Beispiel 5.16

(a) $n = 561 = 3 \cdot 11 \cdot 17$ ist eine Carmichael Zahl.

Sei $b=2$. Es ist $560 = 2^4 \cdot \underbrace{5 \cdot 7}_{t}$

$$\left.\begin{aligned} 2^t &\equiv 263 \mod n \\ 2^{2t} &\equiv 166 \mod n \\ 2^{4t} &\equiv 67 \mod n \\ 2^{8t} &\equiv 1 \mod n \\ 2^{16 \cdot t} &\equiv 1 \mod n \end{aligned}\right\}$$

561 ist keine starke Pseudoprimzahl zur Basis $b=2$.
(demnach ist 561 eine starke Pseudoprimzahl zur Basis $b=50$)

(b) Sei $n = 91 = 7 \cdot 13$ & $b = 10$.

Es ist $n-1 = 90 = 2 \cdot \underbrace{45}_{t}$

Wegen $b^t \equiv -1 \mod 91$ ist 91 eine starke Pseudoprimzahl zur Basis $b = 10$.

Fakt 11.7.2018

Zu einer gegebenen Basis b gibt es unendlich viele starke Pseudoprimzahlen. Für $b=2$ folgt dies aus dem folgenden Satz.

Satz 5.17

Ist n eine Pseudoprimzahl zur Basis $b=2$, so ist $2^n - 1$ eine starke Pseudoprimzahl zur Basis $b=2$.

Beweis:

ähnlich zu B 13 A4 (Rosen Satz 4.2)

Der folgende Satz erlaubt es uns einen guten Primzahltest zu bauen.

Satz 5.18

Ist n eine zusammengesetzte Zahl. Dann ist n für höchstens $\frac{n-1}{4}$ Zahlen b mit $1 \leq b \leq n-1$ eine starke Pseudoprimzahl zur Basis b.

Beweis: siehe z.B. Rosen ☒

Eine zusammengesetzte Zahl n ist also für mindestens 75% der Zahlen in $\{1, \ldots, n-1\}$ keine starke Pseudoprimzahl.

Miller - Rabin - Primzahltest

Sei n gegeben.

- Wähle zufällig k Basen b_i mit $1 \leq b_i \leq n-1$
- Teste ob n eine starke Pseudoprimzahl zur Basis b_i ist $\forall i$
- Ist n bzgl. aller Basen b_i eine starke Pseudoprimzahl, so ist die Wahrscheinlichkeit, dass n zusammengesetzt ist $\leq (0{,}25)^k$
  z.B. für $k = 100$ ist $(0{,}25)^{100} \approx 4 \cdot 10^{-61}$

§6 Das quadratische Reziprozitätsgesetz (QR)

Wir wollen die Lösbarkeit von Gleichungen der Form $x^2 \equiv a \bmod m$ untersuchen. (Zunächst für $m = p$ eine Primzahl)

Definition 6.1.
Sei $p > 2$ eine Primzahl und $a \in \mathbb{N}$ mit $ggT(a,p) = 1$.
Die Zahl a heißt quadratischer Rest modulo p, falls $x^2 \equiv a \bmod p$ eine Lösung hat.
Andernfalls heißt a quadratischer Nichtrest modulo p.

Definition 6.2.
Sei $p > 2$ eine Primzahl. Das Legendre-Symbol (Adrian-Marie Legendre 1752-1833) ist def. als

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } a \text{ quadratischer Rest mod } p \\ -1 & \text{" " " Nichtrest mod } p \\ 0 & \text{falls } p \mid a \end{cases}$$

Lemma 6.3.
Sei $p > 2$ eine Primzahl
(a) Es existieren genau $\frac{p-1}{2}$ quadr. Reste modulo p und $\frac{p-1}{2}$ quadr. Nichtreste
(b) Es gilt das sog. Eulersche Kriterium $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Beweis:
(a) Wir wollen die quadr. Reste unter Zahlen $\{1, \dots, p-1\}$ ausmachen. $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ sind offensichtlich quadr. Reste. $1^2, \dots, \left(\frac{p-1}{2}\right)^2$ sind auch paarweise unterschiedliche Klassen modulo p, da aus $a^2 \equiv b^2 \bmod p$ wegen 3.12 schon $a \equiv \pm b \bmod p$.

