ÜBER DIE ANZAHL DER LÖSUNGEN EINER KONGRUENZ.

Von

GYULA SÁNDOR †.[1]

Bezeichne p eine Primzahl. Die Teilbarkeit $a \mid b$ von ganzen Zahlen a, b soll stets „für p" verstanden werden, ferner bezeichne $a \| b$ dasselbe wie $a \mid b$, $b \mid a$ d. h. die Assoziiertheit von a, b für p. Die Diskriminante eines Polynoms $f(x) (\not\equiv 0)$ bezeichnen wir mit D_f.

Als eine Verschärfung eines Satzes von NAGELL[1] beweisen wir den folgenden:

Satz. *Ist* $f(x) (\not\equiv 0)$ *ein ganzzahliges Polynom vom Grade* $n (\geqq 1)$ *mit* $D_f \not\equiv 0$ *und*

$$p^{\delta} \| D_f, \tag{1}$$

so hängt die Lösungszahl N *der Kongruenz*

$$f(x) \equiv 0 \pmod{p^{\alpha}} \tag{2}$$

im Falle

$$\alpha > \delta \tag{3}$$

nicht von α *ab und dann gilt*

$$N \leqq n p^{\frac{\delta}{2}}. \tag{4}$$

Ferner gilt für alle $\alpha (\geqq 1)$ *die schwächere Abschätzung*

$$N \leqq n p^{\delta}. \tag{4'}$$

---

[1] Der Verfasser, ein sehr begabter ungarischer Mathematiker, starb im Jahre 1944 auf dem Schlachtfeld. Kurz vor seinem Tode schrieb er mir die Skizze vorliegender Arbeit, die ich etwas umgearbeitet und mit obigem Titel versehen aus gewissem Grunde erst jetzt veröffentlichen kann. L. Rédei.

[2] T. NAGELL, *Généralisation d'un théorème de Tchebicheff*. Journ. de Math. VIII, série *4* (1921), 343—356.

Ungeachtet (4') ist dieser Satz (für jedes ungerade p) scharf, wie das die folgenden Beispiele a), b) zeigen:

a) $f(x) = x(x + p^k) + d p^{2k-1}$ $(k \geqq 1,\ p \neq 2,\ p \nmid d)$.

Jetzt gilt

$$D_f = p^{2k-1}(p - 4d),\ \delta = 2k - 1.$$

Alle Lösungen von

$$f(x) \equiv 0 \pmod{p^\delta}$$

sind die

$$x \equiv 0 \pmod{p^k}.$$

Da für diese x stets

$$p^{2k} \nmid f(x)$$

gilt, so hat

$$f(x) \equiv 0 \pmod{p^{\delta+1}}$$

keine Lösungen, somit ist N für $\alpha \geqq \delta$ nicht konstant.

b) $f(x) = x(x + p^k)$ $(k \geqq 1)$.

Jetzt gilt

$$D_f = p^{2k},\ \delta = 2k.$$

Die Lösungen von

$$f(x) \equiv 0 \pmod{p^{2k+1}}$$

sind die

$$x \equiv 0,\ -p^k \pmod{p^{k+1}};$$

ihre Zahl ist

$$2p^k = n p^{\frac{\delta}{2}},$$

wonach sich (4) nicht verschärfen lässt.

Selbst Nagell hat die Konstanz von N nur für $\alpha > 2\delta$ bewiesen und er bekam für N die Abschätzung $N \leqq n p^{2\delta}$ $(\alpha \geqq 1)$.

Unser Verfahren wird, dass wir mit einer Verfeinerung von Nagells elementarer Methode die Behauptung über die Konstanz von N unter der Annahme (3) und zunächst die für alle $\alpha\,(\geqq 1)$ behauptete Abschätzung (4') beweisen, dann beweisen wir (4) mit Hilfe von p-adischen Zahlen.

§ 1.

