K6

Vorlesung Kryptographie

WiSe'23/'24, hhu
K. Halupczok

K6: Quadratische Reste und Kongruenzen

Stichworte: Jacobi-Symbol, schnelle Berechnung des Jacobi- und Legendresymbols, Lösung quadratischer Kongruenzen mod $p \equiv 3\ (4)$.

6.1. **Einleitung:** In K3 sahen wir, dass bestimmte Kryptoverfahren von der Berechnung modularer Quadratwurzeln abhängen. Dies ist von genereller Bedeutung für die algorithmische ZT: speziell, dass mit dem Jacobisymbol algorithmisch schnell entschieden werden kann, ob a ein qR (= quadratischer Rest) mod p ist oder nicht.

6.2. **Erinnerung:** Hatten das Legendre-Symbol: $2 \nmid p$, $a \in \mathbb{Z}$, $p \nmid a$:
$\left(\frac{a}{p}\right) := 1$, falls $x^2 \equiv a\ (p)$ lösbar (d.h. a qu. Rest mod p), $\left(\frac{a}{p}\right) := -1$ sonst (d.h. a qu. Nichtrest).

Eigenschaften: QRG $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$, 1. EG: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, 2. EG: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Euler-Krit.: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (p)$, weiter: $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$ ⌜vgl. EZ10⌟

6.3. **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. $\left(\frac{3}{7\cdot 5}\right) := \left(\frac{3}{7}\right)\cdot\left(\frac{3}{5}\right) = (-1)^2 = 1.$

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

Beachte: $\left(\frac{a}{-b}\right) = \left(\frac{a}{b}\right)$. Für $b = p$ prim ist $\left(\frac{a}{p}\right)_{\text{Jacobi}} = \left(\frac{a}{p}\right)_{\text{Legendre}}$.
Haben so eine Fortsetzung des Legendre-Symbols erklärt.

6.4. **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 $b \Rightarrow \left(\frac{a}{b}\right) = 1$ ⌜$c^2 \equiv a\ (b) \Rightarrow \forall p \mid b: c^2 \equiv a\ (p) \Rightarrow \forall p \mid b: \left(\frac{a}{p}\right) = 1 \Rightarrow \left(\frac{a}{b}\right) = 1$⌟

⚠ nicht „⇐", z.B.: $\left(\frac{3}{133}\right) = \left(\frac{3}{7\cdot 19}\right) = \left(\frac{3}{7}\right)\cdot\left(\frac{3}{19}\right) = (-1)\cdot\underbrace{\left(-\left(\frac{19}{3}\right)\right)}_{\text{nach QRG}} \underset{19\equiv 1(3)}{=} \left(\frac{1}{3}\right) = \left(\frac{1^2}{3}\right) = 1$,
aber 3 kein qu. Rest mod 133 (sonst 3 qu. Rest mod 7 ↯).

Zeigen nun:

6.5. <u>Satz (QRG für das Jacobisymbol)</u>: $b \in \mathbb{Z}$, $2 \nmid b$. 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 $b>0$: $\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$

<u>Bem.:</u> Das 1.EG ist im QRG enthalten: setze $a=-1$.

Zum Beweis erst ein Lemma:

6.6. <u>Lemma:</u> $x,y \in \mathbb{Z}$, $2 \nmid xy$. 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).

<u>Bew.:</u> (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) ✓ □

Beweis von <u>Satz 6.5</u>:

<u>Bew. des 1.EGs und 2.EGs:</u> r.S. und l.S. jeweils multiplikativ wegen <u>Lemma 6.6</u>

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

<u>Bew. des QRGs:</u> 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 <u>Lemma 6.6</u>), außerdem $\Psi(a,b) = \Psi(b,a)$, $\varepsilon(a,b) = \varepsilon(b,a)$.

