Ueber die Anzahl der Lösungen gewisser Kongruenzen nach einem Primzahlmodul

Author(s):
Widmer, Adolf

Publication Date:
1919

Permanent Link:
https://doi.org/10.3929/ethz-a-000107269

Ueber die Anzahl der Lösungen gewisser Kongruenzen nach einem Primzahlmodul.

VON DER

EIDGENÖSSISCHEN TECHNISCHEN HOCHSCHULE
IN ZÜRICH

ZUR ERLANGUNG DER

WÜRDE EINES DOKTORS DER MATHEMATIK

GENEHMIGTE

PROMOTIONSARBEIT

VORGELEGT VON

ADOLF WIDMER, DIPL. FACHLEHRER

AUS HAUSEN b. B. (AARGAU)

Referent: Herr Prof. Dr. A. Hurwitz
Korreferent: Herr Prof. Dr. H. Weyl.

207.

ZÜRICH 1919
Fachschriften-Verlag & Buchdruckerei A.-G.

Einleitung.

Die vorliegende Arbeit zerfällt in drei Teile. Im ersten Kapitel betrachten wir nach dem Vorgange von E. Jacobsthal („Anwendungen einer Formel aus der Theorie der quadratischen Reste", Diss. Göttingen 1906, oder Crelle's Journal Bd. 132 pag. 238) ganze ganzzahlige Funktionen $f(x)$, lassen darin die Variable x nach dem Primzahlmodul p ein vollständiges Restsystem durchlaufen und untersuchen nun die Anzahlen der quadratischen Reste und der Nichtreste (mod. p), wie sie unter den erhaltenen Funktionswerten auftreten. Diese Anzahlen ermöglichen den Nachweis, dass gewisse Zahlen als Summen von Quadraten dargestellt werden können: Herr Jacobsthal zeigt, dass die für $f(x) = x(x^2 + a)$ auftretenden Anzahlen eine Zerlegung der Primzahlen von der Form $4n + 1$ in zwei Quadrate ergeben; werden die Ueberlegungen auf die Funktion $f(x) = x(x^3 + a)$ übertragen, wie es Herr L. v. Schrutka in Crelle's Journal Bd. 140 pag. 252 getan hat, so geht aus ihnen die Darstellung der Primzahlen von der Form $6n + 1$ als Summe eines einfachen und eines dreifachen Quadrates hervor. Der Beweis dieses Satzes ist im folgenden durch Verwendung einer Primitivwurzel des Moduls p wesentlich vereinfacht worden. Werden die Ueberlegungen für $f(x) = x(x^4 + a)$ durchgeführt, so ergeben sie die Zerlegung der Primzahlen von der Form $8n + 1$ in ein einfaches und ein doppeltes Quadrat. Die Bestimmung der Basen der auftretenden Quadrate wurde in allen Fällen mit dem Prinzip durchgeführt, dass eine Zahl a schon durch ihren Rest (mod. p) vollständig bekannt ist, falls ihr absoluter Betrag hinreichend klein ist.

Im II. Kapitel werden, im Anschlusse an eine Arbeit von Herrn Prof. Dr. A. Hurwitz die Lösungsanzahlen der Kongruenz

$$a x^e + b y^e + c z^e \equiv 0 \text{ (mod. } p)$$

und Relationen zwischen diesen Zahlen betrachtet. Diese Resultate werden im III. Kapitel dazu verwendet, um für die Lösungsanzahl der quadratischen Kongruenz

$$a_1 x_1^2 + a_2 x_2^2 + \dots + a_r x_r^2 \equiv 0 \text{ (mod. } p)$$

eine Formel herzuleiten.