Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe'22/'23, Uhu
K. Halupczok

Z7: Quadratisches Reziprozitätsgesetz

Stichworte: Legendre-Symbol, Satz von Euler, QRG mit Galoistheorie, Beweis des EGs, Jacobi-Symbol, Vermeidung der Faktorisierung, Lösung von $x^2 \equiv a\ (p)$

7.1. **Einleitung:** Wir zeigen das QRG und die beiden Ergänzungsgesetze (EG's) unter Verwendung von Galoistheorie. Das Legendre-Symbol wird zum Jacobi-Symbol fortgesetzt (selbst für negative "Nenner"), welches sich zur schnellen Berechnung der Symbole ohne Faktorisierung gut eignet. An das explizite "Wurzelziehen" mod p aus EinfZT EZ11, wird erinnert.

7.2. **Def.:** Für ungerade Pzen $p>0$ und $a \in \mathbb{Z}$ mit $p \nmid a$ sei

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{falls } a \text{ Quadrat mod } p, \text{ d.h. } \exists b \in \mathbb{Z} : a \equiv b^2\ (p), \\ -1, & \text{falls } a \text{ nicht Quadrat mod } p, \text{ d.h. sonst,} \end{cases}$$

→ a heißt quadratischer Rest mod p

→ a heißt quadratischer Nichtrest mod p

sprich "a nach p".

Dies heißt Legendre-Symbol.

7.3. **Eigenschaften:**

(1) **Satz von Euler:** $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (p)$.

Insb. ist $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}\ (p)$, also $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1\ (4), \\ -1, & p \equiv 3\ (4). \end{cases}$

Es ist $(\mathbb{Z}/(p))^\times = \mathbb{F}_p^\times$ zyklisch der Ordnung $p-1$, [vgl. Algebra Satz A21.2]
also $a^{p-1} \equiv 1\ (p)$ ("Kleiner Fermat") für $a \in \mathbb{F}_p^\times$.
Es folgt $a^{\frac{p-1}{2}} \equiv \pm 1\ (p)$. Sei $c \in \mathbb{Z}$ so, dass c mod p die Gruppe $\mathbb{F}_p^\times$ erzeugt (PW mod p). Dann gilt: a Quadrat mod $p \Leftrightarrow a \in \langle c^2 \rangle$.
[$\Leftarrow$ klar, $\Rightarrow$: Sei $a \equiv b^2\ (p)$ und $b \equiv c^i\ (p)$. Dann ist $a = b^2 = c^{2i} \in \langle c^2 \rangle$.]
Nun: $a \in \langle c^2 \rangle \Leftrightarrow a^{\frac{p-1}{2}} = c^{2i \cdot \frac{p-1}{2}} = c^{(p-1)i} = 1 \pmod p$.]

(2) Es gilt: $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

[$\left(\frac{a \cdot b}{p}\right) \equiv (a \cdot b)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)\ (p)$, also $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.]

7.4. **Quadratisches Reziprozitätsgesetz (QRG):** (i) Für ungerade PZ $p,q>0$ gilt: $\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)$, d.h. $\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), \text{ falls } p \text{ oder } q \equiv 1\ (4), \\ -\left(\frac{p}{q}\right), \text{ falls } p \text{ und } q \equiv 3\ (4). \end{cases}$

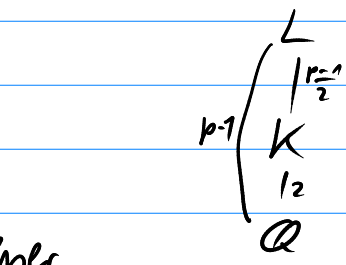
(ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, **1. Ergänzungssatz (1.EG)**,

(iii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv 1 \text{ oder } 7\ (8), \text{ d.h. } p \equiv \pm 1\ (8), \\ -1, & p \equiv 3 \text{ oder } 5\ (8), \text{ d.h. } p \equiv \pm 3\ (8), \end{cases}$

