WiSe '21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ10: Quadratische Reste und das QRG

Stichworte: Quadratische und reinquadratische Kongruenz, qR und qNR, Eulerkriterium, Legendresymbol, Gaußsches Lemma, QRG, 1. EG, 2. EG

10.1. Einleitung: Quadratische Kongruenzen $f(x) \equiv 0\ (m)$, $m \in \mathbb{N}$ und $f \in \mathbb{Z}[X]$, $\deg f = 2$, sind explizit lösbar. Wir führen sie auf reinquadratische Kongruenzen mit Primzahlmodul zurück. Das Legendresymbol drückt ihre Lösbarkeit aus. Die Lösbarkeit von $x^2 \equiv p\ (q)$ hängt dabei mit der von $x^2 \equiv q\ (p)$ zusammen laut dem quadratischen Reziprozitätsgesetz (QRG). Die Ergänzungsgesetze behandeln zusätzlich auch die Kongruenzen $x^2 \equiv -1\ (p)$ und $x^2 \equiv 2\ (p)$.

10.2. Def.: Sei $m \in \mathbb{N}$.

- Eine Kongruenz der Gestalt $ax^2 + bx + c \equiv 0\ (m)$, $a \not\equiv 0$, $a, b, c \in \mathbb{Z}$, heißt quadratische Kongruenz (in x).
- Eine der Gestalt $x^2 \equiv u\ (m)$, $u \in \mathbb{Z}$, heißt reinquadratische Kongruenz.

Gesucht sind alle Lösungen mod m.

Eine quadratische Kongruenz kann stets auf eine reinquadratische zurückgeführt werden.

10.3. Satz: Für $a, b, c \in \mathbb{Z}$, $a \not\equiv 0$, sei $D := b^2 - 4ac$ die Diskriminante von $ax^2 + bx + c$.

Dann ist $ax^2 + bx + c \equiv 0\ (m) \iff \begin{cases} y^2 \equiv D\ (4am) \\ \wedge\ y \equiv b\ (2a) \end{cases}$ für $y = b + 2ax$ → nach x lösbar, wenn y geg.

Bew.: $ax^2 + bx + c \equiv 0\ (m) \iff 4a^2x^2 + 4abx + 4ac \equiv 0\ (4am)$
$\iff (2ax + b)^2 \equiv b^2 - 4ac\ (4am) \iff y^2 \equiv D\ (4am)$, wo $y = b + 2ax$. □

10.4 Bem.:
- Für $(a, m) = 1$ ist die Kongruenz äquivalent zu $x^2 + ba^{-1}x + ca^{-1} \equiv 0\ (m)$. ✓
- Für m, a ungerade ist sie äquivalent zu
$$(ax + b \cdot 2^{-1})^2 - ((b \cdot 2^{-1})^2 - ac) \equiv 0\ (am).$$

10.5 **Satz:** Die Kongruenz $x^2 \equiv D\ (M)$, $(D,M)=d=d_1^2 d_0$ mit d_0 quadratfrei (d.h. $p \mid d_0 \Rightarrow p^2 \nmid d_0$) ist genau dann lösbar, wenn $\left(\frac{M}{d}, d_0\right)=1$ und $x^2 \equiv d_0 \frac{D}{d}\ \left(\frac{M}{d}\right)$ ⊛ lösbar ist.

Bem.: In diesem Fall sind $d_0\frac{D}{d}$ und $\frac{M}{d}$ teilerfremd.

Bew.: „⇒": $x^2 \equiv D\ (M)$, $d_1^2 \mid D$, $d_1^2 \mid M \Rightarrow d_1^2 \mid x^2 \Rightarrow d_1 \mid x$.

Mit $\frac{1}{d_1^2}=\frac{d_0}{d}$ folgt $\left(\frac{x}{d_1}\right)^2 \equiv d_0 \cdot \frac{D}{d}\ \left(d_0\frac{M}{d}\right)$ ⊞ $\Rightarrow \frac{x}{d_1} \in \mathbb{Z}$ Lösung von ⊛, ist also lösbar.

Weiter folgt aus ⊞, dass $d_0 \mid \left(\frac{x}{d_1}\right)^2 \underset{d_0 \text{ q.-frei}}{\Rightarrow} d_0 \mid \frac{x}{d_1}$. Wieder mit ⊞ $\uparrow 1:d_0$ folgt $\left(\frac{x}{d_0 d_1}\right)^2 d_0 \equiv \frac{D}{d}\ \left(\frac{M}{d}\right)$,

also ist $\left(d_0, \frac{M}{d}\right)=1$ da $\left(\frac{D}{d}, \frac{M}{d}\right)=1$.

