§4. Quadratische Reziprozität

Sei p eine Primzahl, $p \neq 2$. Wir betrachten quadratische Reste modulo p. In diesem Fall ist die Theorie viel schöner als im allgemeinen Fall.

Die Hälfte der Zahlen $1, 2, \dots, p-1$ sind quadratische Reste, die andere Hälfte nicht. warum?

$x^2 \equiv (p-x)^2 \pmod p$ warum? $\Rightarrow$ die quadratischen Reste sind $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ (und keine weiteren)

Quadratischer Rest bedeutet gerader Index, Nichtrest bedeutet ungerader Index.

(gerader Index + gerader Index = gerader Index) warum? $\Rightarrow$ Rest $\times$ Rest = Rest

4.1 Definition (Legendre): Das Legendre-Symbol ist definiert als

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{wenn } a \text{ quadratischer Rest mod } p \text{ ist} \\ -1, & \text{wenn } a \text{ quadratischer Nichtrest mod } p \text{ ist} \end{cases}$$

{ u a nach p u

Wie vorher bemerkt gilt also $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

Für $a \neq 0$ ist $a^{p-1} - 1 \equiv 0 \pmod p$ warum?

$p-1$ gerade, $p-1 =: 2q$, d.h. $\underbrace{a^{2q} - 1}_{\text{warum?}} \equiv 0 \Rightarrow \forall a: a^q \equiv 1 \pmod p$ oder $a^q \equiv -1 \pmod p$

u

$(a^q - 1)(a^q + 1)$

4.2 Theorem (Eulers Kriterium): Für alle a mit $a \not\equiv 0 \pmod p$ gilt:

$$\left(\frac{a}{p}\right) \equiv a^q \pmod p \text{ für } q = \frac{p-1}{2}$$

Beweis: Sei g eine Primitivwurzel, $a \equiv g^{\text{ind}\, a} \Rightarrow a^q \equiv g^{(\text{ind}\, a) \cdot q} \pmod p$

Falls ind a gerade: $\exists \alpha \in \mathbb{Z}$: ind $a = 2\alpha \Rightarrow$

$a^q \equiv g^{2\alpha q}$, $2\alpha q = \alpha \cdot (2q) = \alpha(p-1)$, ein Vielfaches von $p-1$

$\Rightarrow a^q \equiv (g^{p-1})^\alpha \equiv 1 \pmod p$

Falls ind a ungerade: $a^q \equiv g^{(\text{ind}\, a) \cdot q} \pmod p$, $2 \nmid \text{ind}\, a \Rightarrow p-1 = 2q \nmid \text{ind}\, a \cdot q$

g Primitivwurzel, $\text{ord}\, g = p-1 \Rightarrow g^{(\text{ind}\, a) q} \not\equiv 1 \pmod p$

$\Rightarrow a^q \equiv -1 \pmod p$. □

Damit sind quadratische Reste und Nichtreste sauber voneinander getrennt.

Beispiel: $a = p-1 \equiv -1 \pmod p \Rightarrow a^q \equiv bla\ (-1)^q = \begin{cases} 1, q \text{ gerade} \\ -1, q \text{ ungerade} \end{cases}$

$q = \frac{p-1}{2}$, also q gerade $\Leftrightarrow 2q$ durch 4 teilbar

$\Leftrightarrow p \equiv 1 \pmod 4 \Rightarrow$ erste Aussage ein:

4.3 Korollar: -1 ist ein quadratischer Rest für Primzahlen $p = 4k+1$ und ein quadratischer Nichtrest für Primzahlen $p' = 4k+3$.

Kennen wir diese Aussage schon?

Für $p = 4k+1$ gilt bla: $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$,

für $p' = 4k+3$ gilt bla: $\left(\frac{a}{p}\right) = -\left(\frac{p-a}{a}\right)$.

Beweis (der zweiten Aussage): $p - a \equiv -a \pmod p \Rightarrow \left(\frac{p-a}{p}\right) = \left(\frac{-1\cdot a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$

und $\left(\frac{-1}{p}\right) = \begin{cases} 1, p = 4k+1 \\ -1, p' = 4k+3 \end{cases}$ □

In Kongruenzen heißt das: $x^2 + 1 \equiv 0$ ist lösbar für $p = 4k+1$ und unlösbar für $p' = 4k+3$.

