WiSe '21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ 11: Modulares Wurzelziehen und das Jacobisymbol

Stichworte: explizite Bestimmung der Lösungen von $x^2 \equiv a\ (p)$, Rechnen in $\mathbb{F}_{p^2}$ über $\mathbb{F}_p$, Jacobisymbol als Fortsetzung des Legendresymbols, QRG und EGe für das Jacobisymbol, schnelle Berechnung des Jacobisymbols

---

11.1. Einleitung:

Wir geben zunächst Verfahren zur expliziten Berechnung der Lösungen von $x^2 \equiv a\ (p)$ im Fall $\left(\frac{a}{p}\right) = 1$ an, welche algorithmisch machbar und effektiv in der Praxis funktionieren. Eine Konstruktion mit PW und dlog wie in EZ 9 ist dabei i.a. leider nicht hilfreich, da die dlog-Berechnung i.a. algorithmisch nicht machbar ist. Der folgende Fall ist einfach, denn $a^{\frac{p+1}{4}}$ ist mit schnellem Potenzieren leicht und schnell zu berechnen.

11.2. Satz: Sei $p \in \mathbb{P}$, $p \equiv 3\ (4)$, $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = 1$.
Dann hat $x^2 \equiv a\ (p)$ die Lösungen $x_{1,2} \equiv \pm a^{\frac{p+1}{4}}\ (p)$.

Bew.: Haben $x_{1,2}^2 \equiv \left(\pm a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}} \equiv a \cdot \left(\frac{a}{p}\right) = a\ (p)$.
($\uparrow$ Expon. $\in \mathbb{Z}$, da $p \equiv 3\ (4)$; $\uparrow$ Euler-Kriterium) □

Der Fall $p \equiv 1\ (4)$ ist i.a. jedoch nicht mit a-Potenzen zu behandeln.
Wir gehen stattdessen in den Erweiterungskörper $\mathbb{F}_{p^2}$ von $\mathbb{F}_p = \mathbb{Z}/p$ über, in dem eine einfache Lösungsmöglichkeit existiert.

11.3. Def.: Für $d \in \mathbb{Z}$, $p \nmid d$, d ein qNR mod p,
setze $R_d := (\mathbb{Z}/p)[\sqrt{d}] := \{u + v\sqrt{d};\ u, v \in \mathbb{Z}/p\}$.
Dann ist R_d mit den Verknüpfungen

$$(u_1 + v_1\sqrt{d}) + (u_2 + v_2\sqrt{d}) := (u_1 + u_2) + (v_1 + v_2)\sqrt{d},$$

$$(u_1 + v_1\sqrt{d}) \cdot (u_2 + v_2\sqrt{d}) := (u_1 u_2 + d v_1 v_2) + (u_1 v_2 + u_2 v_1)\sqrt{d}$$

ein kommutativer Ring mit Einselement $1 + 0\sqrt{d} = 1$.
[klar]

11.4. **Satz:** R_d ist sogar Körper, denn jedes $u+v\sqrt{d} \in R_d \setminus \{0\}$ hat das inverse Element $zu - zv\sqrt{d}$, wenn $z\cdot(u^2-dv^2) \equiv 1 \ (p)$ gilt, d.h. $z \equiv (u^2-dv^2)^{-1} \ (p)$.

Bew.: • z ist wohldef., d.h. $p \nmid u^2 - dv^2$: Wäre sonst $u^2 \equiv dv^2 \ (p)$, wäre $1 = \left(\frac{dv^2}{p}\right) = \left(\frac{d}{p}\right)\cdot\left(\frac{v^2}{p}\right) = (-1)\cdot 1 = -1$ weil d qNR mod p ist, $\lightning$.

