ARKIV FÖR MATEMATIK Band 3 nr 14

Mitgeteilt am 10. November durch T. NAGELL

# Bemerkungen über gleichzeitige Lösbarkeit von Kongruenzen

Von LARS FJELLSTEDT

T. NAGELL hat in einer wenig bekannten Arbeit [1][1] den folgenden Satz bewiesen:

*Es seien $f(x)$ und $g(x)$ zwei ganzzahlige irreduzible Polynome in $x$. Dann gibt es unendlich viele Primzahlen $p$, für welche die Kongruenzen*

$$\begin{aligned} f(x) &\equiv 0 \pmod{p} \\ g(x) &\equiv 0 \pmod{p} \end{aligned} \tag{1}$$

*ebenso viele inkongruente Lösungen haben, wie ihre respektiven Grade betragen.*

Man sieht aber leicht ein, dass die Voraussetzungen über die Irreduzibilität von $f(x)$ und $g(x)$ durch die schwächere Forderung, dass $f(x)$ und $g(x)$ nur einfache Nullstellen besitzen, ersetzt werden können.

Es gilt sogar der folgende allgemeinere Satz, wenn ein algebraischer Zahlkörper $\Omega$ endlichen Grades zugrunde gelegt wird:

**Satz 1.** *Es sei $\Omega$ ein algebraischer Zahlkörper, $f(x)$ und $g(x)$ Polynome ohne mehrfache Nullstellen mit ganzzahligen Koeffizienten aus $\Omega$. Dann gibt es unendlich viele Primideale $\mathfrak{p}$ des Körpers $\Omega$ für welche die Kongruenzen*

$$\begin{aligned} f(x) &\equiv 0 \pmod{\mathfrak{p}} \\ g(x) &\equiv 0 \pmod{\mathfrak{p}} \end{aligned}$$

*genau so viele inkongruente Wurzeln haben wie ihre respektiven Grade betragen.*

Ich zeige auch, dass es unendlich viele Primzahlen $p$ gibt, für welche keine der Kongruenzen (1) lösbar ist, wenn keins von den Polynomen vom ersten Grade ist. Hier müssen allerdings $f(x)$ und $g(x)$ als irreduzibel vorausgesetzt werden.

Zum Beweis von Satz 1 brauchen wir zwei Hilfsätze.

**Hilfsatz 1.** *Es sei $\mathfrak{p}$ vom Grade $f$ in $\Omega$. Dann ist die Funktion $x^{p^{fm}} - x \pmod{\mathfrak{p}}$ kongruent dem Produkte aller verschiedenen primären Primfunktionen $P(x)$ in $\Omega$ deren Grade Teiler von $m$ sind.*

[1] Die Zahlen in eckigen Klammern beziehen sich auf das Literaturverzeichnis am Schluss dieser Arbeit.

**Beweis.** Für den Begriff der primären Primfunktionen und Funktionenkongruenzen bezüglich eines Doppelmoduls siehe z. B. FRICKE [2]. Wir betrachten die Funktion

$$x^{p^{fm}} - x \tag{2}$$

für ein natürliches $m$ und denken sie mod $\mathfrak{p}$ in ihren primären Primfunktionen zerlegt:

$$x^{p^{fm}} - x = P_1 \cdot P_2 \cdots P_r \pmod{\mathfrak{p}}. \tag{3}$$

Von den rechts stehenden Primfunktionen können keine zwei mod $\mathfrak{p}$ kongruent sein, denn die Ableitung der Funktion (2) mod $\mathfrak{p}$ ist mit $-1$ kongruent.

Es findet sich in (3) rechts jede Primfunktion $P$, deren Grad $t$ ein Teiler von $m$ ist. Es gilt bekanntlich

$$x \equiv x^{p^{ft}} \pmod{\mathfrak{p}, P}.$$

Es folgt

$$x \equiv x^{p^{ft}} \equiv x^{p^{f \cdot 2t}} \equiv \ldots \equiv x^{p^{f \cdot at}} \pmod{\mathfrak{p}, P}$$

wo $a$ eine beliebige ganze Zahl ist. Es gilt also auch

$$x \equiv x^{p^{fm}} \pmod{\mathfrak{p}, P},$$

d. h. die Funktion (2) hat den Teiler $P$.

Man sieht sofort ein, dass keine der Primfunktionen in (3) rechts einen Grad haben kann, der grösser ist als $m$.

Der Grad $t$ jedes Primteilers $P$ von (2) ist ein Teiler von $m$. Denn erstens hat man die Kongruenz

$$x^{p^{ft}} \equiv x \pmod{\mathfrak{p}, P} \tag{4}$$

und zweitens kann nicht bereits für eine positive ganze Zahl $\nu$ die Kongruenz

$$x^{p^{f \cdot \nu}} \equiv x \pmod{\mathfrak{p}, P}$$

gelten, da sonst der Grad $t > \nu$ wäre, was unmöglich ist.