„⇐": Sei y Lsg. von ⊛ und $\left(\frac{M}{d}, d_0\right)=1$. Dann:

$$y^2 \equiv d_0 \frac{D}{d}\ \left(\frac{M}{d}\right) \underset{:d_0}{\Rightarrow} \left(\frac{y}{d_0}\right)^2 d_0 \equiv \frac{D}{d}\ \left(\frac{M}{d}\right) \underset{\cdot d}{\Rightarrow} d d_0 \left(\frac{y}{d_0}\right)^2 \equiv D\ (M)$$

$\underset{d=d_0 d_1^2}{\Rightarrow} (y d_1)^2 \equiv D\ (M) \Rightarrow$ Kongruenz $x^2 \equiv D\ (M)$ lösbar. □

Damit ist alles reduziert auf eine reinquadratische Kongruenz $x^2 \equiv a\ (m)$ mit $(a,m)=1$. Ob diese lösbar ist oder nicht, sprich ob a ein Quadrat in $\mathbb{Z}/m$ ist oder nicht, soll unterschieden werden mit einem Symbol, welches zunächst nur Primzahlmoduln behandelt. Da der Fall $m=p=2$ trivial ist, sei dabei p stets eine ungrade Primzahl.

10.6 **Def.** (Quadratische (Nicht-) Reste): Für alle $p \in \mathbb{P}$, $p>2$, und alle $a \in \mathbb{Z}$ mit $(a,p)=1$ heißt a ein quadratischer Rest modulo p (kurz: qR mod p), falls es ein $x \in \mathbb{Z}$ mit $x^2 \equiv a\ (p)$ gibt.

Andernfalls heißt a ein quadratischer Nichtrest modulo p (kurz: qNR mod p).

Bem.: Besser wäre für einen qNR der Ausdruck "nichtquadratischer Rest".
Wir folgen aber der üblichen Bezeichnung "qNR".

10.7 **Def.** (Legendre-Symbol): Für alle $p \in \mathbb{P}$, $p>2$, heißt die Abb.

$$\left(\frac{\cdot}{p}\right): \quad \{b \in \mathbb{Z};\ (b,p)=1\} \longrightarrow \{-1,1\},$$

$$a \longmapsto \left(\frac{a}{p}\right) := \begin{cases} 1, & \text{falls } a \text{ qR mod } p \text{ ist,} \\ -1, & \text{falls } a \text{ qNR mod } p \text{ ist,} \end{cases}$$

das Legendresymbol zu p. sprich: "a nach p", auch "a über p": nicht so gut

Bem.: Man beachte, dass $\left(\frac{a}{p}\right)$ nur für $p>2$ prim und $p \nmid a$ definiert ist.
Mod 2 ex. kein qNR, und für $p \mid a$ ist $a \equiv 0\ (p)$ kein reduzierter Rest mod p.

10.8. Folgerung: Sei $p \in \mathbb{P}$, $p > 2$, $a, b \in \mathbb{Z}$, $(a,p) = 1 = (b,p)$.

(1) Gilt $a \equiv b\ (p)$, so ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) Es gilt $\left(\frac{a^2}{p}\right) = 1$.

(3) Unter den Zahlen $1, \dots, p-1$ sind genau $\frac{p-1}{2}$ viele qRe mod p
und genau $\frac{p-1}{2}$ viele qNRe mod p.

Es ist also $\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0$.

(4) Im Fall $\left(\frac{a}{p}\right) = 1$ gibt es genau zwei $x \in \mathbb{N}$, $x < p$, mit $x^2 \equiv a\ (p)$.

Bew.: (1), (2): ✓, (3): • Die Quadrate $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ (⊛) sind pw. inkongruent mod p.

⌈Denn $k^2 \equiv l^2\ (p)$ mit $k, l \in \mathbb{N}$, $k, l \le \frac{p-1}{2}$, impliziert $(k-l)(k+l) \equiv 0\ (p)$.
Wegen $2 \le k+l \le p-1$ bzw. $p \nmid k+l$ folgt $p \mid k-l$, also $k = l$ da $|k-l| < p$ ist.⌋

• Jede Zahl x^2 mit $x \in \mathbb{Z}$, $p \nmid x$, ist zu einer der Zahlen (⊛) mod p kongruent.

⌈Denn sind $x \in \mathbb{Z}$, $(x,p) = 1$, $y \in \mathbb{Z}$, $y \le p$, $x \equiv y\ (p)$ und $c := \frac{x-y}{p}$,
so gilt $x^2 = (y + cp)^2 \equiv y^2\ (p)$. Im Fall $\frac{p-1}{2} + 1 \le y \le p-1$
ist aber $1 \le p - y \le \frac{p-1}{2}$ und $y^2 \equiv (p-y)^2\ (p)$.
Ein qR mod p ist daher zu einer der Zahlen in (⊛) kongruent.⌋

• Daher ex. je $\frac{p-1}{2}$ viele qRe und $\frac{p-1}{2}$ viele qNRe mod p.