• Man hat $(u+v\sqrt{d})\cdot(zu - zv\sqrt{d}) = (zu^2 - zdv^2) + (zuv - uzv)\sqrt{d}$
$= z\cdot(u^2-dv^2) = 1$. ($uzv - uzv = 0$) □

11.5. **Bem.:** Somit ist R_d ein Körper mit $\#R = p^2$, also $R_d \cong \mathbb{F}_{p^2}$ (bis auf Isomorphie eindeutig bestimmt kont Algebra). Man kann in R_d die Glg. $x^2 = a$ explizit lösen, nach dem Satz von Lagrange 8.6 gibt es in R_d maximal zwei Lösungen. Hat $x^2 = a$ bereits in $\mathbb{Z}/p \subseteq R_d$ zwei Lösungen, stimmen diese mit denen in R_d überein. Diese Idee führt zu folgendem Verfahren (das auch für $p \equiv 3 \ (4)$ funktioniert, was wegen Satz 11.2 aber entbehrlich ist in diesem Fall):

11.6. **Satz:** Sei $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = 1$. Sei $b \in \mathbb{N}$, $b < p$, $\left(\frac{b^2-a}{p}\right) = -1$.
Mit $D := b^2 - a \ (p)$ setze R_D wie in Def. 11.3, ist Körper laut 11.4.
Setze $x := \left(b + 1\cdot\sqrt{D}\right)^{\frac{p+1}{2}} \in R_D$, ist explizit/schnell berechenbar durch schnelles Potenzieren in R_D.

Dann ist $x \in \mathbb{Z}/p$ (d.h. der Teil mit $\sqrt{D}$ ist gleich 0),
und es gilt $(\pm x)^2 \equiv a \ (p)$.

Bew.: 1.) Für alle $u, v \in \mathbb{Z}/p$ ist

$$(u+v\sqrt{D})^p = \sum_{j=0}^{p} \binom{p}{j} u^j \left(v\sqrt{D}\right)^{p-j} = u^p + v^p \left(\sqrt{D}\right)^p + \underbrace{\sum_{j=1}^{p-1} \binom{p}{j} u^j \left(v\sqrt{D}\right)^{p-j}}_{=0,\ \text{da } p \mid \binom{p}{j} \text{ für } 1 \le j < p}$$

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

($u^p = u$, $v^p = v$ nach kleinem Fermat; $D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) = -1 \ (p)$ ↑ Interlevkrit. 10.10)

2.) Damit folgt $x^2 = \left(\left(b+1\sqrt{D}\right)^{\frac{p+1}{2}}\right)^2 = \left(b+1\sqrt{D}\right)^{p+1} = \left(b+1\sqrt{D}\right)^p \cdot \left(b+1\sqrt{D}\right)$
$\overset{1.)}{=} \left(b + (-1)\sqrt{D}\right)\cdot\left(b+1\sqrt{D}\right) = b^2 - D\cdot 1 = b^2 - D = a$ laut Def. von D.

3.) Nach dem Satz von Lagrange 8.6 gibt es im Körper R_D höchstens zwei Lösungen. Wegen $\left(\frac{a}{p}\right) = 1$ gibt es schon zwei in $\mathbb{Z}/p \subseteq R_D$. Damit sind die R_D-Lösungen schon genau die $\mathbb{Z}/p$-Lösungen, sie liegen also in $\mathbb{Z}/p$. □

11.7. **Bsp.:** Sei $p=17$, $a=8$. Gesucht sind alle $x \in \mathbb{N}$ mit $x^2 \equiv 8 \ (17)$.

Es ist $\left(\frac{a}{p}\right) = \left(\frac{8}{17}\right) = \left(\frac{2^2}{17}\right)\cdot\left(\frac{2}{17}\right) = 1 \cdot (-1)^{\frac{17^2-1}{8}} = (-1)^{(17-1)(17+1)/8} = (-1)^{2\cdot 18} = 1$,

also ex. Lösungen. Probiere nun $b := 1$.

Es ist $\left(\frac{1^2-8}{17}\right) = \left(\frac{-1}{17}\right)\cdot\left(\frac{7}{17}\right) = (-1)^{\frac{17-1}{2}} \cdot \left(\frac{17}{7}\right) = 1\cdot\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$. ✓

Sei also $D := 10 \equiv -7 \equiv 1^2 - 8 \ (17)$, $R_{10} := (\mathbb{Z}/17)[\sqrt{10}]$ (schreibe nun R),

und $\xi := b + 1\sqrt{D} = 1 + 1\sqrt{10} \in R$.