**Hilfsatz 2.** *Es sei $\Omega$ ein algebraischer Zahlkörper und $\mathbf{K}(\alpha)$ algebraisch vom Grade $n$ in bezug auf $\Omega$. Es genüge $\alpha$ die Gleichung $F(x) = 0$, wo $F(x)$ ein in $\Omega$ irreduzibles Polynom mit ganzzahligen Koeffizienten aus $\Omega$ bedeutet. Zerfällt dann, in $\mathbf{K}(\alpha)$, ein Primideal $\mathfrak{p}$ aus $\Omega$ das kein Indexteiler ist, in verschiedenen Primidealen ersten Grades so hat die Kongruenz*

$$F(x) \equiv 0 \pmod{\mathfrak{p}} \text{ in } \Omega$$

*genau $n$ inkongruente Wurzeln.*

**Beweis.** Es sei

$$F(x) \equiv \varphi_1(x)^{e_1} \varphi_2(x)^{e_2} \ldots \varphi_r(x)^{e_r} \pmod{\mathfrak{p}}, \tag{5}$$

die Zerlegung von $F(x)$ in Primfunktionen (mod $\mathfrak{p}$). Zwei Zahlen $\varphi_i(\alpha)$ und $\varphi_j(\alpha)$, $i \neq j$ können dann keinen gemeinsamen Primidealfaktor haben, der auch in $\mathfrak{p}$

aufgeht, denn es lässt sich Polynome $A(x)$ und $B(x)$ in $\mathbf{\Omega}$ so bestimmen, dass

$$A(x)\,\varphi_i(x)+B(x)\,\varphi_j(x)\equiv 1 \pmod{\mathfrak{p}}.$$

Wir haben also bisher folgendes Resultat: Wenn $F(x)$ die Primfunktionzerlegung (5) (mod $\mathfrak{p}$) hat, besteht für $\mathfrak{p}$ in $\mathbf{K}(\alpha)$ die Idealzerlegung

$$\mathfrak{p}=\mathfrak{a}_1\,\mathfrak{a}_2\ldots\mathfrak{a}_r,$$

wobei die Ideale $\mathfrak{a}_i$ alle zu einander prim sind, und

$$\mathfrak{a}_i=(\mathfrak{p},\,\varphi_i(\alpha)^{e_i}).$$

Es sei jetzt $\mathfrak{P}_i$ ein Primideal das in $\mathfrak{a}_i$ aufgeht; dann soll bewiesen werden, dass der Relativgrad $f^*$ von $\mathfrak{P}_i$ durch den Grad von $\varphi_i(x)$ teilbar ist. Hieraus folgt unmittelbar unser Hilfsatz.

Alle ganze Zahlen $\vartheta$ in $\mathbf{K}(\alpha)$ genügen der Kongruenz

$$\vartheta^{pf^*}-\vartheta\equiv 0 \pmod{\mathfrak{P}_i}.$$

Nach Hilfsatz 1 gibt es also ein $P(x)$ mit

$$P(\alpha)\equiv 0 \pmod{\mathfrak{P}_i}. \tag{6}$$

Dann ist aber $P(x)=\varphi_i(x)$, denn wäre dies nicht der Fall, könnte man die Polynome $A(x)$ und $B(x)$ so bestimmen, dass

$$A(x)\,P(x)+B(x)\,\varphi_i(x)\equiv 1 \pmod{\mathfrak{p}},$$

woraus mit $x=\alpha$

$$A(\alpha)\,P(\alpha)\equiv 1 \pmod{\mathfrak{P}_i}$$

folgt, im Gegensatz zu (6). Aus $P(x)=\varphi_i(x)$ folgt dann die Behauptung.

**Beweis von Satz 1.** Es sei $\mathbf{\Omega}$ ein algebraischer Zahlkörper vom Grade $m$ über den Körper $\mathbf{P}$ der rationalen Zahlen. Es sei $\mathbf{K}$ ein algebraischer Zahlkörper $N$ten Grades über $\mathbf{\Omega}$ und $\mathbf{k}$ ein Unterkörper $n$ten Grades von $\mathbf{K}$ über $\mathbf{\Omega}$. Es sei ferner $\mathfrak{p}$ ein Primideal ersten Grades in $\mathbf{K}/\mathbf{P}$, dann ist die Relativnorm von $\mathfrak{p}$ bezüglich des Körpers $\mathbf{k}$ ein Ideal $\mathfrak{j}$ in $\mathbf{k}$, also

