Über ein System von Kongruenzen, welches mit dem Wilsonschen Satz zusammenhängt.

(Auszug aus dem vorstehenden Artikel.)

Kleine lateinische Buchstaben bedeuten natürliche Zahlen, p ist stets > 1; $\sigma(k, n)$ ist die k-te elementarsymmetrische Funktion der Größen $1, 2, \ldots, n$ $(1 \leqq k \leqq n)$. Im § 3 der tschechischen Originalarbeit wird gezeigt, daß sich $\sigma(k, n)$ in der Gestalt

$$\sigma(k, n) = \frac{(n+1)\, n\, \eta_{2k-2}(n)}{d_k} \tag{1}$$

schreiben läßt, wo $\eta_{2k-2}(n)$ ein Polynom in n mit ganzen, nur von k abhängigen Koeffizienten ist; auch d_k hängt nur von k ab (vgl. dort die Formeln (16), (17), (17'), (18), (20), (20*).

1. Genau dann ist p eine Primzahl, wenn

$$(p-1)! + 1 \equiv 0 \pmod p \tag{2}$$

(Wilsonscher Satz; alle folgenden Kongruenzen sind auch mod p zu verstehen.)

2. Hier sei $p > 2$; ist p Primzahl, so ist identisch

$$(x-1)(x-2)\ldots(x-(p-1)) \equiv x^{p-1} - 1, \tag{3}$$

also

$$\sigma(1, p-1) \equiv \sigma(2, p-1) \equiv \ldots \equiv \sigma(p-2, p-1) \equiv 0. \tag{4}$$

Gilt umgekehrt (4), so ist $\frac{1}{2}p(p-1) \equiv 0$, p ungerade und die Kongruenz (3) ist mit

$$x^{p-1} + (p-1)! \equiv x^{p-1} - 1 \tag{5}$$

identisch. Da (3) die Wurzel 1 hat, so folgt aus (5) mit $x = 1$ die Kongruenz (2), also ist p eine ungerade Primzahl. Unter den $p > 2$ sind also die Primzahlen durch (4) charakterisiert.

3. Zu dieser Charakterisierung ungerader Primzahlen genügt bereits folgendes System:

$$\sigma(1, p-1) \equiv 0, \quad \sigma(2l, p-1) \equiv 0 \quad (2l < p-1). \tag{6}$$

Denn die erste Kongruenz charakterisiert ungerade Zahlen p; ist aber p ungerade, so ist

$$\begin{aligned}\sigma(2k-1, p-1) &= \Sigma\, \alpha_1 \ldots \alpha_{2k-1} = \Sigma\, (p-\alpha_1)\ldots(p-\alpha_{2k-1}) \\ &\equiv -\sigma(2k-1, p-1), \quad \text{also} \quad 2\sigma(2k-1, p-1) \equiv 0,\end{aligned}$$

$\sigma(2k-1, p-1) \equiv 0$; daraus und aus (6) folgt also (4).

4. Sind m und $k_1, \ldots, k_m$ gegeben, so genügt weder das System

$$\sigma(k_\nu, p-1) \equiv 0 \quad (\nu = 1, \ldots, m) \tag{7}$$

noch das System

$$\sigma(p - k_\nu, p - 1) \equiv 0 \qquad (\nu = 1, \ldots, m) \tag{8}$$

zur Charakterisierung aller hinreichend großen Primzahlen p, d. h. es gibt beliebig große zusammengesetzte p, welche dem System (7) bzw. (8) genügen (für das System (8) kommen nach dem Wilsonschen Satz nur $k_\nu > 1$ in Betracht). Beweis: benutzt man (1), so sieht man, daß die zusammengesetzte Zahl $p = (1 + d_{k_1} \ldots d_{k_m})^r$ $(r > 1)$ den Kongruenzen (7) genügt. Ist zweitens $p = 2^r$ $(r > 1)$, so beachte man, daß die Reihe $1, 2, \ldots, 2^r - 1$ genau $2^{r-1} - 1$ gerade Glieder enthält; also ist $\sigma(p - k_\nu, p - 1)$ durch $2^{2^r - 1 - (k_\nu - 1)}$ teilbar; für hinreichend großes r ist aber $2^r - 1 - (k_\nu - 1) \geqq r$; daher gelten die Kongruenzen (8) für $p = 2^r$, wenn r hinreichend groß ist.