(4): Die Kongruenzen $x^2 \equiv a\ (p)$, wobei $a \in \mathbb{Z}$ alle $\frac{p-1}{2}$ vielen qRe mod p durchläuft,
haben zusammen $p-1$ viele Lösungen $x \in \mathbb{N}$ mit $x < p$. Jede einzelne hat
nach dem Satz 8.6 von Lagrange höchstens zwei Lösungen.
Also hat jede genau zwei Lösungen. (Mit x_0 ist auch $-x_0 \equiv p - x_0 \not\equiv x_0\ (p)$ Lösung mod p.) □

↳ schreibe auch: $\pm x_0$ mod p sind die Lösungen mod p

10.9. Bsp.: • Bestimme alle qRe und qNRe mod $p = 11$, es gibt $\frac{11-1}{2} = 5$ quadratische Reste:

a	± 1	± 2	± 3	± 4	± 5
a^2	1	4	9 $\equiv -2$	5	3

die Liste der qNe im reduz. RS $\{1, \dots, 10\}$ ist
dann: 2, 6, 7, 8, 10.

Die Liste der qRe im reduz. RS $\{\pm 1, \pm 2, \dots, \pm 5\}$ lautet $1, -2, 3, 4, 5$,
die der qNRe lautet $-1, 2, -3, -4, -5$.

• Für $p = 11$ ist -1 ein qNR, für $p = 13$ ist -1 ein qR, da $x^2 \equiv -1\ (13)$
von $x \equiv \pm 5\ (13)$ gelöst wird.

10.10. Satz (Euler-Kriterium (manchmal "Euler Kongruenz" genannt, nicht zu verwechseln mit 7.9 !)):
Seien $p \in \mathbb{P}, p>2$, $a, b \in \mathbb{Z}$, $(ab, p)=1$. Dann gilt $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (p)$.
Bew.: Aus der Euler Kongruenz 7.9 ergibt sich $(a^{\frac{p-1}{2}}-1)\cdot(a^{\frac{p-1}{2}}+1) \equiv 0 \ (p)$. ⊗
Nur einer der zwei Faktoren der l.S. wird von $p>2$ geteilt, da ihre Differenz 2 ist.
- Ist $\left(\frac{a}{p}\right)=1$, gibt es also ein $x \in \mathbb{Z}$ mit $x^2 \equiv a \ (p)$,
  dann gilt nach der Euler Kongruenz 7.9, dass
  $$\boxed{+} \quad a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 = \left(\frac{a}{p}\right) \ (p) \text{ gilt.}$$
  Der erste Faktor der l.S. von ⊗ wird somit von p geteilt, nämlich für die $\frac{p-1}{2}$ vielen qRe a.
  Nach dem Satz von Lagrange 8.6 hat $\boxed{+}$ keine weiteren Lösungen.
- Also gilt im Falle $\left(\frac{a}{p}\right)=-1$, dass $a^{\frac{p-1}{2}}+1 \equiv 0 \ (p)$, d.h. $a^{\frac{p-1}{2}} \equiv -1 = \left(\frac{a}{p}\right) \ (p)$. □

10.11. Satz (Multiplikationssatz für das Legendresymbol):
Seien $p \in \mathbb{P}, p>2$, $a, b \in \mathbb{Z}$, $(ab, p)=1$. Dann gilt $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$.
Bew.: Wegen dem Euler Kriterium 10.10 gilt
$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) \ (p).$$
Wegen $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) \in \{-2, 0, 2\}$ und $p>2$ folgt heraus die Gleichheit. □

Unser Ziel ist nun, das quadratische Reziprozitätsgesetz (QRG) zu beweisen.
Das QRG bringt die Lösbarkeit von $x^2 \equiv p \ (q)$ mit der von $x^2 \equiv q \ (p)$ in Verbindung.
Die Aussage wurde bereits von Euler durch Untersuchung vieler numerischer Beispiele entdeckt und formuliert, erst Gauß konnte 1801 einen vollständigen Beweis liefern.
Gauß hat auch mehrere Beweise gegeben. Ein wichtiger Baustein des Beweises, den wir hier darstellen, ist das folgende Gaußsche Lemma, welches eine nicht naheliegende Berechnungsmöglichkeit des Legendresymbols formuliert.

10.12. Lemma (Gaußsches Lemma, nicht zu verwechseln mit 1.16(2)!)
Sei $p \in \mathbb{P}$, $p>2$, $a \in \mathbb{Z}$, $(a,p)=1$. Für alle $j \le \frac{p-1}{2}$ sei $c_j := ja - \lfloor \frac{ja}{p} \rfloor \cdot p \in \{1, \dots, p-1\}$ der kleinste positive Rest der Zahl ja bei Division durch p, also $a \equiv c_1, 2a \equiv c_2, 3a \equiv c_3, \dots, \frac{p-1}{2}a \equiv c_{\frac{p-1}{2}} \ (p)$.
Sei μ die Anzahl der Reste c_j, die $\frac{p}{2}$ übertreffen, d.h. $\mu := \#\{j \le \frac{p-1}{2};\ c_j > \frac{p}{2}\}$.
Dann gilt $\left(\frac{a}{p}\right) = (-1)^{\mu}$.