$$N_k(\mathfrak{p})=\mathfrak{j}.$$

Ist $p$ die rationale Primzahl, die durch $\mathfrak{p}$ teilbar ist, so ist die Norm in $\mathbf{k}$ von $N_k(\mathfrak{P})$ bezüglich $\mathbf{P}$, gleich $p$, weil $\mathfrak{p}$ vom ersten Grade ist; also

$$N_p(\mathfrak{j})=p.$$

Hieraus folgt, dass $\mathfrak{j}$ ein Primideal ersten Grades in $\mathbf{k}$ ist. Wenn die rationale Primzahl $p$ durch ein Primideal ersten Grades in $\mathbf{K}$ teilbar ist, so ist sie also auch durch ein Primideal ersten Grades in $\mathbf{k}$ teilbar. Es gilt ferner auch: Ist

die rationale Primzahl $p$ gleich dem Produkt von $NM$ Primidealen ersten Grades in $\mathbf{K}$, so ist die gleich dem Produkt von $nM$ Primidealen ersten Grades in $\mathbf{k}$.

Es sei nämlich

$$p = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_{NM}$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_{NM}$ Primidealen ersten Grades in $\mathbf{K}$ sind, und

$$N_k(\mathfrak{p}_i) = \mathfrak{j}_i,$$

wo also $\mathfrak{j}_i$, wie soeben bemerkt, ein Primideal ersten Grades in $\mathbf{k}$ ist. Dann wird

$$N_k(p) = \mathfrak{j}_1 \mathfrak{j}_2 \cdots \mathfrak{j}_{NM} = p^{\frac{N}{n}}.$$

Hieraus folgt aber, dass $p$ nur durch Primideale ersten Grades in $\mathbf{k}$ teilbar ist, und folglich gleich einem Produkt von $nM$ solchen Primidealen ist.

Wenn $\mathbf{K}$ über $\mathbf{P}$ ein Galois'scher Körper ist, dann ist bekanntlich jede (rationale) Primzahl, die durch ein Primideal ersten Grades in $\mathbf{K}$ teilbar ist, gleich dem Produkt von Primidealen ersten Grades. Weiter gibt es ja in jedem algebraischen Körper unendlich viele Primideale ersten Grades. Es sei jetzt $\mathfrak{p} = N_\Omega(\mathfrak{P})$ und es sei $F(x) = 0$ eine irreduzible algebraische Gleichung $N$ten Grades über $\mathbf{\Omega}$, die $\mathbf{K}$ bestimmt; es sei ferner $f(x) = 0$ eine irreduzible algebraische Gleichung $n$ten Grades über $\mathbf{\Omega}$, die $\mathbf{k}$ bestimmt, dann gilt dem Vorhergehenden nach, und nach Hilfsatz 2:

Hat die Kongruenz

$$F(x) \equiv 0 \pmod{\mathfrak{p}} \tag{7}$$

Lösungen für das Primideal $\mathfrak{p}$, so hat auch die Kongruenz

$$f(x) \equiv 0 \pmod{\mathfrak{p}} \tag{8}$$

Lösungen. Ferner: hat (7) $N$ inkongruente Lösungen, so hat (8) $n$ inkongruente Lösungen.

Es seien nun $f(x)$ und $g(x)$ zwei irreduzible Polynome in $x$ mit ganzzahligen Koeffizienten aus $\mathbf{\Omega}$; es seien ferner $\mathbf{k}_1$ und $\mathbf{k}_2$ die beiden algebraischen Zahlkörper über $\mathbf{\Omega}$, die durch $f(x) = 0$ und $g(x) = 0$ bestimmt sind. Es sei endlich $\mathbf{K}$ ein Galois'scher Zahlkörper, der $\mathbf{\Omega}$ sowohl als $\mathbf{k}_1$ wie $\mathbf{k}_2$ enthält, und $F(x) = 0$ eine irreduzible algebraische Gleichung (mit ganzzahligen Koeffizienten aus $\mathbf{\Omega}$), die $\mathbf{K}$ bestimmt. Hat dann die Kongruenz

$$F(x) \equiv 0 \pmod{\mathfrak{p}}$$

für das Primideal $\mathfrak{p}$ ebenso viele inkongruente Lösungen, wie ihr Grad beträgt, so haben auch die Kongruenzen

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

$$g(x) \equiv 0 \pmod{\mathfrak{p}}$$

ebenso viele inkongruente Lösungen, wie ihre respektiven Grade betragen.

Das bisherige Ergebnis gilt natürlich auch dann, wenn wir statt zwei, eine beliebige Anzahl von irreduziblen Polynomen haben.