Wegen $a^2 \equiv -a^2 \bmod p$ folgt, dass $x^2 \equiv a \bmod p$ entweder keine oder zwei Lösungen hat.

$\Rightarrow$ Es kann keine weiteren quadr. Reste geben.

$\rightarrow$ Die Anzahl der quadr. (Nicht-)Reste ist genau $\frac{p-1}{2}$

(b) Für $a \equiv 0 \bmod p$ ist die Aussage klar.

Sei also $a \not\equiv 0 \bmod p$. Nach dem kleinen Satz von Fermat

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \bmod p \quad (ggT(a,p)=1) \Rightarrow a^{\frac{p-1}{2}} \equiv -1 \bmod p \ (3.12)\ (*_1)$$

- Ist a ein quadratischer Rest, so ex. ein $b \in \mathbb{Z}/p\mathbb{Z}$ mit $a \equiv b^2 \bmod p$.

Daher gilt dann

[redacted] $a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} = b^{p-1} \overset{\text{kl. S. v. Fermat}}{\equiv} 1 \bmod p = \left(\frac{a}{p}\right)$

($ggT(b,p)=1$)

- Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, hat die Gleichung $x^{\frac{p-1}{2}} - 1 \equiv 0 \bmod p$ höchstens $\frac{p-1}{2}$ Lösungen. (vgl. Bem. 4.40, B12A4)

Aber die $\frac{p-1}{2}$ quadratischen Reste sind Lösungen dieser Gleichung (wegen [redacted])

Also existieren keine weiteren Lösungen.

- Sei nun a ein quadr. Nichtrest, dann muss wegen $*_1$ gelten, dass $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

$\Rightarrow$ Für einen quadr. Nichtrest gilt $a^{\frac{p-1}{2}} \equiv -1 = \left(\frac{a}{p}\right)$. ☒

Satz 6.4 (Rechenregeln für das Legendre-Symbol)

Es gilt:

(a) $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{a \cdot b}{p}\right)$

(b) $a \equiv b \bmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(c) Ist $ggT(a,p)=1$, dann ist $\left(\frac{a^2 \cdot b}{p}\right) = \left(\frac{b}{p}\right)$

Beweis:

(a) Mit 6.3(b) folgt $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = (a\cdot b)^{\frac{p-1}{2}} \overset{6.3}{\equiv} \left(\frac{ab}{p}\right)$

(b) klar!

(c) Für (c) bemerke, dass $a^2 \cdot b$ genau dann quadr. Nichtrest ist, wenn b quadr. Nichtrest ist. ▭

Korollar 6.5 (1. Ergänzungssatz zum QR)

Sei $p>2$ eine Primzahl, dann

$$\left(\frac{-1}{p}\right) \overset{6.3b)}{=} (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases}$$

Definition 6.6

Sei p eine Primzahl. Sei $x \in \mathbb{Z}$ mit $ggT(x,p)=1$

Wir definieren $\langle x \rangle$ als die eindeutige ganze Zahl mit

$$-\left(\frac{p-1}{2}\right) \leq \langle x \rangle \leq \left(\frac{p-1}{2}\right) \text{ und } \langle x \rangle \equiv x \bmod p.$$

ist $\langle x \rangle < 0$ so heißt x negativer Rest mop p

$\langle x \rangle > 0$ so heißt x positiver Rest mod p

Satz 6.7 (Lemma von Gauß)

Sei $p>2$ eine Primzahl und $a \in \mathbb{Z}$ mit $ggT(a,p)=1$

Sei ferner $S = \{ 1 \leq i \leq \frac{p-1}{2} \mid \langle i\cdot a \rangle \text{ ist ein negativer Rest} \}$

& sei $s = \#S$.

Dann ist $\left(\frac{a}{p}\right) = (-1)^s$

Beweis:

a,p wie oben. Wir schreiben $\{\langle i\cdot a\rangle \mid 1 \leq i \leq \frac{p-1}{2}, i \in S\} = \{u_1, \dots, u_s\}$

$\{\langle i\cdot a\rangle \mid 1 \leq i \leq \frac{p-1}{2}, i \notin S\} = \{v_1 \dots v_t\}$

Wegen dem Kürzungssatz (4.6) sind die u_i & v_j paarweise verschieden.