Zu berechnen ist $x = \xi^{\frac{17+1}{2}} = \xi^9$. Mit schnellem Potenzieren folgt

$\xi^2 = (1+1\sqrt{10})^2 = 1^2 + 2\cdot 1\cdot 1\sqrt{10} + 1^2\cdot 10 = 11 + 2\sqrt{10}$,

$\xi^4 = (11 + 2\sqrt{10})^2 = 11^2 + 2\cdot 11\cdot 2\sqrt{10} + 2^2\cdot 10 = 8 + 10\sqrt{10}$,

$\xi^8 = (8 + 10\sqrt{10})^2 = 8^2 + 2\cdot 8\cdot 10\sqrt{10} + 10^2\cdot 10 = 64 + 160\sqrt{10} + 1000 = 10 + 7\sqrt{10}$

und $\xi^9 = \xi^8\cdot\xi = (10+7\sqrt{10})(1+1\sqrt{10}) = 10 + 70 + 7\cdot 1\sqrt{10} + 10\cdot 1\sqrt{10} = 12 + 0\cdot\sqrt{10} = 12$.

Es ist also $(\pm 12)^2 = 144 \equiv 8 \ (17)$, beachte: $-12 \equiv 5 \ (17)$ gibt $5^2 \equiv 25 \equiv 8 \ (17)$.

11.8. **Bem.:** Wie im Bsp. 11.7 deutlich wird, ist das Verfahren von Satz 11.6 möglich, wenn ein passendes b mit $\left(\frac{b^2-a}{p}\right) = -1$ gefunden wird. Der folgende Satz zeigt, dass die Treffsicherheit bei (zufälligem) Suchen eines b bei ungefähr 50% liegt. Es sind im Mittel also etwa 2 Versuche nötig, um b zu finden, was für die Praxis völlig ausreichend ist.

11.9. **Satz:** Sei $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = 1$.

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

Zum Beweis wird folgender Begriff benötigt.

11.10. **Def.:** Sei $d \in \mathbb{N}$, $d < p$, $\left(\frac{d}{p}\right) = -1$. Betrachte den Körper R_d laut Satz 11.4.

Die Abbildung $N : R_d \to \mathbb{Z}/p$

$$u + v\sqrt{d} \mapsto N(u+v\sqrt{d}) := u^2 - dv^2$$

heißt Normabbildung bzw. Norm auf R_d.

11.11. **Lemma:** Sei N die Norm aus Def. 11.10. Dann ist $N(u+v\sqrt{d}) = (u+v\sqrt{d})^{p+1}$.

Bew: $(u+v\sqrt{d})^{p+1} = (u+v\sqrt{d})^p\cdot(u+v\sqrt{d}) \overset{11.6.1)}{=} (u - v\sqrt{d})\cdot(u+v\sqrt{d})$

$= u^2 + v^2 d = N(u+v\sqrt{d})$. □

11.12. Bew. von 11.9.: Seien also $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = 1$, und $d \in \mathbb{N}$ mit $\left(\frac{d}{p}\right) = -1$ beliebig.

- Für alle $b \in \mathbb{Z}$, $v \in \mathbb{Z}$ mit $p \nmid v$ und $N(b + v\sqrt{d}) = a$ gilt nun

$$v^2 d = (b + v\sqrt{d} - b)^2 = (b + v\sqrt{d})^2 - 2b \cdot (b + v\sqrt{d}) + b^2$$
$$= b^2 + 2bv\sqrt{d} + v^2 d - 2b^2 - 2bv\sqrt{d} + b^2$$
$$= -(b^2 - dv^2) + b^2 = b^2 - N(b + v\sqrt{d}) = b^2 - a.$$

Wegen $\left(\frac{dv^2}{p}\right) = \left(\frac{d}{p}\right) \cdot \left(\frac{v^2}{p}\right) = (-1) \cdot 1 = -1$ für alle $v \in \mathbb{Z}$, $p \nmid v$, ist also $\left(\frac{b^2 - a}{p}\right) = -1$, also b wie gewünscht, sofern nur $N(b + v\sqrt{d}) = a$. ←

Daher ist die Anzahl der $\xi = b + v\sqrt{d}$ zu bestimmen, für die dies zutrifft.

