Die quadratischen Reste zusammengesetzter Moduln.

Von GUSTAV RADOS in Budapest.

Die quadratischen Reste in Bezug auf den Primzahl-Modul p sind unmittelbar durch die Zahlen

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

gegeben und ihre Anzahl stimmt bekanntlich mit derjenigen der quadratischen Nichtreste überein.

Ist n ein zusammengesetzter Modul und seine Zerlegung in Primfaktoren

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \qquad (\alpha \geqq 0);$$

können auch für diesen Modul die quadratischen Reste vermittels einer Formel berechnet werden? Wie gross ist ihre Anzahl? Für welche zusammengesetzten Moduln stimmt wiederum die Anzahl der quadratischen Reste und Nichtreste überein?

Diese Fragen sollen im Nachfolgenden beantwortet werden. Sie werden durch die folgenden Sätze erledigt:

a) *Die quadratischen Reste sowie auch die Nichtreste eines zusammengesetzten Moduls können stets durch je eine Formel berechnet werden.*

b) *Die Anzahl dieser Reste ist*

$$M = \frac{\varphi(n)}{\psi(n)},$$

die der Nichtreste

$$N = \varphi(n)\left(1 - \frac{1}{\psi(n)}\right)$$

wobei $\varphi(n)$, die bekannte Eulerische Funktion, die Anzahl der

Glieder des reduzierten Restesystems für den Modul n —, $\psi(n)$ die Anzahl der verschiedenen Wurzeln einer auflösbaren Kongruenz

$$x^2 \equiv D \pmod{n}$$

bedeutet. (Bekanntlich ist $\psi(n)$ von der Wahl des quadratischen Restes D unabhängig.)

c) *Die Anzahl der quadratischen Reste und Nichtreste von n stimmt dann und nur dann überein, wenn n eine den Typen*

$$n = p^\alpha, 2p^\alpha, 4$$

angehörende zusammengesetzte Zahl ist, wobei p als ungerade Primzahl angenommen wird.

Der Beweis der Sätze *a)* und *b)* soll für die — alle Möglichkeiten erschöpfenden Fälle einzeln geliefert werden:

I. Fall: $\alpha = 0, 1$; hier ist $\psi(n) = 2^r$

II. Fall: $\alpha = 2$; hier ist $\psi(n) = 2^{r+1}$

III. Fall: $\alpha > 2$; alsdann ist $\psi(n) = 2^{r+2}$.

I. In diesem Falle ist n ungerade oder durch 2 teilbar und die notwendigen und hinreichenden Bedingungen für die Lösbarkeit der Kongruenz

$$x^2 \equiv D \pmod{n}$$

sind die folgenden:

$$\left(\frac{D}{p_i}\right) = 1. \qquad (F_1)$$
$$(i = 1, 2, \ldots, r)$$

Diese Bedingungen sind also auch notwendig und hinreichend dafür, dass D quadratischer Rest von n sei.

Die quadratischen Reste von p_i sind die Zahlen

$$1^2, 2^2, \ldots, k_i^2, \ldots, \left(\frac{p_i - 1}{2}\right)^2,$$

sodass die den Bedingungen (F_1) genügenden Zahlen D die in den Wertevorräten der r linearen Formen

$$k_i^2 + p_i u_i \quad (i = 1, 2, \ldots r;\ u_i = 0, \pm 1, \pm 2, \ldots)$$

gemeinschaftlich vorkommenden Zahlen sind.

Die lineare Form $k_i^2 + p_i u_i$ liefert in Bezug auf den Modul $p_i^{\alpha_i}$ die $p_i^{\alpha_i - 1}$ nachfolgenden inkongruenten Zahlen

$$k_i^2, k_i^2 + 1 \,.\, p_i, \ldots, k_i^2 + u_i p_i, \ldots, k_i^2 + (p_i^{\alpha_i - 1} - 1)\, p_i.$$

Es muss demnach D im Sinne der Bedingungen (F_1) eines der folgenden Systeme von linearen Kongruenzen befriedigen:

$$\left.\begin{aligned} D &\equiv k_1^2 + p_1 u_1 \pmod{p_1^{\alpha_1}} \\ D &\equiv k_2^2 + p_2 u_2 \pmod{p_2^{\alpha_2}} \\ &\cdots\cdots\cdots\cdots \\ D &\equiv k_r^2 + p_r u_r \pmod{p_r^{\alpha_r}} \end{aligned}\right\} \qquad (C_1)$$

$$\left(k_i = 1, 2, \ldots, \frac{p_i - 1}{2};\ u_i = 0, 1, \ldots, p_i^{\alpha_i - 1} - 1;\ i = 1, 2, \ldots, r\right).$$