$\rightsquigarrow$ gen. 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, Wert 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. □

6.7. <u>Bem.:</u> Im Gegensatz zum Legendresymbol lassen wir im "Nenner" auch negative ungerade Zahlen zu. Es gibt noch eine Erweiterung auf gerade Zahlen im "Nenner", nämlich das Kroneckersymbol, s. z.B. <u>[O. Bordellès: Arithmetic Tales, §7.3.7]</u>. Es spielt in der algorithmischen ZT eher eine untergeordnete Rolle; das Jacobisymbol und seine "guten" rechnerischen Eigenschaften reichen für fast alles meistens aus.

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

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

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

2.) $\left(\frac{5}{1363}\right) \overset{QRG}{=} \left(\frac{1363}{5}\right) \underset{reduz}{=} \left(\frac{3}{5}\right) = -1$, 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 $b \Rightarrow b$ zerlegb. 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. 6.4.(4)⌋

6.9. **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 nur im Fall $\left(\frac{p}{q}\right)$, p, q beide prim >2, gültig). Selbst $\left(\frac{a}{b}\right)$ kann algorithmisch leicht und schnell berechnet werden, ohne je einen Primzahltest mit a, b durchführen zu müssen. Falls $b = p$ prim ist, kann so leicht entschieden werden, ob a ein qu.Rest mod p ist oder nicht. Wir wissen dann, dass $\boxed{x^2 \equiv a\ (p)}$ lösbar ist, aber es sagt leider nichts darüber aus, wie eine solche (rein-)quadratische Kongruenz gelöst werden kann. In 3.18 haben wir recht einfach Lösungen im Fall $p \equiv 3\ (4)$ finden können. Wir behandeln noch den etwas "schwierigen" Fall $p \equiv 1\ (4)$, bei dem das Konzept eines endlichen Körpers $\mathbb{F}_{p^2}$ angewendet wird. Für b nicht prim ist die Lösung von $x^2 \equiv a\ (b)$ so schwer wie b zu faktorisieren.

vgl. [Crandall/Pomerance: primenumbers] • Die Berechnung von $\left(\frac{a}{p}\right)$ mit 6.5 benötigt $O(\lg^2(p))$ Bitop., die mit $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (p)$ braucht $O(\lg^3(p))$ viele.

6.10. **Lösungen quadratischer Kongruenzen:** $x^2 \equiv a \bmod p$ für $p \equiv 1\ (4)$ prim ("schwieriger Fall"):

Sei davon die Kongruenz wieder lösbar, OE $p \nmid a$ mit $\left(\frac{a}{p}\right) = 1$.

Weiter betr. ein $b \in \mathbb{N}$ mit $1 \le b < p$, $(b^2 - a, p) = 1$ und $\left(\frac{b^2-a}{p}\right) = -1$

Sei nun $D \in \mathbb{N}$ mit $1 \le D < p$ 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.

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. $X = \underline{x}$ in $\mathbb{F}_p$, $x \in \mathbb{Z}$) gilt $(\pm x)^2 \equiv a\ (p)$.

(2) $\#\{b \in \mathbb{N};\ b < p,\ (b^2 - a, p) = 1,\ \left(\frac{b^2-a}{p}\right) = -1\} \ge \frac{p-3}{2}$.

6.11. **Bem.:** • Teil (2) besagt, dass es viele Reste b mod p mit der verlangten Eigenschaft gibt, so dass die zufällige Wahl irgendeines Restes b mod p wahrscheinlich zu einem passenden b führt: Falls nicht, wähle ein neues b zufällig, solange bis eines gefunden wird. Wegen (2) braucht man im Schnitt nur etwa 2 Versuche, bis man so Erfolg hat.

• X kann in $\mathbb{F}_p[\sqrt{D}]$ durch schnelles Potenzieren schnell berechnet werden.

• Der Ring $\mathbb{F}_p[\sqrt{D}]$ ist gleichzeitig der Körper $\mathbb{F}_p(\sqrt{D})$, nämlich bis auf Isomorphie der Körper $\mathbb{F}_{p^2}$ vom Grad 2 über $\mathbb{F}_p$, vgl. Algebra A21.

