LEGENDRESYMBOL & LUCAS-LEHMER-TEST

GABRIEL DETTLING

Lemma 1. *Endliche Körper haben zyklische Einheitengruppen.*

Beweis. Sei K ein endlicher Körper. Nach dem Klassifikationssatz für endlich erzeugte abelsche Gruppen ist

$$K^\times \cong \mathbb{Z}/e_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/e_r\mathbb{Z}$$

mit $e_1 \mid e_2 \mid ... \mid e_r$. Daraus folgt, dass jedes Element von $K^\times$ eine Nullstelle von $X^{e_r} - 1$ ist. Ein Polynom in $K[X]$ vom Grad e_r hat jedoch höchstens e_r verschiedene Nullstellen in K. Es gilt also

$$\prod_{i=1}^{r} e_i = |K^\times| \leqslant e_r$$

und somit $r = 1$. $\square$

Definition 2. *Sei $a \in \mathbb{Z}$. Das **Legendresymbol** $\left(\frac{a}{p}\right)$ ist*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \textit{falls } a \equiv 0 \bmod p \\ +1 & \textit{falls } a \equiv b^2 \bmod p \textit{ für ein } b \in \mathbb{Z} \\ -1 & \textit{sonst} \end{cases}$$

*Man sagt auch a ist ein **quadratischer Rest modulo** p falls $\left(\frac{a}{p}\right) = 1$. Da dies nur von der Restklasse von a modulo p abhängt schreiben wir auch $\left(\frac{a}{p}\right)$ für $a \in \mathbb{Z}/p\mathbb{Z}$.*

Lemma 3. *Sei p eine Primzahl und g eine Primitivwurzel modulo p, d.h. ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$. Dann sind die quadratischen Reste in $\mathbb{Z}/p\mathbb{Z}$ genau $\{g^{2k} \mid k \in \mathbb{Z}\}$, und für p ungerade ist*

$$\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) = 0$$

Beweis. Es ist klar, dass jedes solche Element ein quadratischer Rest ist. Ist umgekehrt $a = b^2$ für $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$, so ist $b = g^k$ für ein $k \in \mathbb{Z}$ und somit $a = g^{2k}$.

Für p ungerade ist $|(\mathbb{Z}/p\mathbb{Z})^\times|$ gerade, und somit sind für ein $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ die k mit $g^k = a$ alle gerade oder alle ungerade. Also ist $\left(\frac{g^{2k+1}}{p}\right) = -1$ für alle $k \in \mathbb{Z}$. Die obige Gleichung folgt also aus $\mathbb{Z}/p\mathbb{Z} = \{0, g, g^2, ..., g^{p-2}, g^{p-1}\}$. $\square$

Theorem 4. *(Eulersches Kriterium) Ist p eine ungerade Primzahl, so gilt*

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

für alle $a \in \mathbb{Z}$

Beweis. Für $a \equiv 0 \bmod p$ sind beide Seiten 0. Sei also ab jetzt $a \not\equiv 0 \bmod p$. Dann gilt

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

$\Rightarrow$ Ist $a \equiv b^2 \bmod p$, so ist $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \bmod p$

$\Leftarrow$ Sei g eine Primitivwurzel modulo p, und schreibe $a \equiv g^k$ für $k \in \{1, ...p-1\}$. Aus

$$g^{k\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1$$

folgt $(p-1) \mid k\frac{p-1}{2}$. Somit ist k gerade und nach Lemma 3 ist $\left(\frac{a}{p}\right) = 1$

Da wegen $(a^{\frac{p-1}{2}})^2 = a^{p-1} \equiv 1$ beide Seiten Werte in $\{\pm 1\}$ haben, beweist dies die Aussage des Satzes. $\square$

Korollar 5. *Für alle $a, b \in \mathbb{Z}$, p prim gilt*

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

Beweis. Mit dem Eulerschen Kriterium (4), bzw. für $p = 2$ mit $\left(\frac{a}{p}\right) \equiv a \bmod 2$, folgt dass die beiden Seiten Kongruent modulo p sind. Da zudem beide Seiten Werte in $\{\pm 1, 0\}$ bzw. für $p = 2$ in $\{0, 1\}$ haben impliziert die Kongruenz eine Gleichheit. □

