Darstellungen von Restklassen (mod n) als Summen von zwei Quadraten

Von OTT-HEINRICH KELLER in Halle

Es sei n eine natürliche Zahl. Wir fragen nach den eigentlichen Darstellungen der zu n primen Restklassen $s \pmod n$ durch Summen zweier Quadrate $s \equiv x^2 + y^2 \pmod n$. Es sei also $(x, y, n) = 1$; $(s, n) = 1$. Falls $4|n$, muß $s \equiv 1 \pmod 4$ sein.

Jede solche Darstellung notieren wir mit dem Zahlenpaar (x, y) und beachten dabei Reihenfolge und Vorzeichen. (Jeder Darstellung, für die $x \not\equiv \pm y; x \not\equiv -x$; $y \not\equiv -y \pmod n$ seien also 8 Zahlenpaare $(\pm x, \pm y)$ und $(\pm y, \pm x)$ zugeordnet.)

Es ist zu zeigen:

1. Jede Zahl s mit $(s, n) = 1$, und, falls $4|n$, mit $s \equiv 1 \pmod 4$ ist darstellbar.
2. Die Anzahl der Darstellungen von $s \pmod n$ ist nur von n, nicht aber von s abhängig; sie sei $\varrho(n)$.
3. $\varrho(n)$ ist eine distributive zahlentheoretische Funktion von n.
4. Es ist $\varrho(1) = 1$, $\varrho(2) = 2$, $\varrho(2^r) = 2^{r+1}\ (r \geqq 2)$,

$$\varrho(p^r) = p^{r-1}\left(p - \left(\frac{-1}{p}\right)\right)$$

$\left(p \text{ ungerade Primzahl}, \left(\frac{-1}{p}\right) \text{ Legendresches Symbol}\right)$.

Zu 2. Wir ordnen jedem in Betracht kommenden Restklassenpaar (x, y) die äquiforme Matrix $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ zu.[1]) Ihre Determinante ist $x^2 + y^2$. Diese Matrizen bilden eine abelsche Gruppe $\mathfrak{M}$; sie wird durch die Determinanten homomorph auf die Gruppe $\mathfrak{R}$ der darstellbaren Restklassen abgebildet. Der Kern dieses Homomorphismus ist die (mod n) orthogonale Gruppe $\mathfrak{O}$ der Darstellungen der Restklasse 1 (mod n). Die Ordnung von $\mathfrak{O}$ sei $\varrho(n)$. Die Darstellungen der Restklassen s erscheinen als Nebengruppen nach $\mathfrak{O}$; die Anzahl ihrer Elemente ist von s unabhängig. Alle Restklassen, die überhaupt darstellbar, sind also gleich oft darstellbar.

Zu 3. Ist $n = n_1 \cdot n_2$ mit $(n_1, n_2) = 1$, so entsprechen sich die Restklassenpaare $(x, y) \pmod n$ und die Paare von Restklassenpaaren $(x_1, y_1) \pmod{n_1}$ und $(x_2, y_2) \pmod{n_2}$ eindeutig. Es ist also $\varrho(n) = \varrho(n_1) \cdot \varrho(n_2)$.

Zu 1. Wir müssen noch zeigen, daß sich jede der erwähnten Restklassen überhaupt darstellen läßt. Nach 3.) genügt es, sich auf den Fall $n = p^r$ (p = Primzahl) zu beschränken.

---

[1]) Ist -1 quadratischer Nichtrest mod n, so sind diese Matrizen den komplexen Restklassen $x + iy$ eineindeutig zugeordnet.

a) Es sei $p=2$. Für $r=1$ und 2 ist nichts zu beweisen. Für $r\geqq 3$ sind alle Zahlen s, für die $s\equiv 1 \pmod 8$ ist, quadratische Reste $s\equiv q^2(2^r)$ und gestatten die Darstellung $s\equiv q^2+0^2 \pmod{2^r}$. Die anderen Restklassen haben die Form $s\equiv q^2+4 \pmod{2^r}$, und dies ist ebenfalls eine Darstellung.

b) p sei ungerade. Ist dann $s \pmod p$ darstellbar, so auch $\pmod{p^r}$. Ist $\left(\frac{s}{p}\right)=1$, so ist $s\equiv q^2 \pmod p$ und $s\equiv q^2+0^2 \pmod{p^r}$ ist eine Darstellung.