Bei Legendre-Symbolen findet man überraschende Zusammenhänge.

Zuerst eine Rechenregel:

Sei $a \not\equiv 0 \pmod p$ wir wollen $\left(\frac{a}{p}\right)$ berechnen, für $p > 2$. Sei $q := \frac{p-1}{2}$.

Wir betrachten die Zahlen $a, 2a, 3a, \dots, qa$. Jede solche Zahl ist, wie jede ganze Zahl, modulo p kongruent zu einer ganzen Zahl im offenen Intervall $\left(-\frac{p}{2}, \frac{p}{2}\right)$. Manche sind kongruent zu einer negativen Zahl, $\not\in \mathbb{N}$ andere zu einer positiven Zahl. $\in \mathbb{N}$

Sei r die Anzahl der negativen Zahlen, die sich dabei ergeben.

Überraschung:

4.4 Lemma (Gauß): $\left(\frac{a}{p}\right) = (-1)^r$

In anderen Worten: a ist ein quadratischer Rest genau dann, wenn r eine gerade Zahl ist.

Beweis: $a \not\equiv 0 \pmod p$, also wähle $a \in \{1, \dots, p-1\} = \{1, \dots, q\} \cup \{q+1, \dots, p-1\}$

$q = \frac{p-1}{2} < \frac{p}{2}$ $\quad \{q+1, \dots, p-1\}$ hat dieselben Repräsentanten modulo p wie $\{q+1-p, \dots, p-1-p = -1\}$, $q+1-p = \frac{p+1}{2} - p = \frac{1-p}{2} > -\frac{p}{2}$

Damit haben wir für $\{1,\dots,q\}$ Repräsentanten in $(0,\frac{p}{2})$ gefunden und für $\{q+1,\dots,p-1\}$ Repräsentanten in $(-\frac{p}{2},0)$.
Nun überlegen wir, wann Vielfache von a derselben Zahl in $\{\pm1,\dots,\pm q\}$ kongruent sind oder kongruent bis auf Vorzeichen.
Sei $h\in\{\pm1,\dots,\pm q\}$ und $\bar{i}a\equiv h\equiv \bar{j}a \pmod p$, für $1\le i,j\le q$.
$\Rightarrow p\mid(i-j)a$. Aber $p\nmid a$ ($q<p$) $\Rightarrow p\mid(i-j)\Rightarrow i=j$ nachprüfen!
Sei $\bar{i}a\equiv h\equiv -\bar{j}a \pmod p$, für $1\le i,j\le q$. $p\nmid a\Rightarrow p\mid(\underbrace{i+j}_{<p})$ ↯
Für $\bar{i}\neq\bar{j}$ erhält man also verschiedene
Vielfache von a. Das bedeutet: Jede der q vielen Zahlen $a,2a,3a,\dots,qa$ wird eindeutig einem Repräsentanten h zugeordnet, $|h|\in\{1,\dots,q\}$, mit einem Vorzeichen, also entweder $|h|$ oder $-|h|$. Modulo p ergibt sich also:
$a\cdot 2a\cdot 3a\cdot\ldots\cdot qa\equiv(\pm1)\cdot(\pm2a)\cdot\ldots\cdot(\pm q) \pmod p$
$2,3,\dots,q$ sind modulo p invertierbar, also kürzbar $\Rightarrow a^q\equiv(-1)^\nu$ (III 4.2) $\left(\frac{a}{p}\right)$ □

Beispiel: $a=2$, die Frage ist also: Wann ist 2 ein quadratischer Rest modulo p, äquivalent dazu: Wann gibt es in $\mathbb{Z}/p\mathbb{Z}$ eine Wurzel aus 2? Um Ψ anzuwenden, berechnen wir
$a,2a,\dots,\tilde{2},\Psi,b,\dots,2q=p-1$
Bis $\frac{p}{2}$ erhalten wir schon gleich die Repräsentanten (alle positiv), danach müssen wir p abziehen und erhalten negative Repräsentanten. Wir müssen also die Zahlen der Form 2x zählen, die zwischen $\frac{p}{2}$ und p liegen: $\frac{p}{2}<2x<p$, bzw $\frac{p}{4}<x<\frac{p}{2}$.
Wir schreiben $p=8k+r$, $r\in\{1,3,5,7\}$ $\Rightarrow$ x sollte fällen: $2k+\frac{1}{4}r<x<4k+\frac{1}{2}r$
oder $\frac{1}{4}r<y<2k+\frac{1}{2}r$ (dieselbe Zahl von y wie von x), oder
$\frac{1}{4}r<z<\frac{1}{2}r$ warum rechtes, diese zu zählen, wenn uns nur das Vorzeichen interessiert?