Bem.: Das Gaußsche Lemma besagt also, dass die Parität der Anzahl der Reste $ja \bmod p$ $(j \leq \frac{p-1}{2})$, die $\frac{p}{2}$ übertreffen, genau darüber entscheidet, ob a ein qR mod p ist oder nicht. Außer zum Beweis des QRGs hat diese Feststellung kaum einen Nutzen.

Bew.: 1. Schritt: Definition von b_k und d_k.

Haben laut Def. die Glg. $ja = \lfloor \frac{ja}{p} \rfloor \cdot p + c_j$ für $0 < c_j \leq p-1$ und $j \leq \frac{p-1}{2}$.

Seien $\nu := \frac{p-1}{2} - \mu$ und $b_1, \dots, b_\mu$ die $c_j \geq \frac{p+1}{2}$,

und $d_1, \dots, d_\nu$ die $c_j \leq \frac{p-1}{2}$.

Die c_j und somit die b_k, d_ℓ sind p.w. inkongruent mod p,

da $\{ja;\ j \in \mathbb{N},\ j \leq p-1\}$ ein reduz. RS mod p ist.

2. Schritt: $\{d_1, \dots, d_\nu, p-b_1, \dots, p-b_\mu\} = \{1, 2, \dots, \frac{p-1}{2}\}$.

Für alle $k \leq \mu$, $\ell \leq \nu$ gilt $p - b_k \not\equiv d_\ell\ (p)$.

Denn aus der Richtigkeit einer solchen Kongruenz folgte $b_k + d_\ell \equiv 0\ (p)$,

also $(j_1 + j_2) a \equiv 0\ (p)$ mit einem Paar $(j_1, j_2) \in \{1, \dots, \frac{p-1}{2}\}^2$ und $j_1 \neq j_2$.

Dies kann wegen $p \nmid a$ und $0 < j_1 + j_2 \leq p-1$ aber nicht sein.

3. Schritt: Nach dem 1. Schritt gilt mit dem Eulerkriterium 10.10, dass

$$P := \prod_{k=1}^{\mu} b_k \cdot \prod_{\ell=1}^{\nu} d_\ell \equiv a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{p-1}{2}\right)!\quad (p).$$

Mit dem 2. Schritt folgt wegen $P = (-1)^\mu \cdot \prod_{k=1}^{\mu} (-b_k) \prod_{\ell=1}^{\nu} d_\ell \equiv (-1)^\mu \cdot \prod_{k=1}^{\mu} (p - b_k) \prod_{\ell=1}^{\nu} d_\ell \quad (p)$

dann $(-1)^\mu \left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{p-1}{2}\right)!\ (p)$.

Wegen $(p, (\frac{p-1}{2})!) = 1$ darf dividiert werden, so dass $(-1)^\mu \equiv \left(\frac{a}{p}\right)\ (p)$ folgt.

Da beide Seiten im Betrag höchstens 1 sind und $p > 2$, folgt die Gleichheit. $\square$

Wir kommen nun zum QRG.

10.13 Motivation zum QRG: Dass die Lösbarkeit von Kongruenzen $x^2 \equiv p\ (q)$ mit der von $x^2 \equiv q\ (p)$ zusammenhängt, fand Euler anhand von Beispielen.

Er fand, dass $x^2 \equiv p\ (q)$ und $x^2 \equiv q\ (p)$ beide lösbar für $p \equiv 1\ (4) \vee q \equiv 1\ (4)$ sind, bzw. beide unlösbar. Andernfalls, wenn $p \equiv 3\ (4) \wedge q \equiv 3\ (4)$ ist, dann ist die eine Kongruenz lösbar und die andere nicht.

Mit dem Legendresymbol lässt sich dieser Sachverhalt wie folgt kompakt formulieren.

10.14. Quadratisches Reziprozitätsgesetz (QRG): Für $p, q \in \mathbb{P}\setminus\{2\}$, $p \neq q$, gilt
$$\boxed{\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}}.$$

10.15. Bem.: Dies bedeutet: $\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{falls } p\equiv 1\ (4) \vee q \equiv 1\ (4), \\ -\left(\frac{q}{p}\right), & \text{falls } p \equiv 3\ (4) \wedge q \equiv 3\ (4). \end{cases}$

