Ein Satz über Kongruenzen höheren Grades.

Von GUSTAV RADOS.

Die rationalen Wurzeln einer vorgelegten ganzzahligen algebraischen Gleichung können stets durch eine endliche Anzahl von Versuchen bestimmt werden und damit auch das Polynom derjenigen Gleichung, deren Wurzeln mit den rationalen Wurzeln der vorgelegten Gleichung übereinstimmen. Bisher ist kein Verfahren bekannt und die Warscheinlichkeit der Existenz eines solchen ist auch äusserst gering, durch das die erwähnten Versuche umgangen werden könnten und das die Bildung dieses Polynoms vermittels einer Formel ermöglichen würde. Umso bemerkenswerter ist die Tatsache, dass das analoge[1] Problem der Theorie der Kongruenzen höheren Grades sich ohne Versuche durch eine Formel glatt lösen lässt. Es ist dies umso merkwürdiger, als das Versuchselement bei der Mehrzahl der zahlentheoretischen Probleme nicht ausgemerzt werden kann.

Es sei die vorgelegte Kongruenz

$$(1)\quad f(x) \equiv a_0 x^{p-2} + a_1 x^{p-3} + \ldots + a_{p-2} \equiv 0 \pmod{p}$$[1]

mit dem Primzahl-Modul p und in der der Koeffizient a_{p-2} durch p nicht teilbar ist, (auf diese Form kann bekanntlich jede Kongruenz zurückgeführt werden) alsdann ist es bekannt, dass die Anzahl ihrer verschiedenen Wurzeln[2] gleich ist dem Überschuss von

[1] Dass die Lösung dieses Problems ohne Versuche durch direkte Berechnung möglich ist, geht schon aus der Tatsache hervor, dass das gesuchte Polynom sich als grösster gemeinschaftlicher Teiler des Polynoms der vorgelegten Kongruenz und desjenigen der entsprechenden Fermat'schen Kongruenz darstellen lässt Hier handelt es sich jedoch um die Darstellung durch eine explicite Formel.

[2] S. meine Arbeit „Zur Theorie der Congruenzen höheren Grades" (Journal f. d. reine u. angewandte Mathematik, Bd 99, Pag. 258)

$p-1$ über den in Bezug auf den Modul p bestimmten Rang der cyklischen Determinante

$$C = \begin{vmatrix} a_0 & a_1 & \ldots & a_{p-3} & a_{p-2} \\ a_1 & a_2 & \ldots & a_{p-2} & a_0 \\ \cdot & \cdot & \ldots & \cdot & \cdot \\ a_{p-2} & a_0 & \ldots & a_{p-4} & a_{p-3} \end{vmatrix} = (a_0, a_1, \ldots, a_{p-3}).$$

Ist daher der Rang von C (mod. p) gleich $p-s-r$, so hat die vorgelegte Kongruenz genau r verschiedene Wurzeln. Es seien dieselben

$$\beta_1, \beta_2, \ldots, \beta_r.$$

Das zu lösende Problem besteht nun in der Bestimmung des Polynoms

$$\varphi(x) = (x-\beta_1)(x-\beta_2)\ldots(x-\beta_r) = \\ = x^r + \varphi_1 x^{r-1} + \ldots + \varphi_r$$

mit Umgehung von Versuchen durch eine Formel.

Die Lösung dieser Aufgabe kann durch das folgende Theorem erledigt werden:

Hat die Kongruenz

$$f(x) \equiv a_0 x^{p-2} + a_1 x^{p-3} + \ldots + a_{p-2} \equiv o \pmod{p}$$
$$(a_{p-2} \not\equiv o \pmod{p}; \; p \text{ ist eine Primzahl})$$

genau r verschiedene Wurzeln, so wird diejenige Kongruenz r-ten Grades, deren Wurzeln mit denjenigen von $f(x) \equiv o$ *(mod. p) übereinstimmen, durch die Formel*

$$\varphi(x) \equiv (-1)^r (r!)^{p-r} \begin{vmatrix} s_1 & 1 & 0 & 0 & \ldots & 0 & 0 \\ s_2 & s_1 & 2 & 0 & \ldots & 0 & 0 \\ s_3 & s_2 & s_1 & 3 & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \ldots & \cdot & \cdot \\ s_{r-1} & s_{r-2} & s_{r-3} & s_{r-4} & \ldots & r-1 & 0 \\ s_r & s_{r-1} & s_{r-2} & s_{r-3} & \ldots & s_1 & r \\ x^r & x^{r-1} & x^{r-2} & x^{r-3} & \ldots & x & 1 \end{vmatrix} \equiv o \pmod{p}$$

geliefert, wo an Stelle von

$$s_i \equiv \sum_{k=1}^{p-1} k^i \left[1 - f(k)^{p-1} \right] \pmod{p}$$

zu setzen ist.

Der Beweis für diesen Satz kann in einfacher Weise geführt werden, indem man eine Wahrnehmung verwertet, die von Lebesgue herrührt und die er für die Bestimmung der Wurzelanzahl einer Kongruenz verwendet hat.[1]

Diese Wahrnehmung besteht darin, dass der Ausdruck

$$G_k = 1 - \left[f(k) \right]^{p-1}$$

in Bezug auf den Primzahl-Modul p kongruent 1 oder o wird, jenachdem k Wurzel oder Nichtwurzel der Kongruenz

$$f(x) \equiv o \pmod{p}$$

ist.

Sind nun

$$\beta_1 , \beta_2 , \ldots , \beta_r$$

die Wurzeln der Kongruenz 1), so können mit Benützung dieser Bemerkung die nachfolgenden Kongruenzen angesetzt werden:

$$s_1 \equiv \sum_{k=1}^{p-1} k \left[1 - f(k)^{p-1} \right] \equiv \beta_1 + \beta_2 + \ldots + \beta_r$$

$$s_2 \equiv \sum_{k=1}^{p-1} k^2 \left[1 - f(k)^{p-1} \right] \equiv \beta_1^2 + \beta_2^2 + \ldots + \beta_r^2 \pmod{p}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$s_r \equiv \sum_{k=1}^{p-1} k^r \left[1 - f(k)^{p-1} \right] \equiv \beta_1^r + \beta_2^r + \ldots + \beta_r^r$$

Auf diese Weise kann man daher die sämtlichen Potenzsummen der Wurzeln

$$\beta_1 , \beta_2 , \ldots , \beta_r$$

bestimmen.

Wenn nun

$$\varphi(x) \equiv (x - \beta_1)(x - \beta_2) \ldots (x - \beta_r) \equiv$$
$$\equiv x^r + \varphi_1 x^{r-1} + \ldots + \varphi_r \pmod{p}$$

gesetzt wird, so dass

$$\varphi_1 = - \sum \beta_1 , \quad \varphi_2 = \sum \beta_1 \beta_2 , \ldots , \varphi_k = (-1)^k \sum \beta_1 \beta_2 \ldots \beta_k$$
$$\ldots \varphi_r = (-1)^r \beta_1 \beta_2 \ldots \beta_r$$

---

[1] Lebesgue: „Recherches sur les nombres", — Journal de Mathématiques pures et appliquées, Tome II. (1837). pag. 254.

S. ferner Hurwitz: „Über höhere Kongruenzen", Archiv der Mathematik und Physik, III. Reihe, Bd. V. Pag. 17. 1902.

die elementaren symmetrischen Funktionen der Wurzeln

$$\beta_1 , \beta_2 . . . . , \beta_r$$

bedeuten, so bestehen zwischen diesen und den Potenzsummen derselben Grössen die nachfolgenden Newton'schen Identitäten:[1]

$$\begin{aligned}
&s_1 + \varphi_1 \equiv 0 \\
&s_2 + s_1 \varphi_1 + 2 \varphi_2 \equiv 0 \\
&s_3 + s_2 \varphi_1 + s_1 \varphi_2 + 3 \varphi_3 \equiv 0 \qquad (\text{mod. } p) \\
&. \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\
&s_r + s_{r-1} \varphi_1 + s_{r-2} \varphi_2 + . . . \quad + r \varphi_r \equiv 0
\end{aligned}$$