$r=1$:	kein z	$\nu=0$	$(-1)^\nu=1$
$r=3$:	$z=1$	1	-1
$r=5$:	$z=2$	1	-1
$r=7$:	$z\in\{2,3\}$	2	1

was folgt daraus?

Ergebnis: 2 ist ein quadratischer Rest modulo p genau für
$p = 8k \pm 1$ (und nicht für $p = 8k \pm 3$)

Beispiel: $a = 3$, also sind die relevanten Zahlen $3, 6, 9, \dots, 3q = \frac{3}{2}(p-1)$,
genauer die negativen Zahlen, die zwischen $\frac{p}{2}$ und p liegen
$\rightsquigarrow \frac{p}{2} < 3x < p$ (oBdA $p \neq 3$) $\rightsquigarrow \frac{p}{6} < x < \frac{p}{3}$
Sei $p = 12k + r$, $r \in \{1, 5, 7, 11\}$ warum nur dieser?
$\rightsquigarrow 2k + \frac{r}{6} < x < 4k + \frac{r}{3} \rightsquigarrow \frac{r}{6} < y < \frac{r}{3}$, gesucht: diese y

$r=1$	kein y	$v=0$	$(-1)^v = 1$
5	$y=1$	$v=1$	-1
7	$y=2$	1	-1
11	$y \in \{2,3\}$	2	1

Ergebnis: 3 ist ein quadratischer Rest modulo $p = 12k \pm 1$
(und nicht modulo $p = 12k \pm 5$).
Das wirkt systematisch: Die Ergebnisse hängen nicht von p ab, sondern
vom Rest r (wovon hängt r ab?). Und es gibt eine Symmetrie: dieselbe
Antwort für r und für $8-r$ bzw $12-r$. Genauer hat Euler vermutet:
4.5 Theorem: Sei $p = 4ak + r$ mit $0 < r < 4a$ und $p' = 4ak' + r'$ mit
$0 < r' < 4a$. Dann ist $\left(\frac{a}{p}\right) = \left(\frac{a}{p'}\right)$ falls $r = r'$ oder $r' = 4a - r$.
Beweis: Wir folgen den Beispielen.
Sei $q := \frac{p-1}{2}$. Wir betrachten $a, 2a, 3a, \dots, qa$ und zählen, wieviele dieser
Zahlen zwischen $\frac{p}{2}$ und p – oder $\frac{3}{2}p$ und $2p$ oder – – liegen und damit zu
negativem Vorzeichen führen. Es geht um die Intervalle $(\frac{1}{2}p, p)$,
$(\frac{3}{2}p, 2p), \dots ((b-\frac{1}{2})p, bp)$ für $b \in \{\frac{1}{2}a, \frac{1}{2}(a-1)\}$ (b ist die ganze Zahl in
dieser Menge) warum ist das der richtige b? warum sind die Intervalle offen?
Wie in den Beispielen können wir durch a dividieren und statt Vielfachen
von a einfach ganze Zahlen suchen, jetzt in den Intervallen
$(\frac{p}{2a}, \frac{p}{a}), (\frac{3p}{2a}, \frac{2p}{a}), \dots, (\frac{(2b-1)}{2}\frac{p}{a}, \frac{bp}{a})$.