$\Rightarrow u_1 \cdot \ldots \cdot u_s \cdot v_1 \cdot \ldots \cdot v_t \equiv \prod_{i=1}^{\frac{p-1}{2}} (i \cdot a) \equiv a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \quad (*)$

Es ist $-u_i \not\equiv v_j \bmod p \ \forall i,j$

Andernfalls schreibe $u_i = \langle k \cdot a \rangle$ & $v_j = \langle \ell \cdot a \rangle$ mit $1 \leq \ell, k \leq \frac{p-1}{2}$.

Kürzungssatz 4.6 $\Rightarrow -k \equiv \ell \bmod p$ ↯

Es sind $-u_i, v_j \in \{1, \ldots, \frac{p-1}{2}\}$ & da $-u_i \not\equiv v_j \bmod p$ ist

$\{-u_1, \ldots, -u_s, v_1, \ldots, v_t\} = \{1, \ldots, \frac{p-1}{2}\}$

$\Rightarrow (-u_1) \cdot (-u_2) \cdot \ldots \cdot (-u_s) \cdot v_1 \cdot \ldots \cdot v_t = 1 \cdot \ldots \cdot \left(\frac{p-1}{2}\right) = \left(\frac{p-1}{2}\right)!$

$\Rightarrow (-1)^s \cdot u_1 \cdot \ldots \cdot u_s v_1 \cdot \ldots \cdot v_t = \left(\frac{p-1}{2}\right)!$

Mit $(*)$ ist nun $(-1)^s \cdot a^{\left(\frac{p-1}{2}\right)} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \bmod p$

Mit dem Eulerschen Kriterium & dem Kürzungssatz (4.6.)

folgt nun $\left(\frac{a}{p}\right) \overset{6.3}{\equiv} a^{\frac{p-1}{2}} \equiv (-1)^s$ ∎

Korollar 6.8 (2. Ergänzungssatz zum QR)

Sei $p > 2$.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \bmod 8 \\ -1 & \text{falls } p \equiv \pm 3 \bmod 8 \end{cases}$$

Beweis:

Mit dem Lemma von Gauß ist

$\left(\frac{2}{p}\right) = (+1)^s$ mit $s = \left| \{ 1 \leq i \leq \frac{p-1}{2} \mid \langle 2 \cdot i \rangle < 0 \} \right|$

wir zeigen: $s = \frac{p^2-1}{8} \bmod 2$

Für j mit $1 \leq j \leq \frac{p-1}{2}$ ist $2 \leq 2j \leq p-1$

Also ist $0 < \langle 2 \cdot j \rangle \leq \frac{p-1}{2}$ ein positiver Rest genau dann, wenn $j \leq \left\lfloor \frac{p-1}{4} \right\rfloor \Rightarrow s = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$

Schreiben p als $p = \alpha + k \cdot 8$ mit $\alpha \in \{1, 3, 5, 7\}$ & unterscheiden 4 Fälle für α:

z.B. $\alpha = 1$, also $p = 1 + k \cdot 8$ ist $s = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor = 4k - 2k = 2k$ gerade

$\frac{p^2-1}{4} = \frac{(1 + 2 \cdot 8k + 8^2 4^2)}{8} = 2k + 8k^2$ gerade

Analog für die anderen $\alpha \in \{1, 3, 5, 7\}$ ∎

Satz 6.9 (quadratisches Reziprozitätsgesetz)

Seien p, q unterschiedliche Primzahlen. Es gilt:

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right)}$$

Bemerkung

Der obige Satz wurde zuerst von Euler vermutet & von Gauß bewiesen (im Alter von 21 Jahren)

Wir können die Aussage des QR wie folgt umformulieren:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\ -\left(\frac{q}{p}\right), & \text{falls } p \equiv 3 \bmod 4 \text{ oder } q \equiv 3 \bmod 4 \end{cases}$$

Lemma 6.11

Sei $p > 2$ eine Primzahl und a ungerade, mit $ggT(a,p) = 1$

Dann ist $\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$ mit $T(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{j\cdot a}{p} \right\rfloor$

Beweis:

Seien $\{u_1, \dots, u_s\}$ & $\{v_1, \dots, v_t\}$ wie in Beweis 6.7.