Fügt man diesen Kongruenzen noch die weitere Kongruenz

$$\left[x^r - \varphi(x)\right] + x^{r-1} \varphi_1 + x^{r-2} \varphi_2 + \ldots + \varphi_r \equiv 0 \pmod{p}$$

hinzu, so folgt aus dem simultanen Bestehen dieser Kongruenzen

$$\begin{vmatrix}
s_1 & 1 & 0 & 0 & \ldots & 0 \\
s_2 & s_1 & 2 & 0 & \ldots & 0 \\
s_3 & s_2 & s_1 & 3 & \ldots & 0 \\
 & . & . & . & \ldots & \\
s_r & s_{r-1} & s_{r-2} & s_{r-3} & \ldots & r \\
x^r - \varphi(x) & x^{r-1} & x^{r-2} & x^{r-3} & \ldots & 1
\end{vmatrix} \equiv 0 \pmod{p}$$

und hieraus schlieszlich, da $r!$ und p teilerfremde Zahlen sind, die Kongruenz

$$\varphi(x) \equiv (-1)^r (r!)^{p-2} \begin{vmatrix}
s_1 & 1 & 0 & 0 & \ldots & 0 \\
s_2 & s_1 & 2 & 0 & \ldots & 0 \\
s_3 & s_2 & s_1 & 3 & \ldots & 0 \\
. & . & . & . & \ldots & \\
s_r & s_{r-1} & s_{r-2} & s_{r-3} & \ldots & r \\
x^r & x^{r-1} & x^{r-2} & x^{r-3} & \ldots & 1
\end{vmatrix} \equiv 0 \pmod{p}$$

deren Wurzeln mit denjenigen der Kongruenz 1) übereinstimmen.

Hat die Kongruenz 1) lediglich eine einzige Wurzel, so kann diese durch die Formel

$$\xi \equiv \sum_{k=1}^{p-1} k \left[1 - f(k)^{p-1}\right] \pmod{p}$$

dargestellt werden.

[1] Diese haben für Kongruenzen, deren Wurzelanzahl mit ihrem Grad übereinstimmt, ebenso Geltung wie für algebraische Gleichungen.

Schliesslich möge die entwickelte Methode auf das Beispiel der Kongruenz

$$f(x) \equiv x^5 + 4x^4 + 2x^3 + 2x^2 + x + 4 \equiv 0 \pmod{7}$$

angewendet werden. Da der Rang der Determinante

$$C = (1, 4, 2, 2, 1, 4)$$

gleich 4 ist, besitzt die vorgelegte Kongruenz genau 2 verschiedene Wurzeln. Indem man s_1 und s_2 berechnet, ergibt sich

$$s_1 = \sum_{k=1}^{6} k\left[1 - f(k)^6\right] \equiv 3 \pmod{7}$$

$$s_2 = \sum_{k=1}^{6} k^2\left[1 - f(k)^6\right] \equiv 5$$

Es ist daher die Kongruenz 2-ten Grades, die die Wurzeln der vorgelegten Kongruenz 5-ten Grades liefert:

$$\varphi(x) \equiv (2!)^5 \begin{vmatrix} s_1 & 1 & 0 \\ s_2 & s_1 & 2 \\ x^2 & x & 1 \end{vmatrix} \equiv 4 \begin{vmatrix} 3 & 1 & 0 \\ 5 & 3 & 2 \\ x^2 & x & 1 \end{vmatrix} \equiv x^2 - 3x + 2 \equiv 0 \pmod{7}$$

Die Wurzeln $x \equiv 1, 2 \pmod{7}$ stimmen in der Tat — wie man sich leicht überzeugt — mit den Wurzeln der vorgelegten Kongruenz 5-ten Grades überein.