10.16. Bsp.: Ist $x^2 \equiv 35\ (43)$ mit $x \in \mathbb{Z}$ lösbar?
Da 43 prim, berechnet man
$$\left(\frac{35}{43}\right) \underset{\text{faktorisier}}{=} \left(\frac{7}{43}\right)\cdot\left(\frac{5}{43}\right) \overset{\text{QRG}}{\underset{43\equiv 7\equiv 3(4)}{=}} -\left(\frac{43}{7}\right)\cdot\left(\frac{5}{43}\right) \overset{\text{reduzier}}{=} -\underbrace{\left(\frac{1}{7}\right)}_{=\left(\frac{1^2}{7}\right)=1}\cdot\left(\frac{5}{43}\right) = -\left(\frac{5}{43}\right)$$
$$\overset{\text{QRG}}{\underset{5\equiv 1(4)}{=}} -\left(\frac{43}{5}\right) \overset{\text{reduzier}}{=} -\left(\frac{3}{5}\right) \overset{\text{QRG}}{\underset{5\equiv 1(4)}{=}} -\left(\frac{5}{3}\right) \underset{\text{reduzier}}{=} -\underbrace{\left(\frac{2}{3}\right)}_{2\equiv -1 \text{ ist qNR mod } 3} = -(-1) = 1,$$
also ist 35 ein qR mod 43.

10.17. Bew. des QRGs:
1. Schritt: Wie im Gaußschen Lemma 10.12 betr. $c_j := jq - \lfloor\frac{jq}{p}\rfloor\cdot p$, $j \leq \frac{p-1}{2}$,
sowie $\mu := \#\{j \leq \frac{p-1}{2};\ c_j > \frac{p}{2}\}$, $\nu := \frac{p-1}{2} - \mu$,
seien $b_1, \dots, b_\mu$ die $c_j \in \{\frac{p+1}{2}, \dots, p-1\}$ und $d_1, \dots, d_\nu$ die $c_j \in \{1, \dots, \frac{p-1}{2}\}$.
Setze nun
$$S_1 := \sum_{j=1}^{(p-1)/2} \left\lfloor\frac{jq}{p}\right\rfloor.$$
Die Summation von jq mit $j = 1, 2, \dots, \frac{p-1}{2}$ ergibt
$$\underbrace{q\cdot\frac{(p-1)(p+1)}{8}}_{\text{laut kleinem Gauß}} = \sum_{j=1}^{(p-1)/2} jq \underset{\text{Def. } c_j}{=} \sum_{j=1}^{(p-1)/2}\left(\left\lfloor\frac{jq}{p}\right\rfloor\cdot p + c_j\right) = pS_1 + \sum_{j=1}^{(p-1)/2} c_j. \quad (1)$$
Wie im 2. Schritt des Beweises des Gaußschen Lemmas 10.12 gilt
$$\sum_{j=1}^{(p-1)/2} c_j = \sum_{k=1}^{\mu} b_k + \sum_{\ell=1}^{\nu} d_\ell = 2\sum_{k=1}^{\mu} b_k + \sum_{k=1}^{\mu}(p - b_k) + \sum_{\ell=1}^{\nu} d_\ell - \mu p$$
$$\underset{\{1,\dots,\frac{p-1}{2}\} = \{d_1,\dots,d_\nu,\, p-b_1,\dots,p-b_\mu\}}{=} 2\sum_{k=1}^{\mu} b_k + \sum_{m=1}^{(p-1)/2} m - \mu p \underset{\text{wieder kleiner Gauß}}{=} 2\sum_{k=1}^{\mu} b_k + \frac{(p-1)(p+1)}{8} - \mu p. \quad (2)$$

Jetzt: (2) in (1) einsetzen und umstellen zeigt $\mu p = pS_1 + \underbrace{(1-q)}_{\equiv 0(2)}\cdot\underbrace{\frac{(p-1)(p+1)}{8}}_{\in\mathbb{Z}} + \underbrace{2\sum_{k=1}^{\mu} b_k}_{\equiv 0(2)}$,
also ist $\mu p \equiv p S_1\ (2) \overset{p>2}{\Longrightarrow} \mu \equiv S_1\ (2)$.
Nach dem Gaußschen Lemma 10.12 folgt $\left(\frac{q}{p}\right) = (-1)^{S_1}$.

<u>2. Schritt</u>: Genau analog folgt $\left(\frac{p}{q}\right) = (-1)^{S_2}$, $S_2 := \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{pj}{q} \right\rfloor$.

<u>3. Schritt</u>: z.z.: $S_1 + S_2 = \frac{p-1}{2}\cdot\frac{q-1}{2}$ ⌜ $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) \underset{\uparrow\ \text{1. \& 2. Schritt}}{=} (-1)^{S_1}\cdot(-1)^{S_2} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ ✓⌟

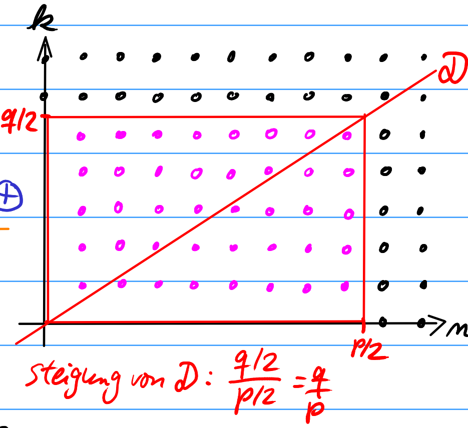
Zum Beweis sei OE $p>q$.