Sei $p = 4ak+r$. $\frac{4ak}{2a}$ ist gerade ganze Zahl. Wie in den Beispielen können wir diese Zahlen ignorieren und nur noch auf r achten. Wir suchen also ganze Zahlen in $\left(\frac{r}{2a}, \frac{r}{a}\right), \left(\frac{3r}{2a}, \frac{2r}{a}\right), -\left(\frac{(2b-1)r}{2a}, \frac{br}{a}\right)$. Deshalb hängt v nur von r ab, aber nicht von k.
Aus $r=r'$ folgt deshalb $\left(\frac{a}{p}\right) = \left(\frac{a}{p'}\right)$. nachprüfen: b hängt nur von a ab, nicht von p
Damit ist die (wichtigere) erste Aussage schon bewiesen.
Zweite Aussage: Was passiert, wenn r a in $4a-r$ geändert wird?
Aus $\left(\frac{r}{2a}, \frac{r}{a}\right)$ wird $\left(\frac{4a-r}{2a}, \frac{4a-r}{a}\right) = \left(2-\frac{r}{2a}, 4-\frac{r}{a}\right)$, und dann folgen die Intervalle $\left(6-\frac{3r}{2a}, 8-\frac{2r}{a}\right), -, \left(4b-2-\frac{(2b-1)}{2a}r, 4b-\frac{br}{a}\right)$. Wir zeigen, daß sich bei dieser Veränderung der Wert von $(-1)^v$ nicht ändert.
Wenn wir allgemein (x,y) durch $(-y,-x)$ ersetzen, bleibt die Anzahl der ganzen Zahlen gleich, also auch das "Vorzeichen" v. Ebenso können wir $(-y,-x)$ durch $(2k-y, 2k-x)$ ersetzen.
Also ist auch $\left(2-\frac{r}{2a}, 4-\frac{r}{a}\right) \rightsquigarrow \left(\frac{r}{a}, 2+\frac{r}{2a}\right)$ erlaubt.
Wir wollen also $\left(\frac{r}{2a}, \frac{r}{a}\right)$ mit $\left(\frac{r}{a}, 2+\frac{r}{2a}\right)$ vergleichen.
$\frac{r}{a} \notin \mathbb{Z} \Rightarrow \underbrace{\left(\frac{r}{2a}, \frac{r}{a}\right)}_{\text{"Vorzeichen" } v} \cup \underbrace{\left(\frac{r}{a}, 2+\frac{r}{2a}\right)}_{\text{"Vorzeichen" } v'}$ enthält genau zwei ganze Zahlen $\Rightarrow v+v' = 2 \Rightarrow (-1)^v = (-1)^{v'}$
Bei den anderen Intervallen genauso. □

Das kann man so umschreiben, daß es sehr mysteriös wirkt und sehr praktisch ist.

4.6 Theorem (Quadratisches Reziprozitätsgesetz, Gauß 1796):
Seien p und q verschiedene ungerade Primzahlen. Dann gilt:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Das bedeutet: $p \equiv q \equiv 1 \pmod 4 \Rightarrow \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ nachprüfen
$p \equiv q \equiv 3 \pmod 4 \Rightarrow \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$
$p \not\equiv q \pmod 4 \Rightarrow \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

In Worten: Falls $p \equiv q \equiv 3 \pmod 4$, ist genau eine der beiden Gleichungen $x^2 \equiv q \pmod p$ und $x^2 \equiv p \pmod q$ lösbar.
Sonst sind immer beide Gleichungen lösbar oder beide nicht lösbar.

Was soll daran praktisch sein? Man kann damit Legendre-Symbole wirklich ausrechnen!
Beispiel: Gesucht ist $\left(\frac{870}{7}\right)$. 7 ist prim
$870 = ? = 2 \cdot 3 \cdot 5 \cdot 29$
Aus $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ folgt hier: $\left(\frac{870}{7}\right) = \left(\frac{2}{7}\right) \cdot \left(\frac{3}{7}\right) \cdot \left(\frac{5}{7}\right) \cdot \left(\frac{29}{7}\right)$

Wir kennen schon: $\left(\frac{2}{7}\right) = 1$ und $\left(\frac{3}{7}\right) = -1$
oder wir benutzen 4.6: $3 \equiv 7 \pmod 4 \Rightarrow \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$, da 1 ein Quadrat ist
wieder mit 4.6: $\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)$ weil $5 \equiv 1 \pmod 4$
$= \left(\frac{2}{5}\right) \equiv -1$ (kennen wir schon)

$\left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = 1$. Insgesamt $\left(\frac{870}{7}\right) = 1 \cdot (-1) \cdot (-1) \cdot 1 = 1$

