Eine Verallgemeinerung des Satzes von WILSON

A. Stoimenow

4. März 1996

Aus der Zahlentheorie ist bekannt folgender Satz :

Satz von WILSON : Ist p eine Primzahl, so gilt :

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv -1(p)$$

Es gibt eine Möglichkeit, diesen Sachverhalt für beliebige natürliche Zahlen zu verallgemeinern, und zwar auf folgender Weise :

Man betrachte für $n \in \mathbb{N}$

$$M_n := \{m \in \mathbb{N} : m < n, \quad (m,n) = 1\}$$

Bekanntlich ist M_n mit der Multiplikation $\bmod n$ eine Gruppe. Wir betrachten weiterhin

$$\prod_{m \in M_n} m \bmod n =: r(n)$$

Der Satz von WILSON besagt, daß, falls n eine Primzahl ist, diese Zahl -1 wird. Nun gilt nicht für alle $n \in \mathbb{N}$ diese Aussage, aber es gilt immer $r(n) = -1$ oder $r(n) = 1$. Das einzusehen, ist nicht schwierig, viel interessanter ist jedoch die Frage, für welche $n \quad -1$ und für welche 1 herauskommt. Sei $m \in M_n$. Falls $m^2 \not\equiv 1(n)$, dann ex. in M_n ein eind. von m verschiedenes Element m', das zu m invers ist.Bezeichne ich mit

$$I_n := \left\{m \in M_n : m^2 \not\equiv 1(n)\right\},$$

so kann ich $M_n \setminus I_n$ in Zweiermengen $\{m, m'\}$ disjunkt zerlegen mit $mm' \equiv 1(n)$ und $m \neq m'$. Daraus folgt sofort

$$\prod_{m \in M_n \setminus I_n} m \mod n = 1,$$

also gilt

$$r(n) = \prod_{m \in I_n} m \mod n \tag{1}$$

Ferner ist klar, daß $m \in I_n \Longrightarrow n - m \in I_n$. Dabei gilt für $n > 2$, daß $m \neq n - m$, da $\frac{n}{2} \notin I_n$. Ich kann also I_n disjunkt zerlegen in Zweiermengen $\{m, m''\}$ mit $m + m'' = n$, und es gilt $mm'' \equiv -1 \mod m$. Daraus und aus (1) folgt, daß $r(n)$ eine Potenz von -1 mit dem Exponenten ist, der die Anzahl der Mengen in der obigen Zerlegung ist.

$$r(n) = (-1)^{\left|\left\{\left\{m_k, m_k''\right\}\right\}_{i=1}^{l}\right|} \qquad \text{mit} \quad m_k + m_k'' = n$$
$$m_{k'}^2 \equiv 1(n)$$
$$m_k \neq m_j \quad k \neq j$$
$$m_k \neq m_j' \quad k \neq j$$
$$\bigcup_{i=1}^{l} \{m_k, m_k'\} = I_n$$

Für unsere weiteren Betrachtungen ist offensichtlich wichtig dir Kardinalität von I_n

$$\pi(n) := |I_n|$$

Klar ist, daß für $n > 2$ gilt $r(n) = (-1)^{\pi(n)/2}$.

Der Fall $n = 2$ ist nicht sonderlich interessant. Es gilt $\pi(2) = 1$ und gleichzeitig $r(2) = \pm 1$.

Im Fall $n = 1$ treffen wir die wichtige Vereinbarung, daß $\pi(1) = 1$ ist. Warum sich das als sinnvoll erweist, werden wir im Anschluss sehen.

Versuchen wir nun, $\pi(n)$ für bel. n zu berechnen.

Dazu betrachten wir zunächst einige Spezialfälle.