Die sämmtlichen quadratischen Reste D von n werden daher durch die Formel

$$D' \equiv \sum_{i=1}^{r} \left(\frac{n}{p_i^{\alpha_i}}\right)^{\varphi(p_i^{\alpha_i})} (k_i^2 + p_i u_i) \pmod{n} \qquad (K_1)$$

$$\left(k_i = 1, 2, \ldots, \frac{p_i - 1}{2};\ u_i = 0, 1, \ldots, p_i^{\alpha_i - 1} - 1;\ i = 1, 2, \ldots, r\right)$$

geliefert. In ähnlicher Weise kann auch eine Formel für die quadratischen Nichtreste hergeleitet werden worauf es sich erübrigt des Näheren einzugehen.

Aus der Formel (K_1) geht zugleich hervor, dass die Anzahl M der zum Modul n gehörigen quadratischen Reste sich folgendermassen ergibt:

$$M = \prod_{i=1}^{r} \frac{p_i - 1}{2} \cdot \prod_{i=1}^{r} p_i^{\alpha_i - 1} = \prod_{i=1}^{r} \frac{p_i^{\alpha_i - 1}(p_i - 1)}{2} =$$

$$= \frac{\varphi(p_1^{\alpha_1})}{2} \cdot \frac{\varphi(p_2^{\alpha_2})}{2} \cdots \frac{\varphi(p_r^{\alpha_r})}{2} = \frac{\varphi(n)}{2^r}$$

und da im Falle I

$$\psi(n) = 2^r$$

ist, so folgt schliesslich

$$M = \frac{\varphi(n)}{\psi(n)},$$

womit für den Fall I der Beweis der Sätze *a)* und *b)* erbracht ist.

II. In diesem Falle ist $\alpha = 2$ und daher

$$n = 4 p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}.$$

Den Bedingungen (F_1) und dem System (K_1) ist für diesen Fall noch die weitere Bedingung resp. Kongruenz

$$D \equiv 1 \pmod 4$$

hinzuzufügen. Die quadratischen Reste von n ergeben sich jetzt aus der Formel

$$D \equiv \left(\frac{n}{4}\right)^2 + \sum_{l=1}^{r} \left(\frac{n}{p_l^{\alpha_l}}\right)^{\varphi(p_l^{\alpha_l})} (k_l^2 + p_l u_l) \pmod{n}$$

$$\left(k_l = 1, 2, \ldots, \frac{p_l - 1}{2};\ u_l = 0, 1, \ldots, p_l^{\alpha_l - 1} - 1;\ i = 1, 2, \ldots, r\right).$$

Aus dieser Formel geht wiederum die Anzahl M der quadratischen Reste von n folgendermassen hervor:

$$M = \prod_{l=1}^{r} \frac{p_l^{\alpha_l - 1}(p_l - 1)}{2} = \frac{\varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \ldots \varphi(p_r^{\alpha_r})}{2^r} =$$

$$= \frac{\varphi(4)\varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \ldots \varphi(p_r^{\alpha_r}}{2^{r+1}} = \frac{\varphi(n)}{2^{r+1}}$$

und da für den Fall II

$$\psi(n) = 2^{r+1}$$

ist, hat man wieder

$$M = \frac{\varphi(n)}{\psi(n)},$$

womit die Sätze *a)* und *b)* auch für den Fall II bewiesen sind.

III. In diesem Falle muss den Bedingungen (F_1) noch die weitere

$$D \equiv 1 \pmod{8}$$

hinzugefügt werden. Es muss also D dem Wertevorrat der linearen Form

$$1 + 8u_0$$

entnommen werden, was für den Modul 2^α die Werte

$$1, 1 + 8.1,\ 1 + 8.2, \ldots 1 + 8u_0, \ldots 1 + (2^{\alpha-3} - 1)\,8$$

liefert. Somit ist dem System (K_1) die weitere Kongruenz

$$D \equiv 1 + 8u_0$$

hinzuzufügen. Für D ergibt sich dann die Formel

$$D \equiv \left(\frac{n}{2^\alpha}\right)^{\varphi(2^\alpha)} (1 + 8u_0) + \sum_{l=1}^{r} \left(\frac{n}{p_l^{\alpha_l}}\right)^{\varphi(p_l^{\alpha_l})} (k_l^2 + p_l u_l) \pmod{n}$$

