot x^q = x^{q+1}$, also durch Koeffizientenvergleich $b = x^{q+1}$.

Sei jetzt $b \in K$ gegeben.
Wir beschaffen uns ein $a \in K$, so daß $f = X^2 + aX + b$ irreduzibel ist. Letzteres ist genau dann der Fall, wenn das Polynom *f* keine Nullstelle in *K* hat, d.h. wenn es keine Wurzel aus $a^2 - 4b$ gibt.
Ist $K = \mathbb{Z}_p$, so können wir dies durch Berechnen des Legendre-Symbols feststellen.

Gehen wir im Folgenden also von der Irreduzibilität von *f* aus:

Wir wissen, daß $b = x^{q+1} = \left(x^{\frac{q+1}{2}}\right)^2$. Also ist $x^{\frac{q+1}{2}}$ Quadratwurzel von b! Eine solche Potenz läßt sich leicht berechnen.

Diese Wurzel liegt auch garantiert in *K*, wenn wir wissen, daß eine Wurzel von *b* in *K* existiert: Deren additiv Inverses ist ja ebenfalls Wurzel und liegt in *K*, und die Gleichung $x^2 = b$ kann im Körper *E* nicht mehr als zwei Wurzeln besitzen.

Beispiel:

$K=\mathbb{Z}_{101}$, b=24.

$\left(\frac{6^2-4b}{101}\right)=-1$, (6 ist die erste Zahl, die klappt), also $X^2+6X+24\in\mathbb{Z}_{101}[X]$ irreduzibel.

Rechnung in Pari:

```
gp > Mod(Mod(1,101)*x,Mod(1,101)*x^2+Mod(6,101)*x+Mod(24,101))^51
%1 = Mod(Mod(78, 101), Mod(1, 101)*x^2 + Mod(6, 101)*x + Mod(24, 101))
```

d.h. in *E* hat man: $x^{51}=78$. Und tatsächlich gilt in $\mathbb{Z}_{101}$: $78^2=24$.