Wir betrachten in $\mathbb{R}^2$ das abgeschlossene Rechteck

$$R := \left[0,\tfrac{p}{2}\right]\times\left[0,\tfrac{q}{2}\right] \subseteq \mathbb{R}^2$$

und sei $G := \#(\mathbb{N}^2 \cap R)$ die Anzahl der darin eingeschlossenen Gitterpunkte. Offenbar gilt $G = \frac{p-1}{2}\cdot\frac{q-1}{2}$. ⊕

Die Hauptdiagonale D von R lässt sich schreiben als $D := \left\{(n,k)\in\mathbb{R}^2;\ k = \frac{q}{p}\cdot n\right\}$.



<u>Beobachtung</u>: Auf D liegen keine Gitterpunkte $(n,k)\in\mathbb{N}^2\cap R$.

⌜Denn $k = \frac{q}{p} n$ bewirkt $p \mid qn$, was wegen $n \le \frac{p-1}{2}$, $(p,q)=1$, nicht sein kann.⌟

Die Gitterpunkte $(n,k)\in\mathbb{N}^2\cap R$ mit $k < \frac{q}{p} n$ sind demnach diejenigen unterhalb der Diagonalen D, und die mit $\underbrace{k > \frac{q}{p} n}_{\Leftrightarrow\, n < \frac{p}{q} k}$ sind diejenigen oberhalb D.

G kann damit berechnet werden durch Aufsummieren der Anzahl der $(n,k)\in\mathbb{N}^2\cap R$ unterhalb und oberhalb der Diagonalen D, nämlich

$$G = \sum_{n=1}^{(p-1)/2}\ \sum_{\substack{k=1\\ k<qn/p}}^{(q-1)/2} 1 \;+\; \sum_{k=1}^{(q-1)/2}\ \sum_{\substack{n=1\\ n<pk/q}}^{(p-1)/2} 1 = \sum_{n=1}^{(p-1)/2}\ \sum_{k=1}^{\lfloor qn/p\rfloor} 1 + \sum_{k=1}^{(q-1)/2}\ \sum_{n=1}^{\lfloor pk/q\rfloor} 1$$

$$= \sum_{n=1}^{(p-1)/2}\left\lfloor\frac{qn}{p}\right\rfloor + \sum_{k=1}^{(q-1)/2}\left\lfloor\frac{pk}{q}\right\rfloor = S_1+S_2,$$

mit ⊕ folgt die Beh. □

Das QRG 10.14 beinhaltet keine Möglichkeit, $\left(\frac{-1}{p}\right)$ oder $\left(\frac{2}{p}\right)$ zu behandeln. Dafür sind die beiden Ergänzungsgesetze hilfreich.

10.18. <u>Erstes Ergänzungsgesetz (1. EG)</u>: Für $p\in\mathbb{P}\setminus\{2\}$ ist $\boxed{\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}} = \begin{cases} 1, & p\equiv 1\ (4), \\ -1, & p\equiv 3\ (4). \end{cases}$

<u>Bew.</u>: Nach dem Eulerkriterium 10.10 gilt $\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}\ (p)$,

und mit $\left|\left(\frac{-1}{p}\right)-(-1)^{\frac{p-1}{2}}\right|\le 2$ und $p>2$ folgt die Gleichheit. □

10.19. Zweites Ergänzungsgesetz (2. EG): Für $p \in \mathbb{P} \setminus \{2\}$ ist $\boxed{\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}} = \begin{cases} 1, & p \equiv \pm 1\,(8), \\ -1, & p \equiv \pm 3\,(8). \end{cases}$

Bew.: Nach dem Gaußschen Lemma 10.12

ist $\left(\frac{2}{p}\right) = (-1)^{\vartheta}$ mit $\vartheta := \#\{j \in \mathbb{N};\ j \le \frac{p-1}{2},\quad j\cdot 2 - \lfloor \frac{j\cdot 2}{p} \rfloor \cdot p > \frac{p}{2}\}$.

Sei $M := \{j\cdot 2;\ j \le \frac{p-1}{2}\}$. Für alle $k \in M$ ist $k \le \frac{p-1}{2}\cdot 2 = p-1$.

Wegen $\# M = \frac{p-1}{2}$ besteht M also aus allen geraden natürlichen Zahlen,

die kleiner als p sind. Insbesondere ist $\lfloor \frac{k}{p} \rfloor = 0$ für alle $k \in M$,

und damit folgt $\vartheta = \#\{k \in M;\ k > \frac{p}{2}\}$.

Für alle $k \in M$, $k \le \frac{p}{2}$, gibt es ein j mit $k = j\cdot 2$, wobei gilt: $j\cdot 2 \le \frac{p}{2} \Leftrightarrow j \le \frac{p}{4}$.

