Wiederholung:

Lemma 5.4: Seien $a, b \in \mathbb{Z}$

(i) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$

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

Beweis: (i): Es ist klar, dass $a^{\frac{p-1}{2}} \equiv 0 \bmod p \iff \left(\frac{a}{p}\right) = 0$.

Also nehmen wir an, dass $p \nmid a$.

Es ist $a^{p-1} \equiv 1 \bmod p$ (kleiner Fermatsche Satz)

also ist $(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \equiv 0 \bmod p$

$\Rightarrow a^{\frac{p-1}{2}} \equiv 1$ oder $-1 \bmod p$.

$\left(\frac{a}{p}\right) = 1 \Rightarrow a \equiv c^2 \bmod p$ für ein $c \in \mathbb{Z}$

$\Rightarrow a^{\frac{p-1}{2}} \equiv (c^2)^{\frac{p-1}{2}} \bmod p$

$\equiv c^{p-1} \bmod p$

$\equiv 1 \bmod p$ (kFS)

Andererseits, sei $a \equiv g^r \bmod p$ für eine primitive Wurzel g und ein $r \in \{1, \dots, p-1\}$

Dann gilt $a^{\frac{p-1}{2}} \equiv 1 \bmod p \Rightarrow g^{r\frac{p-1}{2}} \equiv 1 \bmod p$

$\Rightarrow p-1 \mid r\frac{p-1}{2}$

$\Rightarrow 2 \mid r$

$\Rightarrow a \equiv (g^{r/2})^2 \bmod p$

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

Also $\left(\frac{a}{p}\right) = 1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \mod p$

und daher auch

$$\left(\frac{a}{p}\right) = -1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \mod p$$

■

(ii) Wegen (i) gilt

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p,$$

und da $p > 2$ (also $-1, 0, 1$ paarweise verschieden mod p) ist dann $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

□

Aus (ii) folgt Lemma 5.1 direkt, sogar mit der Erweiterung: Falls c, d quadratische ~~Reste~~ Nichtreste mod p sind, ist cd ein quadratischer Rest mod p.

Satz 5.5: Die Gleichung $X^2 + bX + c = 0$ hat modulo p

- genau zwei verschiedene Lösungen — wenn $\left(\frac{b^2-4c}{p}\right) = 1$
- genau eine Lösung — wenn $\left(\frac{b^2-4c}{p}\right) = 0$
- keine Lösung — wenn $\left(\frac{b^2-4c}{p}\right) = -1$.

Beweis: $X^2 + bX + c \equiv 0 \mod p$

$\Leftrightarrow 4X^2 + 4bX + 4c \equiv 0 \mod p$

$\Leftrightarrow (2X+b)^2 - b^2 + 4c \equiv 0 \mod p$

$\Leftrightarrow (2X+b)^2 \equiv b^2 - 4c \mod p$

Daraus folgt die Behauptung $\square$

(Falls $\left(\frac{b^2-4c}{p}\right) = 1$ existiert eine Lösung zu $y^2 \equiv b^2 - 4c \mod p$ und $-y \neq y$ ist die zweite Lösung.)

Sei $H = \{1, 2, \ldots, \frac{p-1}{2}\}$

Jede Zahl $a \in \{1, \ldots, p-1\}$ hat die Form $a \equiv \pm h \mod p$ für ein $h \in H$

z. B. für $p=5$, $H = \{1, 2\}$

$1 \equiv +1 \mod 5$
$2 \equiv +2 \mod 5$
$3 \equiv -2 \mod 5$
$4 \equiv -1 \mod 5$

Sei a fixiert

Es ist
$$\left.\begin{aligned} a &\equiv \varepsilon_1 h_1 \\ 2a &\equiv \varepsilon_2 h_2 \\ &\vdots \\ \tfrac{p-1}{2} a &\equiv \varepsilon_{\frac{p-1}{2}} h_{\frac{p-1}{2}} \end{aligned}\right\} \quad \begin{aligned} h_i &\in H \\ \varepsilon_i &\in \{1, -1\} \end{aligned}$$

Lemma 5.6 (Gauß Lemma):

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i$$

Beweis: Erst zeigen wir, dass die h_i paarweise verschieden sind.