2. Ergänzungssatz (2.EG).

Bew.: Sei $\omega = e^{2\pi i/p}$, $L = \mathbb{Q}(\omega)$. Haben Isomorphie

$$\mathbb{F}_p^\times = (\mathbb{Z}/(p))^\times \xrightarrow{\cong} G = \mathrm{Gal}(L|\mathbb{Q}),$$
$$a \longmapsto \sigma_a \text{ mit } \sigma_a(\omega) = \omega^a.$$



Weiter sei ρ ein erzeugendes El. von G, $K := \mathrm{Fix}(\rho^2)$, haben $[G:\langle\rho^2\rangle] = 2$. K ist der einzige Zwischenkörper vom Grad 2 über $\mathbb{Q}$ (laut HS der Galoistheorie), nämlich: [$\mathrm{disc}(\omega) = (-1)^{\frac{p-1}{2}} p^{p-2}$, 6.18]

$K = \mathbb{Q}(\sqrt{p^*}) = \mathbb{Q}(\delta)$, wo $p^* = (-1)^{\frac{p-1}{2}} p$ und $\delta = \sqrt{\mathrm{disc}(\omega)}$, nach 6.23.

Nun ist auch $\delta = \det\left((\omega^{ij})_{\substack{1\le i\le p-1 \\ 0\le j\le p-2}}\right)$, also $\delta = \prod_{1\le i<j\le p-1}(\omega^j - \omega^i)$ [Vandermonde].

(i): Es gilt: $\left(\frac{q}{p}\right) = 1 \iff \sigma_q \in \langle\rho^2\rangle$ bzw. $\langle\sigma_q\rangle \subseteq \langle\rho^2\rangle$

$\iff \mathbb{Q}(\sqrt{p^*}) = K = \mathrm{Fix}(\rho^2) \subseteq \mathrm{Fix}(\sigma_q) \iff \sigma_q x = x$, mit $x := \sqrt{p^*}$.

Da $\sigma_q x = \pm x$ [bek. $\sigma_q|_K$, $K = \mathbb{Q}(x)$], folgt: $\sigma_q x = \left(\frac{q}{p}\right) x$.

Für $z = a_0 + a_1\omega + \ldots + a_{p-2}\omega^{p-2} \in \mathbb{Z}[\omega]$ gilt:

$\sigma_q z = a_0 + a_1\omega^q + \ldots + a_{p-2}\omega^{q(p-2)}$, d.h. $\forall z \in \mathbb{Z}[\omega]: \sigma_q z \equiv z^q \pmod{\mathbb{Z}[\omega]\cdot q}$.

Speziell folgt: $x^q \equiv \left(\frac{q}{p}\right) x \ (q)$.

Somit: $p^* \cdot (p^*)^{\frac{q-1}{2}} = (p^*)^{\frac{q+1}{2}} = x^{q+1} \equiv \left(\frac{q}{p}\right) x^2 = \left(\frac{q}{p}\right) p^* \ (q)$.

Da p^* Einheit mod q ist, folgt:

$$\left(\frac{q}{p}\right) \equiv (p^*)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} \underset{\text{Euler, 7.3(1)}}{\equiv} (-1)^{(p-1)(q-1)/4}\cdot\left(\frac{p}{q}\right) \ (q),$$

also $\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)$, da Terme ± 1, und $q > 2$.