- Sei $\mathcal{M} := \{\xi \in R_d^* ; N(\xi) = a\}$.

Dann ist $\xi \in \mathcal{M} \Leftrightarrow N(\xi) = a \Leftrightarrow \bar{a}^{-1} \cdot \overbrace{N(\xi)}^{= \xi^{p+1} \text{ nach 11.11}} = 1 \Leftrightarrow \xi^{p+1} - a = 0$ (*),

dabei ist $\bar{a}^{-1}$ das Inverse von $\bar{a}$ in $\mathbb{Z}/p$.

Also betr. $\mathcal{M} = \{\xi \in R_d^* ; \bar{a}^{-1} N(\xi) = 1\} = \ker(\bar{a}^{-1} \cdot N)$,

wo $\bar{a}^{-1} \cdot N : \underbrace{R_d^*}_{= R_d \setminus \{0\}} \to (\mathbb{Z}/p)^*, \xi \mapsto \bar{a}^{-1} \cdot N(\xi)$, bzgl. $\cdot$ ein Gruppenhom. ist.

Da (*) nach dem Satz von Lagrange 8.6 höchstens $p+1$ Lösungen hat, folgt $\#\ker(\bar{a}^{-1} \cdot N) \leq p+1$, und da $\bar{a}^{-1} \cdot N(\xi) \in (\mathbb{Z}/p)^*$

ist $\#\operatorname{im}(\bar{a}^{-1} N) \leq \#(\mathbb{Z}/p)^* = p - 1$.

Mit dem Homomorphiesatz der Algebra folgt $(R_d^*)/\ker \bar{a}^{-1} N \cong \operatorname{im} \bar{a}^{-1} N$

bzw. $R_d^* \cong \operatorname{im} \bar{a}^{-1} N \times \ker \bar{a}^{-1} N$, also $(p-1)(p+1) = p^2 - 1 = \#(R_d^*)$

$$= \#\operatorname{im}(\bar{a}^{-1} N) \cdot \#\ker(\bar{a}^{-1} N) \leq (p-1)(p+1).$$

(↑ Hom.Satz)

$R_d^* \xrightarrow{\bar{a}^{-1}N} \operatorname{im} \bar{a}^{-1} N \subseteq \mathbb{Z}/p$
$\downarrow$ $\quad \nearrow \cong$
$R_d^*/\ker \bar{a}^{-1} N$

Damit folgt Gleichheit.

Es ergibt sich $\#\ker(\bar{a}^{-1} N) = p+1$, $\#\operatorname{im}(\bar{a}^{-1} N) = p-1$, und $\#\mathcal{M} = p+1$.

- Es ist $\#(\mathcal{M} \cap (\mathbb{Z}/p)) \leq 2$, denn für ein $\bar{x} \in \mathbb{Z}/p$ ist $N(\bar{x}) = \bar{x}^2$,

und nach dem Satz von Lagrange 8.6 hat $y^2 - \bar{a} = 0$ im Körper $\mathbb{Z}/p$ höchstens 2 Lösungen.

- Für alle $b, v_1, v_2 \in \mathbb{Z}$ ist $N(b + v_1\sqrt{d}) = N(b + v_2\sqrt{d}) \Leftrightarrow b^2 - dv_1^2 = b^2 - dv_2^2$

$$\Leftrightarrow v_1 = \pm v_2.$$

- Also gibt es mindestens $\frac{\#\mathcal{M}}{2} - \underbrace{2}_{\text{nicht die mit } v=0} = \frac{p+1}{2} - 2 = \frac{p-3}{2}$ viele b,

$\underbrace{\quad}_{\text{wegen } v_1 = \pm v_2 \neq 0}$

so dass es ein $v \in \mathbb{Z}$, $p \nmid v$, gibt mit $N(b + v\sqrt{d}) = a$ und $\left(\frac{b^2 - a}{p}\right) = 1$. □

Ein weiteres algorithmisches Hindernis stellen noch die Berechnungen von Legendresymbolen dar, weil dafür i.a. faktorisiert werden muss. Dies wird durch die Fortsetzung des Symbols zum Jacobisymbol umgangen.