$$\left(k_l = 1, 2, \ldots, \frac{p_l - 1}{2};\ u_0 = 0, 1, \ldots, 2^{\alpha-3} - 1;\ u_l = 0, 1, \ldots, p_l^{\alpha_l - 1} - 1;\right.$$

$$\left. i = 1, 2, \ldots, r\right.$$

und hieraus ergibt sich für die Anzahl der quadratischen Reste für den Modul n:

$$M = 2^{\alpha-3} \prod_{r=1}^{r} \frac{p_l^{\alpha_l - 1}(p_l - 1)}{2} = 2^{\alpha-3} \frac{\varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \ldots \varphi(p_r^{\alpha_r})}{2^r} =$$

$$= \frac{\varphi(2^\alpha)\,\varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \ldots \varphi(p_r^{\alpha_r})}{2^{r+2}}.$$

Da im Falle III

$$\psi(n) = 2^{r+1}$$

ist, hat man wieder

$$M = \frac{\varphi(n)}{\psi(n)},$$

womit auch der Fall III erledigt ist.

Wir übergehen nun zum Nachweis des Satzes *c)*. Da die Anzahl der zum zusammengesetzten Modul n gehörigen quadratischen Reste

$$M = \frac{\varphi(n)}{\psi(n)}$$

ist, so wird die Anzahl N der im reduzierten System von Resten (mod. n) enthaltenen Nichtresten

$$N = \varphi(n) - \frac{\varphi(n)}{\psi(n)} = \varphi(n)\left(1 - \frac{1}{\psi(n)}\right)$$

im Allgemeinen von M verschieden sein. Die beiden können dann und nur dann übereinstimmen, wenn

$$\psi(n) = 2$$

ist.

Im Falle I ist $\psi(n) = 2^r$, somit kann $M = N$ nur dann statt haben, wenn $r = 1$ ist, daher n vom Typus $n = p^\alpha$, $2p^\alpha$ ist.

Im Falle II ist $\psi(n) = 2^{r+1}$, somit kann M nur dann mit N gleich sein, falls $r = 0$ und daher $n = 4$ ist.

Im Falle III ist $\psi(n) = 2^{r+2}$, also stets gröszer als 2 und somit M stets verschieden von N.

Da durch die Fälle I, II, III sämmtliche Möglichkeiten erschöpft werden, *kann man zusammenfassend erklären, dass* $n = p^\alpha$, $2p^\alpha$, 4 *sämmtliche Typen von zusammengesetzten Moduln liefern, für welche die Anzahl der Reste und Nichtreste die gleiche ist.*

Es sind dies dieselben Typen von zusammengesetzten Moduln für die die Verallgemeinerung des Wilsonschen Satzes und die Existenz von primitiven Wurzeln nachgewiesen werden kann.

Schliesslich möge noch erwähnt werden, dass die Anzahl der im reduzierten System von Resten enthaltenen quadratischen

Reste auch auf einfacherer Weise hergeleitet werden kann, falls auf die Darstellung dieser quadratischen Reste durch eine Formel verzichtet wird.

Es seien die sämmtlichen quadratischen Reste des reduzierten Systems von Resten (mod. n)

$$D_1, D_2, \ldots, D_M$$

alsdann sind

$$x^2 \equiv D_i \pmod{n} \qquad (i = 1, 2, \ldots, M) \tag{B}$$

die sämmtlichen auflösbaren binomischen quadratischen Kongruenzen. Jede dieser Kongruenzen hat dieselbe Anzahl von Wurzeln, da diese Anzahl $\psi(n)$ nur von n und nicht von D_i abhängt. Die Wurzeln aller Kongruenzen (B) liefern somit $M\psi(n)$ Zahlen, die alle verschieden und gegen n teilerfremd sind, da die D_i es auch sind.

Es seien diese Wurzeln

$$\omega_1, \omega_2, \ldots, \omega_{M\varphi(n)} \tag{S_1}$$

so sind dieselben alle verschieden und im reduzierten System von Resten (mod. n)

$$r_1, r_2, \ldots, r_{\varphi(n)} \tag{S_2}$$

enthalten.

Es kann aber auch gezeigt werden, dass jede Zahl von (S_2) auch in (S_1) enthalten ist, da ja r_i gewiss eine Wurzel von

$$x^2 \equiv r_i^2 \pmod{n}$$

ist. Es ist somit

$$M\psi(n) = \varphi(n)$$

und daher wieder

$$M = \frac{\varphi(n)}{\psi(n)}.$$

Budapest, am 1. Juni 1926.

(*Eingegangen am 4. Juni 1926*).