6.12. Zur Erläuterung, wie in $\mathbb{F}_p[\sqrt{D}]$ invertiert wird:
Sei $u+v\sqrt{D} \in \mathbb{F}_p[\sqrt{D}]$, $u+v\sqrt{D} \neq 0$. Dann ist $(u^2-Dv^2, p)=1$, denn wäre $Dv^2 \equiv u^2\ (p)$, wäre $1=\left(\frac{Dv^2}{p}\right)=\left(\frac{D}{p}\right)=\left(\frac{b^2-a}{p}\right)=-1$ ↯. Also sei $A^* \in \mathbb{Z}$ mit $A^* \cdot (u^2-Dv^2) \equiv 1\ (p)$, d.h. das Inverse von u^2-Dv^2 mod p.
Dann: $(u+v\sqrt{D})\cdot(A^*u-A^*v\sqrt{D}) = A^*u^2-A^*v^2D = A^*(u^2-Dv^2)=1$,
also: $(u+v\sqrt{D})^{-1} = A^*u - A^*v\sqrt{D}$ in $\mathbb{F}_p[\sqrt{D}]$. $\left[\hat{=}\ \frac{u-v\sqrt{D}}{u^2-Dv^2}\right]$

6.13. **Bsp.:** Sei $p=17$, $a=8$, gesucht: Lsgn. $\pm x$ von $x^2 \equiv 8\ (17)$.
Haben $\left(\frac{a}{p}\right)=\left(\frac{8}{17}\right)=\left(\frac{2^2\cdot 2}{17}\right)=\left(\frac{2}{17}\right) \overset{2.\,EG}{=} (-1)^{\frac{17^2-1}{8}} = 1$, also ex. Lsgn.
Finde b: probiere $b=1$: $\left(\frac{1^2-8}{17}\right)=\left(\frac{-1}{17}\right)\cdot\left(\frac{7}{17}\right)=(-1)^{\frac{17-1}{2}}\cdot\left(\frac{17}{7}\right)=\left(\frac{3}{7}\right)=-1$
Treffer! Seien also $D \equiv 1^2-8 \equiv -7 \equiv 10\ (17)$, also $D=10$,
und $X := (b+1\sqrt{D})^{\frac{17+1}{2}} = (1+1\sqrt{10})^9$.

x	0	± 1	± 2	± 3
x^2	0	1	4	2

Quadrate mod 7

Schnelles Potenzieren: $X^2 = 1+2\sqrt{10}+10 = 11+2\sqrt{10}$,
$X^4 = 11^2+44\sqrt{10}+40 = 8+10\sqrt{10}$, $X^8 = (8+10\sqrt{10})^2 = 64+160\sqrt{10}+1000$
$= 10+7\sqrt{10}$, $X^9 = (10+7\sqrt{10})(1+1\sqrt{10}) = 10+17\sqrt{10}+70 = 80 = 12$.
Es ist also $\underline{\underline{x = \pm 12\ (17)}}$ das Lösungspaar: $x^2 \equiv 12^2 \equiv 8\ (17)$, $(\underbrace{-12}_{5})^2 \underset{\hat{=}25}{\equiv} 8\ (17)$ ✓.
(bzw. $\underline{\underline{\pm 5\ (17)}}$, da $\pm 12 \equiv \mp 5\ (17)$)

6.14. Bew. von 6.10: Zu (1): Für alle $u, v \in \mathbb{F}_p[\sqrt{D}]$ gilt (in $\mathbb{F}_p[\sqrt{D}]$):

$$(u + v\sqrt{D})^p = \sum_{j=0}^{p} \underbrace{\binom{p}{j}}_{\substack{=0 \text{ für } 1 \le j \le p-1, \text{ da dann } p \mid \binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j!} \checkmark}} u^j (v\sqrt{D})^{p-j} = u^p + v^p (\sqrt{D})^p$$

$$= u + v \cdot D^{\frac{p-1}{2}} \sqrt{D} = u + -v \cdot \sqrt{D}.$$

da $u^p \equiv u\ (p)$, $v^p \equiv v\ (p)$; da laut Euler-Krit.: $D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \underset{\text{Wahl von } b}{=} -1\ (p)$,

Damit folgt in $\mathbb{F}_p[\sqrt{D}]$:

$$x^2 = (b + 1\sqrt{D})^{p+1} = (b + (-1)\sqrt{D}) \cdot (b + 1\sqrt{D}) = b^2 - D = a.$$

Die Glg. $x^2 = a$ hat im Körper $\mathbb{F}_p[\sqrt{D}]$ höchstens zwei Lösungen.