(ii): s. 7.3 (1), □

(iii): Z.Z.: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Wie in (i) folgert man: $\left(\frac{2}{p}\right)=1 \Leftrightarrow \sigma_2\delta=\delta$, $\omega := e^{2\pi i/p}$, sei $L := \mathbb{Q}(\omega)$, haben $\sigma_2 \in Gal(L|\mathbb{Q})$ mit $\sigma_2\omega = \omega^2$, und $\delta = \prod_{1\le i<j\le p-1}(\omega^i-\omega^j)$, also $\sigma_2\delta = \left(\frac{2}{p}\right)\delta$. Nun ist $\sigma_2\delta = \sigma_2\left(\prod_{1\le i<j\le p-1}\omega^i-\omega^j\right) = \prod_{1\le i<j\le p-1}(\omega^{2i}-\omega^{2j})$, dabei durchlaufen die ω^{2i} die Potenzen $\omega, \omega^2, \dots, \omega^{p-1}$, d.h. σ_2 ist Permutation von $\{\omega,\dots,\omega^{p-1}\}$ [denn $\omega^{2i}=\omega^{2j} \Rightarrow \omega^{2(i-j)}=1 \Rightarrow p|i-j \Rightarrow i=j$.]

Diese induziert eine Permutation σ von $\{1,\dots,p-1\}$, und somit eine Permutation $\bar\sigma$ von $\{(i,j);\ 1\le i\ne j\le p-1\}$. Dabei ist $\delta = \prod_{\{i,j\}\subseteq\{1,\dots,p-1\},\ \#\{i,j\}=2} \Delta(\{i,j\})$, wo $\Delta(\{i,j\}) := \begin{cases}\omega^i-\omega^j, & i<j,\\ -(\omega^i-\omega^j), & i>j.\end{cases}$

Es gilt $\sigma_2\Delta(\{i,j\}) = \pm\Delta(\{\sigma i,\sigma j\})$,

daher ist $\sigma_2\delta = \varepsilon\delta$ mit $\varepsilon=(-1)^A$

und $A := \#\{\{i,j\}\subseteq\{1,\dots,p-1\};\ i\ne j,\ \Delta(\{i,j\}) = -\Delta(\{\sigma i,\sigma j\})\}$ (Vz.-Unterschied immer dann, wenn ein gerades $2i$ und ungerades $2j \bmod p$ zusammentreffen, $2j \pmod p < 2i$)

$= \sum_{i=1}^{\frac{p-1}{2}} \#\{j;\ p+1\le 2j\le 2i-1+p\} = \sum_{i=1}^{(p-1)/2} \#\{j;\ \frac{p+1}{2}\le j\le \frac{p+1}{2}-1+i\} = \sum_{i=1}^{(p-1)/2} i \underset{\text{kl. Gauß}}{=} \frac{1}{2}\cdot\frac{p-1}{2}\cdot\frac{p+1}{2} = \frac{p^2-1}{8}$.

Es folgt $\left(\frac{2}{p}\right)=\varepsilon=(-1)^{(p^2-1)/8}$. □

7.5. **Bsp.:** Es ist 1093 prim, ferner $\left(\frac{514}{1093}\right) \overset{\text{Euler 7.3(a)}}{\equiv} 514^{546} \ (1093)$.

Mit dem QRG folgt:

$\left(\frac{514}{1093}\right) = \left(\frac{2\cdot257}{1093}\right) = \underbrace{\left(\frac{2}{1093}\right)}_{=-1,\ 2.EG}\cdot\left(\frac{257}{1093}\right) \overset{QRG}{=} -\left(\frac{1093}{257}\right) \overset{\text{Reduktion mod 257}}{=} -\left(\frac{65}{257}\right) = -\left(\frac{5}{257}\right)\cdot\left(\frac{13}{257}\right)$ (Faktorisieren)

QRG & Reduzieren

$= -\left(\frac{2}{5}\right)\cdot\left(\frac{-3}{13}\right) = -\underbrace{\left(\frac{2}{5}\right)}_{=-1}\cdot\underbrace{\left(\frac{-1}{13}\right)}_{=1,\ 1.EG}\cdot\left(\frac{3}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{1}{3}\right) = 1$. Also ist 514 Quadrat mod 1093.

Erklären als Fortsetzung des Legendresymbols das Jacobisymbol (wo "Nenner" <0 erlaubt sind, im Gegensatz zu Def EZ11 !)

