Ein Bilderrätsel aus Hurwitz' Nachlass

Nicola Oswald

Das hier gezeigte Bild findet sich ohne weiteren Kommentar in handschriftlichen Vorlesungsnotizen¹ aus dem Sommersemester 1891 zur „Elementaren Zahlentheorie“ von Adolf Hurwitz. Was illustriert dieses Bild?

Das Bild besteht aus insgesamt 88 in vier Farben koloreierten Quadraten. Aufgrund des beistehenden Schriftzu-

ges $p = 89$ denkt man bei diesen Quadraten vielleicht an die $p - 1$ primen Restklassen modulo p , reihenweise mit den kleinsten nicht-negativen Vertretern angeordnet, so dass also die Reste $1, 2, \dots, 9$ die erste Zeile von links nach rechts füllen, dann folgen die Reste $10, 11, 12, \dots, 19$ in der nächsten Reihe bis schließlich $80, 81, 82, \dots, 88$ in der

letzten Reihe. Vielleicht fällt dann eine Symmetrie in der Farbverteilung auf: Die Quadrate zu den Resten $a \bmod 89$ und $89 - a \bmod 89$ sind in derselben Farbe koloriert. Hier könnte man sich an das symmetrische Auftreten der quadratischen Reste in der primen Restklassengruppe modulo p erinnern. Und tatsächlich verifiziert man dann (mit oder ohne Computer), dass die primen Restklassen zu den Farben „rot“ und „grün“ zusammengefasst genau die 44 quadratischen Reste bilden und entsprechend die Farben „gelb“ und „blau“ für die ebenfalls 44 Nichtreste modulo 89 stehen. Damit ist schon einmal eine erste Einteilung gelungen.

Welche Bedeutung haben aber die „rot“ eingefärbten Reste gegenüber den „grünen“?

An dieser Stelle könnte man die Idee haben, mit höheren Potenzresten zu experimentieren. Und in der Tat stellt sich so heraus, dass die „rot“ eingefärbten Reste sogar bi-quadratische Reste modulo 89 sind (was sich relativ leicht über eine Zerlegung der vierten Potenz in das Quadrat eines Quadrates verifizieren lässt).

Es verbleibt nunmehr die Frage, was die „gelb“ eingefärbten Nichtreste von den „blauen“ abgrenzt?

Spätestens an dieser Stelle sollte man vor Augen haben, dass jede der vier Farben gleich oft vertreten ist, nämlich $22 = \frac{1}{4}(89 - 1)$ mal. In Erinnerung an eine einführende Vorlesung zur Zahlentheorie könnte man nun die Zyklizität der primen Restklassengruppe modulo einer Primzahl ins Spiel bringen. Nach einem Satz von Gauß existiert eine (tatsächlich sogar recht viele) sogenannte Primitivwurzel, deren Potenzen die gesamte multiplikative Gruppe erzeugt. Nennen wir diese Restklasse g (im Beispiel $p = 89$ etwa $g = 3$), so liefern die Potenzen g^j für $j = 1, 2, \dots, 88$ sämtliche primen Restklassen modulo 89. Hierbei lässt sich der Exponent mittels Division mit Rest als $j = 4\ell + r$ darstellen, wobei $r \in \{0, 1, 2, 3\}$. Färben wir nun die primen Restklassen $g^j = g^{4\ell+r}$ dem Rest des Exponenten entsprechend ein, ergeben sich vier disjunkte (wegen $88 = 4 \cdot 22$) gleichmächtige Teilmengen $\mathcal{M}_r$, welche genau die vier verschieden gefärbten Mengen von Resten liefern: So enthält $\mathcal{M}_4$ die „rot“ kolorierten Restklassen, die Elemente von $\mathcal{M}_3$ sind „blau“ eingefärbt, $\mathcal{M}_2$ mit den Quadraten in