Proposition 6. *Ist p eine ungerade Primzahl, so gilt*

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

Beweis. Wir bemerken zunächst, dass $(-1)^{\frac{p^2-1}{8}}$ nur von p modulo 8 abhängt:

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

Dasselbe gilt für $\left(\frac{2}{p}\right)$: nach dem Eulerschen Kriterium 4 ist

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

Mit $2 = (-i)(1+i)^2$ gilt in $\mathbb{Z}[i]$:

$$2^{\frac{p-1}{2}} = (-i)^{\frac{p-1}{2}}(1+i)^{(p-1)} = \frac{(-i)^{\frac{p-1}{2}}}{1+i}(1+i)^p \equiv \frac{(-i)^{\frac{p-1}{2}}}{(1+i)}(1+i^p) \bmod p$$

Wegen $i^4 = 1$ ist der rechte Term auch nur abhängig von p modulo 8. Da p ungerade ist, genügt es die Gleichheit für $p \equiv \pm 1, \pm 3 \bmod 8$ zu prüfen. Sowohl im obigen Ausdruck als auch in $(-1)^{\frac{p^2-1}{8}}$ erhalten wir 1 für $p \equiv \pm 1 \bmod 8$ und -1 für $p \equiv \pm 3 \bmod 8$. □

Definition 7. *Sei p prim, $\xi = e^{\frac{2\pi i}{p}}$. Die* ***Gaussumme*** *von $a \in \mathbb{Z}$ ist*

$$g_a = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi^{ai}.$$

Lemma 8. *Seien p, q verschiedene ungerade Primzahlen und $a \in \mathbb{Z}$, $a \not\equiv 0 \bmod p$. Dann gilt*

(1) $g_a = \left(\frac{a}{p}\right) g_1$
(2) $g_1^2 = \left(\frac{-1}{p}\right) p$
(3) $g_1^q \equiv g_q \bmod q$

Beweis. (1) Da alle Summanden nur von der Restklasse von i modulo p abhängen, können wir die Indexverschiebung $i \mapsto ai$ anwenden:

$$\left(\frac{a}{p}\right) g_1 = \left(\frac{a}{p}\right) \sum_{i=1}^{p-1} \left(\frac{ai}{p}\right) \xi^{ai} = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi^{ai} = g_a$$

Die zweite Gleichheit verwendet die Multiplikativität des Legendresymbols und $\left(\frac{a^2}{p}\right) = 1$.

(2) Wie in (1) verwenden wir die Indexverschiebung $j \mapsto ij$, und erhalten

$$g_1^2 = \sum_{i,j=1}^{p-1} \left(\frac{ij}{p}\right) \xi^{i+j} = \sum_{i,j=1}^{p-1} \left(\frac{i^2 j}{p}\right) \xi^{i(j+1)} = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \sum_{i=1}^{p-1} \xi^{i(j+1)}$$

Für $j = p-1$ ist $\xi^{i(j+1)} = (\xi^p)^i = 1$. Für $j + 1 \not\equiv 0 \bmod p$ ist

$$\sum_{i=1}^{p-1} \xi^{i(j+1)} = \sum_{i=1}^{p-1} \xi^i = \frac{\xi^p - 1}{\xi - 1} - 1 = -1$$

Also erhalten wir

$$g_1^2 = (p-1)\left(\frac{p-1}{p}\right) - \sum_{i=1}^{p-2} \left(\frac{i}{p}\right)$$

Aber nach Lemma 3 ist $\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)=0$. Somit folgt (2):

$$g_1^2 = p\left(\frac{p-1}{p}\right) = p\left(\frac{-1}{p}\right)$$

(3) Da q prim und ungerade ist, gilt

$$g_1^q = \left(\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\xi^i\right)^q \equiv \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)^q \xi^{iq} = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\xi^{iq} = g_q \bmod q$$

□

Theorem 9. *(quadratische Reziprozität) Sind p,q ungerade verschiedene Primzahlen, so gilt*

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

Beweis. Nach Lemma 8, Teil (2) und (3) ist

$$g_q \equiv g_1^q = g_1(g_1^2)^{\frac{q-1}{2}} = g_1\left(\left(\frac{-1}{p}\right)p\right)^{\frac{q-1}{2}} \bmod q$$

