# Elementare Bemerkung über identische Kongruenzen.

Von MICHAEL BAUER in Budapest.

In der Arbeit „Zur Theorie der identischen Kongruenzen mit Idealmoduln"[1]) berechnet Herr ZÁNYI das Produkt

$$\prod_{\tau_\alpha} f(x+(\tau_\alpha \pi)^n) \qquad (\text{mod. } \mathfrak{p}^{\alpha+1}),$$

wo $f(x)$ ein Polynom bedeutet, dessen Koeffizienten wieder Polynome von neuen Unbestimmten mit ganzen Koeffizienten aus einem algebraischen Zahlkörper $\mathfrak{K}$ sein können. Die Zahlen $\tau_\alpha$ durchlaufen alle Zahlklassen (mod. $\mathfrak{p}^\alpha$), $\mathfrak{p}$ ist ein Primideal und $\pi$ eine genau durch $\mathfrak{p}$ teilbare ganze Zahl. Der Verfasser bemerkt, daß für $n>1$ schärfere Resultate erzielt werden können. Tatsächlich läßt sich das Produkt

$$\prod_{\tau_\alpha} f(x+(\tau_\alpha \pi)^n) \qquad (\text{mod. } \mathfrak{p}^{\alpha+n})$$

vollständig berechnen und man bekommt sehr einfache Resultate.

I. *Wenn* $N(\mathfrak{p})>2$ *und* $\varphi(\mathfrak{p}) \nmid n$ *sind*[2]), *so gilt die Kongruenz*

$$(1) \qquad \prod_{\tau_\alpha} f(x+(\tau_\alpha \pi)^n) \equiv f(x)^{N(\mathfrak{p}^\alpha)} \qquad (\text{mod. } \mathfrak{p}^{\alpha+n}).$$

*In den Fällen* $\varphi(\mathfrak{p}) \mid n$, $N(\mathfrak{p})=p^f$, $f>1$, *oder* $\varphi(\mathfrak{p}) \mid n$, $N(\mathfrak{p})=p>2$, $\mathfrak{p}^2 \mid p$, *besteht dieselbe Kongruenz mit der Einschränkung* $\alpha>1$, *also wird*

$$(1^*) \qquad \prod_{\tau_\alpha} f(x+(\tau_\alpha \pi)^n) \equiv f(x)^{N(\mathfrak{p}^\alpha)} \qquad (\text{mod. } \mathfrak{p}^{\alpha+n}), \qquad \alpha>1.$$

[1]) *Diese Acta*, **5** (1930—1932), S. 117—131 und S. 168—171.

[2]) $N$ bedeutet die Norm, $\varphi$ ist das Eulersche Zeichen, $a \nmid b$ bedeutet, daß $a$ kein Teiler von $b$ ist, $p$ ist die natürliche Primzahl, welche durch $\mathfrak{p}$ teilbar ist, also wird $\mathfrak{p} \mid p$. Wir setzen noch $\tau_1=\tau$.

*Im Falle* $\varphi(\mathfrak{p})\,|\,n$, $N(\mathfrak{p})=p>2$, $\mathfrak{p}^2 \nmid p$, *ist*

$$(2)\qquad \prod_{\tau_\alpha} f(x+(\tau_\alpha\pi)^n) \equiv \left(f(x)f^{p-1}(x+p^n)\right)^{p^{\alpha-1}} \qquad (\text{mod. } \mathfrak{p}^{\alpha+n}).$$

II. *Wenn* $N(\mathfrak{p})=2$, $2\,|\,n$ *ausfallen, so sind die Formeln* (1*) *bzw.* (2) *gültig, je nachdem* $\mathfrak{p}^2|2$ *oder* $\mathfrak{p}^2\nmid 2$. Der Fall $N(\mathfrak{p})=2$, $n=1$ ist a. a. O. erledigt. *Wird* $n>1$, $2\nmid n$, *so ist im Falle* $\mathfrak{p}^2\nmid 2$ *die Formel* (1*) *gültig, während im Falle* $\mathfrak{p}^2|2$

$$(1^{**})\qquad \prod_{\tau_\alpha} f(x+(\tau_\alpha\pi)^n) \equiv f(x)^{N(\mathfrak{p}^\alpha)} \qquad (\text{mod. } \mathfrak{p}^{\alpha+n}),\ \alpha>2$$