Also ist $\#\{k \in M;\ k \le \frac{p}{2}\} = \lfloor \frac{p}{4} \rfloor$, und es folgt $\vartheta = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$.

Wegen $2 \nmid p$ gibt es ein $\ell \in \mathbb{N}$ und ein $r \in \{1,3,5,7\}$ mit $p = 8\ell + r$.

Es folgt $\left(\frac{2}{p}\right) = (-1)^{\vartheta}$ mit $\vartheta = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor = 4\ell + \frac{r-1}{2} - \lfloor 2\ell + \frac{r}{4} \rfloor = 2\ell + \frac{r-1}{2} - \lfloor \frac{r}{4} \rfloor$.

$\lfloor x+k \rfloor = \lfloor x \rfloor + k$ für $k \in \mathbb{Z}$, $x \in \mathbb{R}$

Für $r = 1$ ist $\frac{r-1}{2} - \lfloor \frac{r}{4} \rfloor = 0 - 0 = 0$ gerade, $\rightarrow p \equiv 1\,(8)$

für $r = 3$ ist " $= 1 - 0 = 1$ ungerade, $\rightarrow p \equiv 3\,(8)$

für $r = 5$ ist " $= 2 - 1 = 1$ ungerade, $\rightarrow p \equiv -3\,(8)$

für $r = 7$ ist " $= 3 - 1 = 2$ gerade. $\rightarrow p \equiv -1\,(8)$ $\square$

10.20. Bem.: Mit den Ergebnissen dieses Kapitels, speziell das QRG und die beiden EGe, kann im Prinzip jedes Legendresymbol $\left(\frac{a}{p}\right)$ berechnet werden.

Man verwendet die Reduktion des "Zählers" modulo p, den Multiplikationssatz für den "Zähler" und die Invertierung des Symbols nach dem QRG.

Die dabei i.a. nötige Faktorisierung des Zählers stellt aber ein algorithmisches Hindernis dar.

Die aufwändige Zerlegung des "Zählers" a in seine PFZ kann, wie in EZ 11 gezeigt wird, mit Hilfe des Jacobisymbols umgangen werden.

10.21. Bsp.: Da 43 prim ist, gilt

$$\left(\frac{-77}{43}\right) \overset{\text{Faktorisieren!}}{=} \left(\frac{-1}{43}\right)\cdot\left(\frac{7}{43}\right)\cdot\left(\frac{11}{43}\right) \underset{43\equiv 3(4)}{\overset{1.EG}{=}} (-1)\cdot\left(\frac{7}{43}\right)\cdot\left(\frac{11}{43}\right) \underset{43\equiv 3\equiv 7(4)}{\overset{QRG}{=}} (-1)\cdot\left(-\left(\frac{43}{7}\right)\right)\cdot\left(\frac{11}{43}\right)$$

$$\underset{11\equiv 3\equiv 43(4)}{\overset{QRG}{=}} \left(\frac{43}{7}\right)\cdot\left(-\left(\frac{43}{11}\right)\right) \underset{\text{Reduktion}}{=} -\left(\frac{\overset{=1}{1}}{7}\right)\cdot\left(\frac{10}{11}\right) = -\left(\frac{2}{11}\right)\cdot\left(\frac{5}{11}\right) \underset{11\equiv 3(8)}{\overset{2.EG}{=}} -(-1)\cdot\left(\frac{5}{11}\right) = \left(\frac{5}{11}\right) \underset{5\equiv 1(4)}{\overset{QRG}{=}} \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1,$$

$$\text{oder: } = -\left(\frac{-1}{11}\right) \underset{11\equiv 3(4)}{\overset{1.EG}{=}} -(-1) = 1.$$

Es gibt viele Wege, das Symbol zu berechnen.

Die Kongruenz $x^2 \equiv -77\,(43)$ ist somit lösbar.

Wie die Lösungspaare $\pm x_0$ einer lösbaren Kongruenz $x^2 \equiv a \ (p)$ explizit berechnet werden können, klären wir in Kapitel EZ 11. Im Moment sind diese für uns nur durch Probieren erhältlich. Wir können, wenn Lösungen vorliegen, aber damit problemlos zu Lösungen der Kongruenz $x^2 \equiv a \ (p^k)$, $k \geq 2$, aufsteigen.
Dabei ist $p=2$ ein Sonderfall.