11.13. **Def.** (Jacobisymbol): Sei $m \in \mathbb{N}_{>1}$, $2 \nmid m$, $m = \prod_p p^{e_p}$ die PFZ von m und $a \in \mathbb{Z}$ mit $(a,m) = 1$. Dann wird das Jacobisymbol definiert durch

$$\left(\frac{a}{m}\right)_J := \prod_{\substack{p \\ (a,p)=1}} \left(\frac{a}{p}\right)^{e_p}.$$

Wir nennen a den Zähler und m den Nenner des Symbols $\left(\frac{a}{m}\right)$.

11.14. **Bem.:** 1.) Für $m \in \mathbb{P} \setminus \{2\}$ stimmen die Symbole überein. Wir schreiben den Index J hier zur Unterscheidung. Normalerweise werden die Symbole gleichermaßen benutzt, da i.a. keine Verwechslung zu befürchten ist; im Zweifelsfall liegt das Jacobisymbol vor. Es kann auch durch $\left(\frac{a}{m}\right) = \left(\frac{a}{-m}\right)$ zu negativen Nennern erweitert werden (tun wir hier nicht).

2.) Für zusammengesetztes $m \in \mathbb{N} \setminus \mathbb{P}$, $m \neq 1$, bedeutet $\left(\frac{a}{m}\right) = 1$ nicht notwendig, dass die Kongruenz $x^2 \equiv a \ (m)$ lösbar ist. Diese "Deutung" des Legendresymbols geht also beim Jacobisymbol verloren. Z.B. ist $\left(\frac{2}{9}\right) = 1$, aber $x^2 \not\equiv 2 \ (9)$ für alle $x \in \mathbb{Z}$.
Man hat: a qR mod $m \not\Rightarrow \left(\frac{a}{m}\right) = 1$.
Ist ein Jacobisymbol aber gleich einem Legendresymbol, wenn der Nenner des Symbols einen Primzahltest bestanden hat, so gilt die Deutung "wieder".

3.) Die Definition des Jacobisymbol hängt von der Faktorisierung des Nenners m ab. Dass dieses stets schnell berechnet werden kann, ist anhand der Def. nicht klar, sondern erst ein Ergebnis von Satz 11.15.

11.15. **Satz** (Rechenregeln für das Jacobisymbol): Seien $m,n \in \mathbb{N}_{>1}$, $2 \nmid mn$, $a,b \in \mathbb{Z}$, $(ab, mn) = 1$.
Dann gilt:

(1) $\left(\frac{a}{m}\right)_J = \left(\frac{b}{m}\right)_J$, falls $a \equiv b \ (m)$ ist,

(2) $\left(\frac{ab}{m}\right)_J = \left(\frac{a}{m}\right)_J \cdot \left(\frac{b}{m}\right)_J$

(3) $\left(\frac{a^2}{m}\right)_J = 1$

(4) $\left(\frac{a}{mn}\right)_J = \left(\frac{a}{m}\right)_J \cdot \left(\frac{a}{n}\right)_J$

(5) $\left(\frac{-1}{m}\right)_J = (-1)^{\frac{m-1}{2}}$

(6) $\left(\frac{2}{m}\right)_J = (-1)^{(m^2-1)/8}$

(7) $\left(\frac{m}{n}\right)_J = \left(\frac{n}{m}\right)_J \cdot (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}$, falls $(m,n) = 1$ ist.

Die Aussagen können auf die entsprechenden Beziehungen des Legendresymbols zurückgeführt werden. Dies sei beispielhaft anhand von (7) gezeigt.