⌜ $x^2 - c^2 = 0 \iff (x-c)\cdot(x+c) = 0 \underset{\text{Körper}}{\iff} x = \pm c$ ⌟

Diese hat aber schon im Teilkörper $\mathbb{F}_p$ zwei Lösungen, da $\left(\frac{a}{p}\right) = 1$, $p \nmid a$.

Lösungen in $\mathbb{F}_p[\sqrt{D}]$ sind also schon Elemente von $\mathbb{F}_p$, d.h. $\pm x \in \mathbb{F}_p$.

Zu (2): Betr. die Normabb. $N: \mathbb{F}_p[\sqrt{D'}] \to \mathbb{F}_p$, $N(u + v\sqrt{D'}) = u^2 - D'v^2$, wo $\left(\frac{D'}{p}\right) = -1$.

Für alle $b \in \mathbb{Z}$, $v \in \mathbb{Z}$, $p \nmid v$, mit $N(b + v\sqrt{D'}) = a$ gilt:

$$v^2 D' = b^2 - (b^2 - D'v^2) = b^2 - N(b + v\sqrt{D'}) = b^2 - a = b^2 - a.$$

Dann ist: $\left(\frac{b^2-a}{p}\right) = \left(\frac{v^2 D'}{p}\right) = \left(\frac{D'}{p}\right) = -1$. Betr. $M := \{\xi \in \mathbb{F}_p[\sqrt{D'}];\ N(\xi) = a\}$.

Haben $N(u + v\sqrt{D'}) = u^2 - v^2 D' = (u - v\sqrt{D'})(u + v\sqrt{D'}) = (u + v\sqrt{D'})^{p+1}$ nach obigem,

d.h. $\xi \in M \iff N(\xi) = a \iff a^{-1} \cdot N(\xi) = 1 \iff a^{-1} \cdot \xi^{p+1} = 1$, d.h. $M = \ker(a^{-1}N)$.

Da $\xi^{p+1} - a = 0$ höchst. $p+1$ Lösungen hat ($\mathbb{F}_p(\sqrt{D'})$ Körper), ist $\#\ker(a^{-1}N) \le p+1$.

$\overset{\text{Hom-Satz}}{\leadsto}$ $\mathbb{F}_p[\sqrt{D'}]^\times / \ker(a^{-1}N) \cong \operatorname{im}(a^{-1}N) \Rightarrow p^2 - 1 = \#\mathbb{F}_p(\sqrt{D'})^\times \le \#\operatorname{im}(a^{-1}N) \cdot (p+1) \le (p-1)(p+1)$.

Weil hier Gleichheit gilt, ist $\#M = \#\ker(a^{-1}N) = p+1$.

Nun ist $\#(M \cap \mathbb{F}_p) \le 2$, da $N(x) = x^2$ für $x \in \mathbb{F}_p$, in $\mathbb{F}_p$ hat $x^2 - a = 0$ höchst. 2 Lsgn.

Für $b, v_1, v_2 \in \mathbb{F}_p$ ist $N(b + v_1\sqrt{D'}) = N(b + v_2\sqrt{D'}) \iff b^2 - D'v_1^2 = b^2 - D'v_2^2 \iff v_1 = \pm v_2$.

Also ex. $\ge \frac{\#M}{2} - 2 = \frac{p+1}{2} - 2 = \frac{p-3}{2}$ viele b mit $N(b + v\sqrt{D'}) = a$ für ein $v \in \mathbb{F}_p$. □