(Das geht auch einfacher: $870 \equiv 2 \pmod 7$.
Oder mit Eulers Kriterium: $\left(\frac{a}{q}\right) \equiv a^q \pmod p$ für $q = \frac{p-1}{2}$. Also hier:
$\left(\frac{2}{7}\right) \equiv 2^3 \equiv 8 \equiv 1 \pmod 7$, $\left(\frac{3}{7}\right) \equiv 3^3 \equiv -1 \pmod 7$,
$\left(\frac{5}{7}\right) = \left(\frac{-2}{7}\right) \equiv (-2)^3 \equiv -1 \pmod 7$, $\left(\frac{29}{7}\right) = \left(\frac{1}{7}\right)$.)

Quadratische Reziprozität hilft besonders, wenn p und q verschieden groß sind. Dann kann man die große Primzahl nach oben bringen und modulo der kleineren reduzieren.
Beispiel dazu:

Ist $x^2 \equiv 57 \pmod{127}$ lösbar?

$\left(\frac{57}{127}\right) = \left(\frac{3}{127}\right) \cdot \left(\frac{19}{127}\right)$

$\left(\frac{3}{127}\right) = (-1)\left(\frac{127}{3}\right) = (-1)\left(\frac{1}{3}\right) = -1$ nachrechnen

$\left(\frac{19}{127}\right) = (-1)\left(\frac{127}{19}\right) = (-1)\left(\frac{13}{19}\right) = (-1)\left(\frac{19}{13}\right) = (-1)\left(\frac{6}{13}\right) =$

$= (-1)\left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right) = (-1) \cdot (-1)\left(\frac{13}{3}\right) = (-1) \cdot (-1) \cdot \left(\frac{1}{3}\right) = 1$

$\Rightarrow \left(\frac{57}{127}\right) = -1 \Rightarrow$ Die Kongruenz hat keine Lösung.

Beweis von 4.6: Wir unterscheiden zwei Fälle:

Erster Fall: $p \equiv q \pmod 4$, o.B.d.A. $p > q$, $p - q = 4a$, $p = q + 4a$

$\Rightarrow \left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{4}{q}\right) \cdot \left(\frac{a}{q}\right)$

$\left(\frac{4}{q}\right) = 1$, da $4 = 2^2$

und $\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right)\left(\frac{a}{p}\right)$

$\left(\frac{4}{p}\right) = 1$

Wegen $p \equiv q \pmod 4$ ist 4.5 anwendbar $\Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$

$\Rightarrow \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right) \overset{\text{warum?}}{=} \begin{cases} 1 \text{ falls } p \equiv q \equiv 1 \pmod 4 \\ -1 \text{ falls } p \equiv q \equiv 3 \pmod 4 \end{cases}$

Zweiter Fall: $p \not\equiv q \pmod 4$, also $p \equiv -q \pmod 4$ weil $3 \equiv -1$

$\Rightarrow 4 \mid p + q =: 4a$

$\Rightarrow \left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{4}{q}\right) \cdot \left(\frac{a}{q}\right) = \left(\frac{a}{q}\right)$

$\left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = ? = \left(\frac{a}{p}\right)$

$p \equiv -q \pmod 4 \underset{4.5}{\Rightarrow} \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ □

Die Hälfte der Zahlen $1, \dots, p-1$ sind quadratische Reste, die andere Hälfte nicht. Häufen die Reste sich irgendwo oder ist die Verteilung eher zufällig, d.h. „gleichverteilt“? Wenn z.B. erst alle Reste kommen und dann alle Nichtreste, oder umgekehrt, d.h. etwa RR...RN...N oder N...NR...R, dann ist es sehr selten, daß bei Nachbarn RN oder NR vorkommt. Wenn Reste und Nichtreste sich gleichmäßig abwechseln, dann ist NN und RR sehr selten. Um „Zufall“ zu sehen, können wir überlegen wie oft NN, NR, RN und RR vorkommen.

Die Folge $1, \dots, p-1$ beginnt mit R ($1 = 1^2$). $\underbrace{p-1}_{\equiv -1 \pmod p}$ hat Legendre-Symbol $(-1)^{\frac{1}{2}(p-1)}$.