7.6. **Def.:** Seien $a,b\in\mathbb{Z}\setminus\{0\}$, $2\nmid b$, $(a,b)=1$.

Das **Jacobi-Symbol** $\left(\frac{a}{b}\right)$ (sprich "a nach b") ist def. als

$\left(\frac{a}{b}\right) := \prod_{p^{e(p)}\| b} \underbrace{\left(\frac{a}{p}\right)}_{\text{Legendre-Symbol}}^{e(p)}$, also z.B. $\left(\frac{3}{7\cdot5}\right) := \left(\frac{3}{7}\right)\cdot\left(\frac{3}{5}\right) = (-1)^2 = 1$.

	0	±1	±2	±3
□ mod 7:	0	↑	4	2
□ mod 5:	0	1	4	

Beachte: $\left(\frac{a}{-b}\right) = \left(\frac{a}{b}\right)$. Für $b=p$ prim ist $\left(\frac{a}{p}\right)_{Jacobi} = \left(\frac{a}{p}\right)_{Legendre}$.

Der Deutlichkeit halber kann auch $\left(\frac{a}{b}\right)_J$ und $\left(\frac{a}{p}\right)_L$ geschrieben werden.

7.7. **Eigenschaften:** (1) $a \equiv a' (b) \Rightarrow \left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$

(2) $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\cdot\left(\frac{a'}{b}\right)$, $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$

(3) $\left(\frac{x^2}{b}\right) = 1 = \left(\frac{a}{y^2}\right)$, $\left(\frac{ax^2}{b}\right) = \left(\frac{a}{b}\right) = \left(\frac{a}{by^2}\right)$, $(x,b)=1=(y,a)$, $2\nmid y$

(4) a qu. Rest mod $b \Rightarrow \left(\frac{a}{b}\right)=1$ $\quad\lceil c^2 \equiv a (b) \Rightarrow \forall p|b: c^2 \equiv a (p) \Rightarrow \forall p|b: \left(\frac{a}{p}\right)=1 \Rightarrow \left(\frac{a}{b}\right)=1\rfloor$

⚠ nicht „$\Leftarrow$", z.B.: $\left(\frac{3}{133}\right) = \left(\frac{3}{7\cdot 19}\right) = \left(\frac{3}{7}\right)\cdot\left(\frac{3}{19}\right) = (-1)\cdot\left(-\left(\frac{19}{3}\right)\right) \overset{\text{QRG}}{=} \left(\frac{1}{3}\right) = \left(\frac{1^2}{3}\right) = 1$, $\quad 19 \equiv 1 (3)$

aber 3 kein qu. Rest mod 133 (sonst 3 qu. Rest mod 7 u. 19).

7.8. **Satz (QRG für das Jacobisymbol):** $b \in \mathbb{Z}$, $2 \nmid b$. Dann:

1. EG: $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2} + \frac{\operatorname{sgn}(b)-1}{2}}$, für $b>0$: $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$

2. EG: $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$

QRG: $a \in \mathbb{Z}$, $2 \nmid a$, $(a,b)=1 \Rightarrow \left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2} + \frac{\operatorname{sgn}(a)-1}{2}\cdot\frac{\operatorname{sgn}(b)-1}{2}}$,

falls $a>0$ oder $b>0$: $\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$

7.9. **Bem.:** Das 1. EG ist im QRG enthalten: setze $a=-1$.

7.10. **Lemma:** $x,y \in \mathbb{Z}$, $2 \nmid xy$. Dann: (i): $\frac{xy-1}{2} \equiv \frac{x-1}{2} + \frac{y-1}{2}$ (2), und (ii): $\frac{(xy)^2-1}{8} \equiv \frac{x^2-1}{8} + \frac{y^2-1}{8}$ (2).