11.16. Bew. von 11.16. (7): Seien $(n,m)=1$, $m=\prod_{j=1}^{r} p_j$, $n=\prod_{k=1}^{s} q_k$ die PFZen mit Pzen $p_j, q_k \neq 2$. Dabei darf eine Primzahl häufiger als einmal als Faktor im Produkt vorkommen. Dann ist $p_j \neq q_k$ für alle Paare (j,k). Nach Def. 11.13 des Jacobisymbols ist dann

$$\left(\frac{m}{n}\right)_J = \prod_{k=1}^{s}\prod_{j=1}^{r}\left(\frac{p_j}{q_k}\right) \overset{QRG}{=} \prod_{k=1}^{s}\prod_{j=1}^{r}\left(\frac{q_k}{p_j}\right)(-1)^{\frac{p_j-1}{2}\cdot\frac{q_k-1}{2}} = \left(\frac{n}{m}\right)_J \cdot (-1)^{\alpha}$$

mit $\alpha := \sum_{k=1}^{s}\sum_{j=1}^{r} \frac{p_j-1}{2}\cdot\frac{q_k-1}{2} = \left(\sum_{j=1}^{r}\frac{p_j-1}{2}\right)\cdot\left(\sum_{k=1}^{s}\frac{q_k-1}{2}\right)$.

Man überprüft $\sum_{j=1}^{r}\frac{p_j-1}{2} \equiv \frac{m-1}{2}\ (2)$ und $\sum_{k=1}^{s}\frac{q_k-1}{2} \equiv \frac{n-1}{2}\ (2)$ leicht durch Induktion nach r bzw. s, woraus die Beh. folgt. □

11.17. Bem.: Dieser Satz 11.16. erlaubt nun, die Berechnung von $\left(\frac{a}{p}\right)$ bzw. $\left(\frac{a}{m}\right)_J$ mit $p \nmid a$ bzw. $(a,m)=1$ ohne Faktorisierung des Zählers des Symbols zu berechnen. Denn folgende Operationen sind dafür ausreichend.

a) Reduzieren des Zählers, so dass der Betrag des Zählers kleiner wird als die Hälfte des Nenners, d.h. Anwenden von (1).

b) Herausziehen von Zweierpotenzen im Zähler, d.h. Anwenden von (2).

c) Berechnen von $\left(\frac{-1}{m}\right)_J$ und $\left(\frac{2}{m}\right)_J$ mit (5) und (6).

d) Anwenden des QRGs für das Jacobisymbol, nämlich (7).

11.18. Bspl: Es soll die Lösbarkeit der Kongruenz $x^2 \equiv 383\ (443)$ untersucht werden. Da 443 prim ist, kann dies mit dem Legendresymbol $\left(\frac{383}{443}\right)=\left(\frac{383}{443}\right)_J$ bestimmt werden, indem wir die Rechenregeln 11.16 des Jacobisymbols benutzen:

$$\left(\frac{383}{443}\right)_J \overset{(7)}{=} -\left(\frac{443}{383}\right)_J \overset{(1)}{=} -\left(\frac{60}{383}\right)_J \overset{(2)}{=} -\left(\frac{2^2}{383}\right)_J\cdot\left(\frac{15}{383}\right)_J \overset{(3)}{=} -\left(\frac{15}{383}\right)_J \overset{(7)}{=} \left(\frac{383}{15}\right)_J \overset{(1)}{=} \left(\frac{8}{15}\right)_J$$

(da $443 \equiv 383 \equiv 3\ (4)$; da $383 \equiv 15 \equiv 3\ (4)$)

$$\overset{(2)}{=} \left(\frac{2^2}{15}\right)_J\cdot\left(\frac{2}{15}\right)_J \overset{(3)}{=} \left(\frac{2}{15}\right)_J \overset{(6)}{=} 1.$$

(da $15^2-1 \equiv (-1)^2-1 \equiv 0\ (16)$)

In keinem Schritt ist eine Faktorisierung erforderlich!

Die Kongruenz $x^2 \equiv 383\ (443)$ ist somit lösbar. Nach Satz 11.2 sind (wegen $443 \equiv 3\ (4)$) die beiden Lösungen $x_{1/2} \equiv \pm 383^{\frac{443+1}{4}} = \pm 383^{111} \equiv \pm 238\ (443)$.

↑ schnelles Potenzieren...