Stets bezeichne a eine Lösung von (2), d. h. es soll

$$f(x) \equiv (x - a)\, g(x) \pmod{p^\alpha} \tag{5}$$

mit einem mod p^α bestimmten ganzzahligen Polynom $g(x)$ gelten. Nach Differenzieren entsteht

$$f'(a) \equiv g(a) \pmod{p^\alpha}. \tag{6}$$

Nunmehr werde (3) angenommen. Aus (5) folgt dann

$$D_f \equiv g^2(a) D_g \pmod{p^\alpha}.$$

Dies und (6) ergeben (wegen (1))

$$(f'(a))^2 \mid p^\delta. \tag{7}$$

Wir führen die Zahl β durch

$$p^\beta f'(a) \parallel p^\alpha \tag{8}$$

ein, dann gilt nach (7) $2\alpha \leqq 2\beta + \delta$ also nach (3) $2\alpha \leqq 2\beta + \alpha - 1$,

$$\frac{\alpha + 1}{2} \leqq \beta \, (\leqq \alpha). \tag{9}$$

Wegen dieses ist die Kongruenz

$$f(a + p^\beta z) \equiv 0 \pmod{p^{\alpha+1}} \tag{10}$$

gleichbedeutend mit

$$f(a) + p^\beta z f'(a) \equiv 0 \pmod{p^{\alpha+1}}$$

d. h. mit

$$\frac{f(a)}{p^\alpha} + \frac{p^\beta f'(a)}{p^\alpha} z \equiv 0 \pmod{p}.$$

Beide Koeffizienten links sind ganz und der zweite wegen (8) zu p prim. Hiernach hat diese Kongruenz genau eine Lösung, folglich machen die Lösungen von (10) eine Restklasse mod p aus. Ebenso sieht man, dass (10) mod p^α identisch erfüllt ist. Beide besagen, dass $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ und (2) gleich viele (nämlich $p^{\alpha-\beta}$) Lösungen in der Restklasse $a \pmod{p^\beta}$ haben. Das beweist die Behauptung über (3).

Es gilt trivial $N \leqq n p^{\alpha-1}$ $(\alpha \geqq 1)$. Hiernach ist (4') zunächst für $1 \leqq \alpha \leqq \delta + 1$ also wegen des jetzt Bewiesenen auch allgemein richtig.

§ 2.

Wir haben noch (4) zu beweisen. Nach einem Satz von SCHÖNEMANN (vgl. ORE[1]) gilt stets eine Umformung

$$f(x) \equiv f_1(x)(c + p f_2(x)) \pmod{p^\alpha}$$

---

[1] Ö. ORE, *Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern*, I. Math. Ann. *96* (1927), 313—352, insb. S. 317, Satz 2.

mit einer zu p primen ganzen Zahl c und zwei Polynomen f_1, f_2, von denen das erste den Leitkoeffizienten 1 hat. Deshalb dürfen wir beim Beweis von (4) voraussetzen, dass $f(x)$ den Leitkoeffizienten 1 hat. Wird wieder (3) angenommen, so besagt ein Satz von HENSEL[1] folgendes: Gilt (5) und wird für die Resultante $g(a)$ von $x-a$ und $g(x)$

$$p^{\varrho} \| g(a) \tag{11}$$

gesetzt, so hat $f(x)=0$ eine p-adische Nullstelle ξ mit

$$\xi \equiv 0 \pmod{p^{\alpha-\varrho}}. \tag{12}$$

Wir betrachten unter der Annahme (3) alle diejenigen a, zu denen auf diesem Wege ein festes ξ gehört. Unter den entsprechenden ϱ gibt es ein maximales[2], wofür wir die Bezeichnung ϱ beibehalten. Dann gilt (12) für die gesagten a noch mehr, folglich ist ihre Zahl höchstens p^{ϱ}. Die Anzahl der ξ ist höchstens n, somit gilt

$$N \leqq n p^{\varrho}.$$

Nun folgt aber aus (3), (6), (7), (11) $p^{2\varrho} | p^{\delta}$, somit haben wir (4) bewiesen.

---

[1] K. HENSEL, *Theorie der algebraischen Zahlen*. Berlin 1908, 1—349, insb. S. 71.

[2] Übrigens besagt der zitierte Henselsche Satz auch die Gleichheit der obigen ϱ, weswegen man einsehen kann, dass der oben folgende Schluss nicht zu verschärfen ist.