Sei $n = 2^k, k > 1$

Dann gilt $m \in I_n \iff m^2 \equiv 1(2^k) \iff 2^k|(m-1)(m+1)$. Es muß also zunächst m ungerade sein. Dann teilt 2 beide Faktoren. Da 4 nicht gleichzeitig beide teilen kann, folgt

$$2^{k-1}|m-1 \quad \text{oder} \quad 2^{k-1}|m+1$$

Daraus ergeben sich für m nur 4 Möglichkeiten : $1, 2^{k-1}-1, 2^{k-1}+1, 2^k-1$. Für $k = 2$, d.h. $n = 4$ fallen jewils die ersten und die letzten beiden Zahlen zusammen, für $k > 2$ sind alle 4 Zahlen voneinander verschieden. Nehmen wir noch die Spezialfälle n=1 und n=2 hinzu, sokönnen wir zusammenfassend schreiben

$$\pi(2^k) = 2^{l(k)} \qquad l(k) = \begin{cases} 0 & : \quad k = 0,1 \\ 1 & : \quad k = 2 \\ 2 & : \quad k > 2 \end{cases}$$

oder

$$\pi(2^k) = 2^{sign(k-2)+1}. \tag{2}$$

Sei nun $n = p^k, k > 0$, wobei p eine ungerade Primzahl darstellt. Dann gilt $m \in I_n \iff p^k|(m-1)(m+1)$. Da sicherlich p nicht gleichzeitig beide Faktoren teilen kann, folgt

$$p^k|m-1 \quad \text{oder} \quad p^k|m+1,$$

d.h. $I_n = \{1, n-1\}$, also $\pi(p^k) = 2$. Nehmen wir den Fall $k = 0$,d.h. $n = 1$ dazu, so haben wir

$$\pi(p^k) = p^{sign(k)} \tag{3}$$

Nun seien $n, s > 1$ teilerfremd

Beh.:

$$\pi(n \cdot s) = \pi(n) \cdot \pi(s) \tag{4}$$

Hieraus sieht man, daß die oben getroffene Konvention den Sachverhalt für $n, s \geq 1$ verallgemeinert und deshalb gerechtfertigt ist.

Betrachten wir nun $m \in I_{n \cdot s}$

$$\begin{aligned} m \in I_{n \cdot s} \iff m^2 \equiv 1(n \cdot s) &\iff m^2 \equiv 1(n) \wedge m^2 \equiv 1(s) \\ &\iff m \bmod n \in I_n \wedge m \bmod s \in I_s \end{aligned}$$

Da jetzt $(n, s) = 1$ gilt

$$\forall n' < n \quad \forall s' < s \quad \exists! m' < n \cdot s \quad : \quad m \equiv n' \bmod n \quad \wedge \quad m \equiv s' \bmod s$$

Daraus folgt die Beziehung (4)

(2),(3) und (4) erlauben es nun, $\pi(n)$ für bel. $n \in \mathbb{N}$ aufzuschreiben.

Sei $n = 2^{k_1} \cdot 3^{k_2} \cdot \ldots \cdot p_l^{k_l}$ mit $p_l = max\{p : p \text{ Primzahl}, \ p \mid n\}$. Dann gilt

$$\pi(n) = 2^{sign(k_1-2)+\sum_{i=2}^{l} sign(k_i)}$$

Aus dieser Formel sieht man folgendes :

$$\pi(n) = \begin{cases} 1 & : \text{ für } n = 1, 2 \\ 2 & : \text{ für } n = 4, p^k, 2 \cdot p^k \quad p \text{ ungerade Primzahl} \\ 4 \cdot k & : \text{ sonst} \end{cases}$$

Das erlaubt uns nun, die gesuchte Klassifizierung vorzunehmen. Als zusammenfassendes Ergebnis erhält man :

Satz (Verallgemeinerung des Satzes von WILSON)

$$\prod_{\substack{m < n \\ (m,n) = 1}} m \quad \begin{cases} \equiv -1(n) & : \quad n = 4, p^k, 2 \cdot p^k \text{ mit } p > 2 \text{ Primz.} \\ \equiv 1(n) & : \quad \text{sonst} \end{cases}$$

$(n \geq 2)$ $\square$