Nach Teil (1) ist

$$g_q = g_1\left(\frac{q}{p}\right)$$

Da aus Lemma 8, Teil (2) $g_1 \not\equiv 0 \bmod q$ folgt, ist

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

Mit dem Eulerschen Kriterium 4 und der Multiplikativität erhalten wir

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

Analog zum Beweis der Multiplikativität sind hier beide Seiten in $\{\pm 1\}$, und deshalb sind sie nicht nur kongruent sondern sogar gleich. □

Theorem 10. *(Lucas-Lehmer-Test) Sei $(S_k)_{k\geqslant 1}$ die Folge definiert durch $S_1 = 4$ und $S_{k+1} = S_k^2 - 2$. Ist p eine ungerade Primzahl, und $n = 2^p - 1$ so gilt:*

$$n \textit{ ist prim} \iff n \mid S_{p-1}$$

Beweis. Seien $\omega = 2+\sqrt{3}, \bar\omega = 2-\sqrt{3}$. Mit einem Induktionsargument folgt $S_{k+1} = \omega^{2^k} + \bar\omega^{2^k}$ für alle $k \geqslant 1$.

⇒ Angenommen n sei Prim: Aus dem eulerschen Kriterium folgt

$$2^{\frac{n-1}{2}} \equiv \left(\frac{2}{n}\right) = \left(\frac{2+2n}{n}\right) = 1 \bmod n$$

Mit $\omega = \frac{1}{2}(1+\sqrt{3})^2$ und $2^{p-1} = \frac{n+1}{2}$ rechnen wir nun

$$\omega^{2^{p-1}} \equiv 2^{\frac{n-1}{2}}\omega^{\frac{n+1}{2}} = \frac{1}{2}(1+\sqrt{3})^{n+1} \equiv \frac{1}{2}(1+\sqrt{3}^n)(1+\sqrt{3}) = \frac{1}{2}(1+3^{\frac{n-1}{2}}\sqrt{3})(1+\sqrt{3}) \bmod n$$

Aus dem quadratischen Reziprozitätsgesetz, sowie $n \equiv (-1)^p - 1 \equiv -2 \equiv 1 \bmod 3$ erhalten wir

$$3^{\frac{n-1}{2}} \equiv \left(\frac{3}{n}\right) = -\left(\frac{n}{3}\right) = -\left(\frac{1}{3}\right) = -1 \bmod n$$

Insgesamt folgt also

$$\omega^{2^{p-1}} \equiv \frac{1}{2}(1-\sqrt{3})(1+\sqrt{3}) = -1 \bmod n$$

$$S_{p-1} = \omega^{2^{p-2}} + \bar\omega^{2^{p-2}} = \bar\omega^{2^{p-2}}(\omega^{2^{p-1}}+1) \equiv 0 \bmod n$$

$\Leftarrow$ Sei umgekehrt $S_{p-1} = an$ für $a \in \mathbb{N}$. Falls ein Primfaktor $q \in [3, \sqrt{n}]$ von n existiert, so ist

$$\omega^{2^{p-1}} = S_{p-1}\omega^{2^{p-2}} - 1 \equiv -1 \bmod q$$

Somit ist ω eine Einheit der Ordnung 2^p in $\mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}]$:

Wegen $\omega^{2^p} = 1$ ist ω eine Einheit, und die Ordnung von ω teilt 2^p.

Wegen $\omega^{2^{p-1}} = -1$ und $-1 \neq 1$ da $q \neq 2$, kann die Ordnung von ω kein Teiler von 2^{p-1} sein. Also bleibt nur 2^p.

Aber $\mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}]$ hat nur $q^2 - 1$ von 0 verschiedene Elemente, und

$$2^p \leqslant q^2 - 1 \leqslant n - 1 = 2^p - 2$$

geht nicht. Also ist n eine Primzahl.

$\square$

References

[1] S. Müller–Stach und J. Piontkowski, *Elementare und algebraische Zahlentheorie.* Second edition. Vieweg + Teubner, Wiesbaden, 2011

[2] A. Schmidt, *Einführung in die algebraische Zahlentheorie.* Springer, Berlin, 2007

Email address: `gabriede@student.ethz.ch`