„grün“ und schließlich $\mathcal{M}_1$ in „gelb“ (inkl. der Primitivwurzel $g^1 = 3$). Die Menge der Biquadrate ist dann wegen $g^{4\ell} = (g^\ell)^4$ gegeben durch $\mathcal{B} := \mathcal{M}_4$ und die Menge der Quadrate (ganz ähnlich) durch $\mathcal{Q} := \mathcal{M}_4 \cup \mathcal{M}_2$; diese Mengen $\mathcal{B}$ und $\mathcal{Q}$ bilden Untergruppen in der primen Restklassengruppe. Die weiteren Mengen $\mathcal{M}_1$ und $\mathcal{M}_3$ entstehen als Rechtsnebenklassen von $\mathcal{M}_4$, denn ganz allgemein gilt $\mathcal{M}_r \cdot \mathcal{M}_s = \mathcal{M}_t$, wobei t der kleinste positive Rest von $rs \bmod 4$ ist. Dabei besteht ein Isomorphismus $g^{4\ell+r} \mapsto r$ von der primen Restklassengruppe modulo $p = 89$ in die additive (zyklische) Gruppe der Reste $r \bmod 4$, wobei also letztlich die Farben genau die vier Elemente repräsentieren.

Das Hurwitzsche Bilderrätsel liefert also eine genaue Beschreibung der multiplikativen Struktur der primen Restklassengruppe modulo $p = 89$.

Wir illustrieren die obigen Erläuterungen noch an einem kleinen Beispiel, welches man ohne Aufwand per Hand rechnen kann. Sei hierzu $p = 13$. In diesem Fall ist $g = 2$ eine Primitivwurzel, denn

$$\begin{aligned} 2^1 &= 2, & 2^2 &= 4, & 2^3 &= 8, & 2^4 &\equiv 3, & 2^5 &\equiv 6, & 2^6 &\equiv 12, & 2^7 &\equiv 11, \\ 2^8 &\equiv 9, & 2^9 &\equiv 5, & 2^{10} &\equiv 10, & 2^{11} &\equiv 7, & 2^{12} &\equiv 1 \pmod{13}. \end{aligned}$$

Hier ergibt sich also die Einteilung

$$\begin{aligned} \mathcal{M}_4 &= \{3, 9, 1\}, & \mathcal{M}_3 &= \{8, 11, 7\}, \\ \mathcal{M}_2 &= \{4, 12, 10\}, & \mathcal{M}_1 &= \{2, 6, 5\} \end{aligned}$$

und beispielsweise gilt $2 \cdot \{3, 9, 1\} = \{2, 6, 5\}$, also

$$\mathcal{M}_1 \cdot \mathcal{M}_4 = \mathcal{M}_1.$$

Selbstverständlich kann man das Ganze auch mit Primzahlen $p \equiv 3 \bmod 4$ realisieren, bloß sind dann nicht alle Farben gleichmächtig vertreten.

Anmerkung

1. Der handschriftliche Nachlass wird im Hochschularchiv der ETH Zürich, ETH-Bibliothek, aufbewahrt. Das lose Blatt befindet sich in den Vorlesungsnotizen mit der Signatur Hs 582:55.

*Dr. Nicola Oswald, Leibniz Universität Hannover,
Institut für Didaktik der Mathematik und Physik,
AG Didaktik der Mathematik, Welfengarten 1, 30167 Hannover
oswald@idmp.uni-hannover.de*

Nach ihrem Studium der Mathematik und Informatik in Würzburg und Caen (Frankreich), promovierte Nicola Oswald 2014 mit einer zahlentheoretischen Dissertation an der Julius-Maximilians-Universität Würzburg. Anschließend führte sie ihr Habilitationsprojekt an die Bergische Universität Wuppertal, wo Nicola Oswald in der Arbeitsgruppe für Didaktik und Geschichte der Mathematik an der Universität Wuppertal forschte und lehrte. Nach einem Aufenthalt als Gastwissenschaftlerin an der Eidgenössischen Technischen Hochschule Zürich, war sie als Vertretungsprofessorin in Wuppertal tätig. Aktuell ist Nicola Oswald Gastprofessorin für Gender und Diversität in der Mathematik an der Leibniz Universität Hannover.