Bew.: (i) $\Leftrightarrow xy-1 \equiv x-1+y-1$ (4) $\Leftrightarrow (x-1)(y-1) \equiv 0$ (4) ✓

(ii) $\Leftrightarrow (xy)^2-1 \equiv x^2-1+y^2-1$ (16) $\Leftrightarrow (x^2-1)(y^2-1) \equiv 0$ (16) ✓ □

7.11. **Bew. des 1. EGs und 2. EGs:** r.S. und l.S. jeweils multiplikativ wegen Lemma 7.10.

Betr. OE nur die Fälle 1. $b = p \neq 2$ prim, 2. $b = -1$. Num: 1. bekannt, da dies das 1. EG für Legendre-symbol. Zu 2: $\left(\frac{-1}{-1}\right)=1$, $(-1)^{\frac{-1-1}{2} + \frac{\operatorname{sgn}(-1)+\operatorname{sgn}(-1)}{2}} = (-1)^{-1-1} = 1$. ✓ □

7.12. **Bew. des QRGs:** Sei $\Psi(a,b) := \left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right)$, $\varepsilon(a,b) := (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2} + \frac{\operatorname{sgn}(a)-1}{2}\cdot\frac{\operatorname{sgn}(b)-1}{2}}$.

Haben: Ψ, ε sind mult. in a und b (ε wegen Lemma 7.10), außerdem $\Psi(a,b) = \Psi(b,a)$, $\varepsilon(a,b) = \varepsilon(b,a)$.

$\rightsquigarrow$ ges. z.z.: (i) $\Psi(p,q) = \varepsilon(p,q)$ für $p,q \in \mathbb{P}\setminus\{2\}$, $p \neq q$, (ii) $\Psi(p,-1) = \varepsilon(p,-1)$, (iii) $\Psi(-1,-1) = \varepsilon(-1,-1)$.

(iii): klar, weil ist jeweils $=1$ ✓ (ii): $\varepsilon(p,-1) = (-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right) = \Psi(p,-1)$, (i): ist QRG für Legendre-Symbol. □

7.13. **Bsp.:** 1) $\left(\frac{219}{383}\right) \overset{\text{QRG}}{=} -\left(\frac{383}{219}\right) \overset{\text{reduz.}}{=} -\left(\frac{164}{219}\right) \overset{\text{zerraus}}{=} -\left(\frac{2^2\cdot 41}{219}\right) = -\left(\frac{41}{219}\right) \overset{\text{QRG}}{=} -\left(\frac{219}{41}\right) \overset{\text{reduz}}{=} -\left(\frac{14}{41}\right)$

$\overset{\text{zerraus}}{=} -\left(\frac{2}{41}\right)\cdot\left(\frac{7}{41}\right) \overset{2.\text{EG}}{=} -\left(\frac{7}{41}\right) \overset{\text{QRG}}{=} -\left(\frac{41}{7}\right) \overset{\text{reduz}}{=} -\left(\frac{-1}{7}\right) \overset{1.\text{EG}}{=} -(-1) = 1$,

also ist, da 383 prim, das Legendre-Symbol $= 1$, d.h. 219 ist qu. Rest mod 383.

2.) $\left(\frac{5}{1363}\right) \overset{QRG}{=} \left(\frac{1363}{5}\right)_{\text{mod } 5} \left(\frac{3}{5}\right) = -1$, also ist 5 qu. Nichtrest mod 1363 (obwohl $1363 = 29 \cdot 47$ nicht prim!)

3.) $\left(\frac{5}{219}\right) \overset{QRG}{=} \left(\frac{219}{5}\right) = \left(\frac{4}{5}\right) = 1$, dennoch ist 5 ein qu. Nichtrest mod 219. ($219 = 3 \cdot 73$)

[Logik: $\left(\frac{a}{b}\right) = 1$ und b prim $\Rightarrow$ a qu. Rest mod b heißt: a qu. Nichtrest mod b $\Rightarrow$ b zerges. oder $\left(\frac{a}{b}\right) = -1$.
$\left(\frac{a}{b}\right) = -1 \Rightarrow$ a qu. Nichtrest mod b heißt: a qu. Rest mod b $\Rightarrow$ $\left(\frac{a}{b}\right) = 1$, vgl. 7.7(4)]