Es sei jetzt über $f(x)$ und $g(x)$ nur vorausgesetzt, dass sie keine mehrfache Wurzeln haben, und dass

$$f(x)=f_1(x)\,f_2(x)\cdots f_r(x)$$
$$g(x)=g_1(x)\,g_2(x)\cdots g_s(x)$$

die Zerlegung von $f(x)$ und $g(x)$ in irreduziblen Faktoren sei. Wir können natürlich annehmen, dass $f(x)$ und $g(x)$ keine gemeinsame Faktoren haben. Da die Polynome $F(x)$, $f_i(x)$ und $g_k(x)$ alle irreduzibel und verschieden sind, gibt es ganzzahlige Polynome in $x$, $h_{i,j}(x)$, $k_{i,j}(x)$, $u_{i,j}(x)$ und $v_{i,j}(x)$ mit

$$\left.\begin{aligned} h_{i,j}(x)\,f_i(x)+k_{i,j}(x)\,f_j(x)&=A_{i,j}, \quad \begin{cases} i=1,\,2,\,\ldots,\,r \\ j=1,\,2,\,\ldots,\,r \end{cases} \\ u_{i,j}(x)\,g_i(x)+v_{i,j}(x)\,g_j(x)&=B_{i,j}, \quad \begin{cases} i=1,\,2,\,\ldots,\,s \\ j=1,\,2,\,\ldots,\,s \end{cases} \end{aligned}\right\} \tag{9}$$

wo $A_{i,j}$ und $B_{i,j}$ von Null verschiedene Konstanten sind.

Es sei $T=\max\limits_{i,j}\{N_p(A_{i,j}),\,N_\rho(A_{i,j})\}$. Da es unendlich viele Primidealen $\mathfrak{p}$ gibt, die nicht in $T$ aufgeht, für welche

$$f_i(x)\equiv 0 \pmod{\mathfrak{p}},\ i=1,\,2,\,\ldots,\,r$$

und

$$g_k(x)\equiv 0 \pmod{\mathfrak{p}},\ k=1,\,2,\,\ldots,\,s$$

alle genau so viele inkongruente Wurzeln haben wie ihre respektiven Grade betragen, folgt der Behauptung aus (9).

Nach FROBENIUS [3] gibt es unendlich viele Primzahlen $p$, für welche die Kongruenz

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

wo $f(x)$ ein ganzzahliges irreduzibles Polynom in $x$ vom Grade $n\geqq 2$ bedeutet, keine Lösungen haben. Aus diesem Resultat folgt nun ganz einfach:

**Satz 2.** *Gegeben zwei ganzzahlige irreduzible Polynome in $x$, $f(x)$ und $g(x)$, von welchen kein vom ersten Grade ist. Dann gibt es unendlich viele Primzahlen $p$, für welche die Kongruenzen*

$$\left.\begin{aligned} f(x)&\equiv 0 \pmod{p} \\ g(x)&\equiv 0 \pmod{p} \end{aligned}\right\} \tag{10}$$

*keine Lösungen haben.*

**Beweis.** Es sei $f(x)=0$ die definierende Gleichung des Körpers $\mathbf{K}_1$ und $g(x)=0$ die des Körpers $\mathbf{K}_2$. Es sei $F(x)=0$ die definierende Gleichung eines Galoisschen Körpers $\mathbf{\Omega}$ das $\mathbf{K}_1$ und $\mathbf{K}_2$ als Unterkörper enthält. Nach dem FROBENIUSschen Satze gibt es unendlich viele Primzahlen, für die $F(x)\equiv 0 \pmod{p}$ keine Lösungen haben. Das bedeutet nun das $p$ in $\mathbf{\Omega}$ unzerlegt bleibt. Dann ist $p$ natürlich auch in $\mathbf{K}_1$ und $\mathbf{K}_2$ unzerlegt, d. h. die Kongruenzen (10) haben keine Lösungen. Das Ergebnis lässt sich selbstverständlich auf mehrere Polynome aus-

dehnen. Es kann auch die Forderung, dass $f(x)$ und $g(x)$ irreduzibel sein soll, durch die Bedingung ersetzt werden, dass kein irreduzibler Faktor vom ersten Grade ist.

## LITERATUR

1. T. NAGELL, Zahlentheoretische Notizen I–VI. Videnskapsselskapets Skrifter. I. Mat.-Naturv. Klasse. 1923. No. 13.
2. R. FRICKE, Lehrbuch der Algebra III. Braunschweig 1928.
3. G. FROBENIUS, Berl. Ber. 1896, I, S. 689–703.

Tryckt den 18 januari 1955

Uppsala 1955. Almqvist & Wiksells Boktryckeri AB