*wird.*

**1.** Aus der Formel (42) der zitierten Arbeit folgt zunächst, daß für $N(\mathfrak{p})>2$, $\alpha>1$, oder $N(\mathfrak{p})=2$, $\alpha>2$, oder endlich für $N(\mathfrak{p})=2$, $\alpha>1$, $2|n$

$$(3)\qquad \prod_{\tau_\alpha} f(x+(\tau_\alpha\pi)^n) \equiv \prod_{\tau_{\alpha-1}} f(x+(\tau_{\alpha-1}\pi)^n)^{N(\mathfrak{p})} \qquad (\text{mod. } \mathfrak{p}^{\alpha+n})$$

ausfällt. Nun betrachten wir die Kongruenz

$$(4)\qquad \begin{aligned} \prod_{\tau} f(x+(\tau\pi)^n) &\equiv \prod_{\tau}(f(x)+(\tau\pi)^n f'(x)) \equiv \\ &\equiv f(x)^{N(\mathfrak{p})} + \pi^n f(x)^{N(\mathfrak{p})-1} f'(x) \sum_{\tau} \tau^n \qquad (\text{mod. } \mathfrak{p}^{1+n}). \end{aligned}$$

Da (vergl. z. B. a. a. O., S. 129) im Falle $N(\mathfrak{p})>2$, $\varphi(\mathfrak{p})\nmid n$,

$$\sum \tau^n \equiv 0 \qquad (\text{mod. } \mathfrak{p})$$

wird, ist (1) richtig. Die Formel (1*) ist in den unter I. angegebenen Fällen richtig, weil für $N(\mathfrak{p})=p^f$, $f>1$, oder $N(\mathfrak{p})=p>2$, $\mathfrak{p}^2|p$, die Kongruenz

$$(5)\qquad \begin{aligned} \prod_{\tau_2} f(x+(\tau_2\pi)^n) &\equiv \left\{f(x)^{N(\mathfrak{p})} + \pi^n f(x)^{N(\mathfrak{p})-1} f'(x) \sum_{\tau} \tau^n\right\}^{N(\mathfrak{p})} \equiv \\ &\equiv f(x)^{N(\mathfrak{p}^2)} \qquad (\text{mod. } \mathfrak{p}^{2+n}) \end{aligned}$$

gilt. Dieselbe besteht auch für $N(\mathfrak{p})=2$, $2|n$, $\mathfrak{p}^2$ 2.

**2.** In den Fällen $N(\mathfrak{p})=p>2$, $\varphi(\mathfrak{p})|n$, $\mathfrak{p}^2\nmid p$, oder $N(\mathfrak{p})=2$, $2|n$, $\mathfrak{p}^2\nmid 2$, wird $\varphi(\mathfrak{p})=p-1$ und jede ganze Zahl des Körpers $\mathfrak{K}$ ist nach jedem Modul $\mathfrak{p}^\beta$ einer rationalen ganzen Zahl kongruent, es kann $\pi=p$ gesetzt werden, womit (2) bewiesen ist. Zu behandeln bleibt noch der Fall $N(\mathfrak{p})=2$, $n>1$, $2\nmid n$. Es ist

$$(5^*)\qquad \begin{aligned} \prod_{\tau_2} f(x+(\tau_2\pi)^n) &\equiv f(x)f(x+\pi^n)f(x+\pi^{2n})f(x+\pi^n(1+\pi)^n) \equiv \\ &\equiv f^2(x)f(x+\pi^n)f(x+\pi^n+\pi^{n+1}) \qquad (\text{mod. } \mathfrak{p}^{2+n}). \end{aligned}$$

Man bekommt weiter

$$f(x+\pi^n)f(x+\pi^n+\pi^{n+1})\equiv(f(x)+\pi^n f'(x))(f(x)+(\pi^n+\pi^{n+1})f'(x))\equiv$$
$$\equiv f^2(x)+(2\pi^n+\pi^{n+1})f(x)f'(x) \pmod{\mathfrak{p}^{2+n}}.$$

Wenn $\mathfrak{p}^2 \nmid 2$ ausfällt, so kann $\pi=2$ gesetzt werden, also wird

$$\prod_{\tau_2} f(x+(\tau_2\pi)^n)\equiv f^4(x) \qquad \pmod{\mathfrak{p}^{2+n}}$$

und die Formel (1*) ist gültig. Ist $\mathfrak{p}^3|2$, so wird

$$\prod_{\tau_3} f(x+(\tau_3\pi)^n)\equiv f(x)^{N(\mathfrak{p}^3)} \qquad \pmod{\mathfrak{p}^{3+n}}$$

und man bekommt die Formel (1**)

**3.** Analog läßt sich ohne Mühe auch das Produkt

$$\prod_{\varkappa_\alpha} f(x+(\varkappa_\alpha\pi)^n) \qquad \pmod{\mathfrak{p}^{\alpha+n}}$$

berechnen, wo $\varkappa_\alpha^\prime$ (mod. $\mathfrak{p}^\alpha$) die gegen $\mathfrak{p}$ relativ primen Zahlklassen durchläuft. Es können auch gewisse Verallgemeinerungen behandelt werden, worauf wir nicht eingehen.

*(Eingegangen am 4. Juni 1932.)*