Denn $h_i = h_j \Rightarrow h_i^2 = h_j^2$

$$\Rightarrow (\varepsilon_i h_i)^2 = (\varepsilon_j h_j)^2$$

$$\Rightarrow (ia)^2 \equiv (ja)^2 \mod p$$

$$\Rightarrow i^2 \equiv j^2 \mod p$$

$$\Rightarrow (i+j)(i-j) \equiv 0 \mod p$$

$$\Rightarrow i \equiv \pm j \mod p$$

$$\Rightarrow i = j \quad (\text{da } i, j \in H)$$

Also ist $\{h_1, \ldots, h_{\frac{p-1}{2}}\} = \{1, \ldots, \frac{p-1}{2}\} = H$

Beispiel: $p = 7$, $a = 2$

$2 \equiv +2 \mod 7$

$4 \equiv -3 \mod 7$

$6 \equiv -1 \mod 7$

$\hookrightarrow H = \{1, 2, 3\}$

Also

$$a^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} i = \prod_{i=1}^{\frac{p-1}{2}} (ia) \equiv \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \prod_{i=1}^{\frac{p-1}{2}} h_i \mod p$$

$$\equiv \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \prod_{i=1}^{\frac{p-1}{2}} i$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \mod p$$

$$\Rightarrow \left(\frac{a}{p}\right) \equiv \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \mod p \quad \text{(Eulersches Kriterium)}$$

$$\Rightarrow \left(\frac{a}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i$$

Satz 5.7 (Das Quadratisches Reziprozitätsgesetz):

Seien $p, q \in \mathbb{P} \setminus \{2\}$. Dann gilt

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{wenn } p, q \equiv 3 \mod 4 \\ \left(\frac{p}{q}\right) & \text{sonst.} \end{cases}$$

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

Um $\left(\frac{a}{p}\right)$ leicht ausrechnen zu können, brauchen wir noch die zwei „Ergänzungssätze".

Satz 5.8 (1. Ergänzungssatz zum QRG)

$$\left(\frac{-1}{p}\right) = \begin{cases} -1 & \text{wenn } p \equiv 3 \mod 4 \\ 1 & \text{wenn } p \equiv 1 \mod 4 \end{cases}$$

äquivalent: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Mit Satz 5.7 kann man ein Legendre-Symbol für Primzahlen „umdrehen": um $\left(\frac{q}{p}\right)$ auszurechnen können wir auch $\left(\frac{p}{q}\right)$ ausrechnen.

Aber nicht wenn $q = 2$.

Satz 5.9 (2. Ergänzungssatz zum QRG)

$$\left(\frac{2}{p}\right) = \begin{cases} -1 & \text{falls } p \equiv 3,5 \mod 8 \\ 1 & \text{falls } p \equiv 1,-1 \mod 8. \end{cases}$$

äquivalent: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Beispiel: $\left(\frac{110}{173}\right)$ $\left(\equiv 110^{86} \mod 173 \text{ - Eulersches Kriterium} \right.$
$\left. \equiv ? \right)$

$$\left(\frac{110}{173}\right) = \left(\frac{2}{173}\right)\left(\frac{5}{173}\right)\left(\frac{11}{173}\right)$$

$$= (-1)\cdot\left(\frac{173}{5}\right)\cdot\left(\frac{173}{11}\right) \qquad 173 \equiv 5 \mod 8 \equiv 1 \mod 4$$

$$= (-1)\cdot\left(\frac{3}{5}\right)\cdot\left(\frac{8}{11}\right)$$

$$= (-1)\cdot\left(\frac{5}{3}\right)\cdot\left(\frac{-1}{11}\right)\left(\frac{3}{11}\right) \qquad 5 \equiv 1 \mod 4$$

$$= (-1)\cdot\left(\frac{2}{3}\right)\cdot(-1)\cdot\left(-\left(\frac{11}{3}\right)\right) \qquad 11 \equiv 3 \mod 4,\ 3 \equiv 3 \mod 4$$

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

$$= -1$$

110 ist ein quadratischer Nichtrest modulo 173

Beweise: Nächstes Mal.