In der Reihe der Restklassen $1, 2, \ldots, p-1$ muß mindestens einmal auf einen Rest ein Nichtrest folgen. Es gibt also einen solchen quadratischen Rest q_1^2, daß $N_1=q_1^2+1$ ein Nichtrest $\pmod p$ ist. N_1 gestattet also eine Darstellung. Jeder andere Nichtrest N entsteht aus N_1 durch Multiplikation mit einem quadratischen Rest q^2 und gestattet die Darstellung $N\equiv(qq_1)^2+q^2 \pmod p$.

Zu 4. Es ist noch $\varrho(p^r)$ zu berechnen.

a) $p=2$. Es ist $\varrho(2)=2$. Für $r\geqq 2$ ist für die Hälfte der in Betracht kommenden Restklassenpaare x gerade und y ungerade. Da es 2^{r-1} gerade und ebensoviele ungerade Restklassen $\pmod{2^r}$ gibt, gibt es 2^{2r-2} Restklassenpaare, in denen die erste ungerade, die zweite gerade ist, also im ganzen 2^{2r-1} Paare. Da es nun 2^{r-2} solche Restklassen s gibt, für die $s\equiv 1 \pmod 4$, entfallen auf jede von ihnen 2^{r+1} Darstellungen.

b) p ungerade. Es gibt p^{2r} Zahlenpaare $\pmod{p^r}$; davon sind p^{2r-2} uneigentlich, d. h. $p|x$ und $p|y$. Es bleiben also $p^{2r-2}(p^2-1)$ eigentliche Zahlenpaare.

bα) Ist $p\equiv 3 \pmod 4$, so stellen sie alle eine zu p prime Restklasse dar. Deren Anzahl ist $\varphi(p^r) = p^{r-1}(p-1)$. Da sie sich gleich oft darstellen lassen, entfallen auf jede von ihnen $\varrho(p^r) = p^{r-1}(p+1)$ Darstellungen.

bβ) Ist $p\equiv 1 \pmod 4$, so ist $-x^2$ quadratischer Rest, und es gibt zu jedem der $p^{r-1}(p-1)$ möglichen Werte von x noch $2p^{r-1}$ solche Werte von y, daß $x^2+y^2 \equiv 0 \pmod p$. Für die zu p teilerfremden Restklassen bleiben also nur $p^{2r+2}(p^2-1)-2p^{2r-2}(p-1) = p^{2r-2}(p-1)^2$ Restklassenpaare zur Verfügung. Jede der $p^{r+1}(p-1)$ zu p teilerfremden Restklassen gestattet also noch $\varrho(p^r) = p^{r-1}(p-1)$ Darstellungen.

B e m e r k u n g. Es sei $\mathfrak{U}$ die Untergruppe

$$\mathfrak{U}=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix}\right\}.$$

Die Nebengruppen von $\mathfrak{M}/\mathfrak{U}$ sind dann

$$\left\{\pm\begin{pmatrix}x&y\\-y&x\end{pmatrix},\ \pm\begin{pmatrix}y&-x\\x&y\end{pmatrix}\right\}.$$

Ihre Elemente unterscheiden sich nur unwesentlich. $\mathfrak{M}/\mathfrak{U}$ wird ebenfalls auf $\mathfrak{R}$ homomorph abgebildet. Die Anzahl der dann noch verschiedenen Darstellungen irgend einer Restklasse ist dann $\frac{\varrho(n)}{4}$. Dabei sind die Paare $(0, x)$, $(x, \pm x)$ und, falls $2|n$, $\left(\frac{n}{2}, x\right)$ je einfach, die Paare aber (x, y) mit $2x, 2y, x\pm y \not\equiv 0 \pmod n$ je doppelt, nämlich einmal als (x, y) und einmal als (y, x) zu zählen.

(Eingegangen am 29. Januar 1964)