7.14. **Bem.:** Das QRG für das Jacobisymbol ermöglicht uns, ein Legendre-Symbol $\left(\frac{a}{p}\right)$ ohne Faktorisierung des "Zählers" in Zwischenschritten auszurechnen, wie es sonst mit dem Legendre-Symbol nötig war (das QRG dafür war neu im Fall $\left(\frac{p}{q}\right)$, p, q beide prim, gültig). Damit kann $\left(\frac{a}{p}\right)$ algorithmisch leicht und schnell berechnet werden, d.h. entschieden werden, ob a ein qu. Rest mod p ist oder nicht! Wir wissen dann, dass $x^2 \equiv a \ (p)$ lösbar ist.
Wie eine solche (rein-) quadratische Kongruenz gelöst werden kann, sagen folgende Ergebnisse.
(Vgl. Einf. ZT, EZ11)

7.15. **Lösungen quadratischer Kongruenzen:** $x^2 \equiv a \bmod p$ für $p \equiv 3 \ (4)$ prim (leichte Fall).
Dabei sei a mit $p \nmid a$ ein quadratischer Rest mod p, d.h. so, dass es Lösungen gibt, d.h. es gilt $\left(\frac{a}{p}\right) = 1$. Da $\mathbb{F}_p$ Körper, gibt es nun zwei Lösungen $\pm b \ (p)$.
Nach dem Kleinen Fermat gilt $b^{4k+2} = b^{p-1} \equiv 1 \ (p)$. [$p = 3 + 4k$]
Es folgt: $(a^{k+1})^2 \equiv (b^2)^{2(k+1)} = b^{(4k+2)+2} \equiv 1 \cdot b^2 \equiv a \ (p)$,
d.h. die Lösungen von $b^2 \equiv a \ (p)$ sind $\boxed{b = \pm a^{k+1} \ (p)}$,
wo $a^{k+1} \ (p)$ mit schnellen Potenzieren berechnet werden kann.

7.16. **Lösungen quadratischer Kongruenzen:** $x^2 \equiv a \bmod p$ für $p \equiv 1 \ (4)$ prim (schwierigerfall):
Sei davon die Kongruenz wieder lösbar, o.E. $p \nmid a$ mit $\left(\frac{a}{p}\right) = 1$.
Weiter betr. ein $b \in \mathbb{N}$ mit $1 \leq b < p$, $(b^2 - a, p) = 1$ und $\left(\frac{b^2-a}{p}\right) = -1$
Sei nun $D \in \mathbb{N}$ mit $1 \leq D < p$ geg. mit $D \equiv b^2 - a \ (p)$.
Betrachte $\mathbb{F}_p[\sqrt{D}] := \{u + v\sqrt{D} : u, v \in \mathbb{F}_p\}$ mit der offensichtlichen Addition/Multiplikation versehen. (Ist isomorph $\mathbb{F}_{p^2}$!)
Berechne $X := (b + 1 \cdot \sqrt{D})^{\frac{p+1}{2}} \in \mathbb{F}_p[\sqrt{D}]$.
Beh.: (1) $X \in \mathbb{F}_p$, für alle $x \in X$ (d.h. $X = x$ in $\mathbb{F}_p$, $x \in \mathbb{Z}$) gilt $(\pm x)^2 \equiv a \ (p)$.
(2) $\#\{b \in \mathbb{N} : b < p, (b^2 - a, p) = 1, \left(\frac{b^2-a}{p}\right) = -1\} \geq \frac{p-3}{2}$.
Bew.: Nur (1): $X^2 = (b + 1\sqrt{D})^{p+1} = (b - 1\sqrt{D})(b + 1\sqrt{D}) = b^2 - D \cdot 1 = b^2 - (b^2 - a) = a$ in $\mathbb{F}_p[\sqrt{D}]$. □