Bezeichnung: (RR) ist die Anzahl der Paare $i, i+1$, sodaß i und $i+1$ quadratische Reste sind.

(*)
$$\begin{cases} \text{Gleichungen: } (RR)+(RN) = \#\{(u,u+1) : u \text{ ist Rest}\} = \frac{1}{2}(p-2-(-1)^{\frac{1}{2}(p-1)}) \\ \text{Warum? } u \text{ läuft durch alle quadratischen Reste mit Ausnahme von } p-1, \\ \text{falls dieser ist - weil es dafür kein } u+1 \text{ in } \{1,\dots,p-1\} \text{ gibt} \quad \text{nachprüfen} \\ (NR)+(NN) = \frac{1}{2}(p-2+\varepsilon),\ \varepsilon := (-1)^{\frac{1}{2}(p-1)} \\ (RR)+(NR) = \frac{1}{2}(p-1)-1 \quad \text{warum?} \\ (RN)+(NN) = \frac{1}{2}(p-1) \end{cases}$$

$\rightsquigarrow$ 4 Gleichungen, aber lineare Abhängigkeit:

Erste Gleichung + zweite Gleichung = dritte Gleichung + vierte Gleichung

Außerdem: $\left(\frac{u}{p}\right)\cdot\left(\frac{u+1}{p}\right) = \begin{cases} 1 \text{ für RR und NN} \\ -1 \text{ für RN und NR} \end{cases}$

$$\Rightarrow (RR)+(NN)-(RN)-(NR) = \sum_{u=1,\dots,p-2}\left(\frac{u(u+1)}{p}\right) \text{ - diese Summe berechnen wir}$$

u läuft von 1 bis $p-2$, ist also modulo p immer invertierbar.

Für u fest sei $q := u^{-1} \pmod p$.

$$\Rightarrow u(u+1) \equiv u(u+uq) \equiv u^2(1+q) \pmod p$$

$$\Rightarrow \left(\frac{u(u+1)}{p}\right) \overset{?}{=} \left(\frac{u^2}{p}\right)\left(\frac{1+q}{p}\right)$$

$u = -1 \Rightarrow q = -1$, d.h. die Inversen von $u \in \{1,\dots,p-2\}$ sind $q \in \{1,\dots,p-2\}$

$$\Rightarrow \sum_{n=1}^{p-2} \left(\frac{n(n+1)}{p}\right) = \sum_{n=1}^{p-2} \left(\frac{1+q}{q}\right) = \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \dots + \left(\frac{p-1}{2}\right)$$

Aber: $\left(\frac{1}{p}\right) + \dots + \left(\frac{p-1}{p}\right) = 0$, da zur Hälfte Reste, zur Hälfte Nichtreste

$$\Rightarrow \sum_{n=1}^{p-2} \left(\frac{n(n+1)}{p}\right) = -\left(\frac{1}{p}\right) = -1$$

$$\Rightarrow (RR) + (NN) - (RN) - (NR) = -1 \quad +$$

$$+ \quad (RR) \quad + (RN) \quad = \frac{1}{2}(p-2-\varepsilon) +$$

$$+ \quad (NN) \quad + (NR) = \frac{1}{2}(p-2+\varepsilon)$$

$$\Rightarrow 2(RR) + 2(NN) = p-3$$

3. Gleichung minus 2. Gleichung: $(RR) - (NN) = -\frac{1}{2}(1+\varepsilon)$ (Tafel vorige Seite)

$\Rightarrow (RR) = \frac{1}{4}(p-4-\varepsilon)$, analog für die anderen Daten Dafür?

$\Rightarrow$ alle sind ungefähr $\frac{p}{4}$ (da ist keine ganze Zahl), genauer: alle zwischen $\frac{1}{4}(p-5)$ und $\frac{1}{4}(p+1)$

$\Rightarrow$ alle ungefähr gleich groß $\rightsquigarrow$ die Verteilung wirkt "zufällig"

↑ aber es gibt eine kleine Abweichung, weil 1 ein Rest ist, und nicht "zufällig"

Quadratische Reste kommen auch in ganz anderen Bereichen der Zahlentheorie vor. Im nächsten Kapitel sehen wir eine Anwendung.