10.22 **Satz** (quadratische Reste modulo Primpotenzen):
Seien $p \in \mathbb{P} \setminus \{2\}$, $k \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a,p)=1$, $2 \nmid b \in \mathbb{Z}$, $f(X) := X^2 - b$. Dann:

(1) Die Kongruenz $x^2 \equiv a \ (p^k)$ hat genau $1 + \left(\frac{a}{p}\right)$ viele Lösungen $x \in \mathbb{Z}$ mod p^k, die in Abhängigkeit der Lösungen x_0 mod p^{k-1} explizit angegeben werden können

(2) Die Lösungszahl der Kongruenz $x^2 \equiv b \ (2^k)$ bzw. $f(x) \equiv 0 \ (2^k)$ ist

$$S(2^k, f) = \begin{cases} 1, & k=1, & (\text{nämlich } x \equiv 1 \ (2)) \\ 2, & k=2 \text{ und } b \equiv 1 \ (4), & (\text{nämlich } x \equiv \pm 1 \ (4)) \\ 0, & k=2 \text{ und } b \equiv 3 \ (4), & \\ 4, & k \geq 3 \text{ und } b \equiv 1 \ (8), & (\text{explizit angebbar}) \\ 0, & k \geq 3 \text{ und } b \not\equiv 1 \ (8). & \end{cases}$$

Bew.: Zu (1): Für $k=1$ ist dies 10.8(4). Für $k>1$ wendet man den Aufsteigesatz 8.8 auf $h(x) = x^2 - a$ an. Wegen $p \nmid 2a$ gilt $h'(x_0) = 2x_0 \not\equiv 0 \ (p)$ für jede Lösung $x_0 \in \mathbb{Z}$ von $x_0^2 - a \equiv 0 \ (p^{k-1})$. Es tritt also stets der 1. Fall im Aufsteigesatz 8.8 ein.

Zu (2): Die Fälle $k=1$, $k=2$ sind klar: $x^2 \equiv 1 \ (2) \Leftrightarrow x \equiv 1 \ (2)$, und $x^2 \equiv 1 \ (4) \Leftrightarrow x \equiv \pm 1 \ (4)$.
Sei also OE $k \geq 3$. Gibt es ein $x \in \mathbb{Z}$ mit $x^2 \equiv b \ (2^k)$ (*), dann muss x wegen $2 \nmid b$ ungerade sein, und es gibt ein $c \in \mathbb{Z}$ mit $x = 2c+1$.
Im Falle der Lösbarkeit gilt also $b \equiv (2c+1)^2 \equiv 4c(c+1)+1 \equiv 8 \cdot \frac{c(c+1)}{2} + 1 \ (2^k)$, also $b \equiv 1 \ (8)$, und (*) hat für $k=3$ die 4 Lösungen $\pm 1, \pm 3$ mod 8.

- Dies diene als Induktionsanfang, als Induktionsvor. für $k \geq 4$ gelte $x^2 \equiv b \ (2^{k-1})$ für ein $x \in \mathbb{Z}$. Es gilt $2 \nmid x$, und deshalb ex. $x^* \in \mathbb{Z}$ mit $x x^* \equiv 1 \ (2^k)$.

Setzen $d := x^* \cdot \frac{b - x^2}{2^{k-1}} \in \mathbb{Z}$. Dann gilt

$$(x + 2^{k-2} d)^2 \equiv x^2 + 2^{k-1} x d \equiv x^2 + b - x^2 \equiv b \quad (2^k),$$

es gibt also Lösungen von (*) mod 2^k.

• Seien $x_1, x_2 \in \mathbb{Z}$ zwei Lösungen von (*) mod 2^k. Dann gilt

$$x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2) \equiv 0 \quad (2^k).$$

Da $2 \nmid x_1 x_2$, kann durch 4 dividiert werden: $\frac{x_1 - x_2}{2} \cdot \frac{x_1 + x_2}{2} \equiv 0 \quad (2^{k-2})$.

Nun können $\frac{x_1 - x_2}{2}$ und $\frac{x_1 + x_2}{2}$ nicht zugleich gerade oder ungerade sein, da sonst ihre Summe x_1 gerade wäre.

Sei also im ersten Fall $\frac{x_1 - x_2}{2} \equiv 0 \ (2^{k-2})$, d.h. $x_2 \equiv x_1 \ (2^{k-1})$.

Dies induziert modulo 2^k die zwei Werte x_1 und $x_1 + 2^{k-1}$.

Genauso erhält man im Fall $\frac{x_1 + x_2}{2} \equiv 0 \ (2^{k-2})$ die zwei Werte $-x_1$ und $-x_1 + 2^{k-1}$.

Diese vier Zahlen sind p.w. verschieden mod 2^k.

Alle vier lösen die Kongruenz (*) laut binomischer Formel, und andere Lösungen kann es nicht geben. □

10.23. Bsp.: $x^2 \equiv 1 \ (2^3)$ hat die 4 Lösungen $\pm 1, \pm 3$ mod $2^3 = 8$,

$x^2 \equiv 1 \ (2^4)$ " " $\pm 1, \pm 7$ mod $2^4 = 16$,

$x^2 \equiv 1 \ (2^5)$ " " $\pm 1, \pm 15$ mod $2^5 = 32$,

$x^2 \equiv 1 \ (2^6)$ " " , ± 31 mod $2^6 = 64$, ...