Insbesondere $\{-u_1, \dots, u_s, v_1, \dots, v_t\} = \{1, \dots, \frac{p-1}{2}\}$

Für $1 \leq j \leq \frac{p-1}{2}$ schreiben wir $j \cdot a$ als

$$j \cdot a = \left\lfloor \frac{j\cdot a}{p} \right\rfloor \cdot p + \rho_j \text{ mit } \rho_j \in \{1, \dots, \tfrac{p-1}{2}\}$$

Schreiben $\rho_j = \{u_1 + p, \dots, u_s + p\}$ falls $< \rho_j >$ negativ ist.

$\rho_j = \{v_1, \dots, v_t\}$ falls $< f_j >$ positiver Rest.

$$\Rightarrow \sum_{j=1}^{\frac{p-1}{2}} j\cdot a = p \cdot \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{j\cdot a}{p} \right\rfloor + \underbrace{\sum_{j=1}^{\frac{p-1}{2}} \rho_j}_{= p\cdot s + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j} \qquad (1)$$

Wegen $\{-u_1, \dots, -u_s, v_1, \dots, v_t\} = \{1, \dots, \frac{p-1}{2}\}$ folgt

$$\sum_{j=1}^{\frac{p-1}{2}} j = -\sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_t$$

$$(1)\cdot(2) \Rightarrow \underbrace{(a-1)\cdot\sum_{j=1}^{\frac{p-1}{2}} j}_{\equiv 0 \bmod 2 \text{ (da } a-1 \text{ gerade)}} \equiv p\cdot\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{ja}{p}\right\rfloor + p\cdot s + a\sum_{j=1}^{s} u_j$$

$$\equiv p\cdot T(p,a) + p\cdot s \bmod 2$$

Also $0 \equiv p\cdot T(p,a) + p\cdot s \bmod 2$

Da p ungerade ist folgt $s \equiv T(p,a) \bmod 2$, also mit dem Lemma v. Gauß folgt.

$$\left(\frac{a}{p}\right) \overset{\text{Gauß}}{=} (-1)^s \equiv (-1)^{T(p,a)} \qquad \square$$

Beweis von QR:

Mit Lemma 6.11 ist $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{T(p,q)+T(q,p)}$ mit

$T(p,q) = \sum_{j=1}^{\frac{q-1}{2}}\left\lfloor\frac{j\cdot p}{q}\right\rfloor$ & $T(q,p) = \sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{j\cdot q}{p}\right\rfloor$

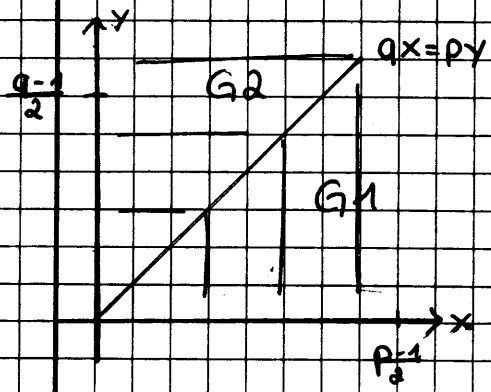
Wir zeigen $T(p,q) + T(q,p) \equiv \frac{(p-1)(q-1)}{4} \bmod 2$

Betrachte Menge

$G = \{(x,y)\in\mathbb{Z}\times\mathbb{Z} \mid 1 \le x \le \frac{p-1}{2},\ 1 \le y \le \frac{q-1}{2}\}$ & Teilmengen

$G_1 = \{(x,y)\in G \mid q\cdot x > p\cdot y\}$

$G_2 = \{(x,y)\in G \mid q\cdot x < p\cdot y\}$



Da p & q unterschiedliche Primzahlen sind ex. kein Paar $(x,y)\in G$ mit $qx = py$ $\Rightarrow G = G_1 \dot\cup G_2$

$\Rightarrow |G| = |G_1| + |G_2|$

Die Anzahl der Gitterpunkte (also Punkte von G) unterhalb der Geraden $qx = py$, also die Ordnung von G_1 ist

$$|G_1| = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor = T(q,p) \quad . \text{ Ebenso ist}$$

$$|G_2| = \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor = T(p,q)$$

$\Rightarrow$ Da $|G| = \frac{(p-1)(q-1)}{4}$ ist $T(p,q) + T(q,p) = \frac{(p-1)(q-1)}{4}$. $\square$