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 Ω endlichen Grades zugrunde gelegt wird:

Satz 1. *Es sei Ω ein algebraischer Zahlkörper, $f(x)$ und $g(x)$ Polynome ohne mehrfache Nullstellen mit ganzzahligen Koeffizienten aus Ω. Dann gibt es unendlich viele Primideale $\mathfrak{p}$ des Körpers Ω 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 Ω. Dann ist die Funktion $x^{p^{fm}} - x \pmod{\mathfrak{p}}$ kongruent dem Produkte aller verschiedenen primären Primfunktionen $P(x)$ in Ω deren Grade Teiler von m sind.*

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