

Werk

Titel: Bemerkung über die Auflösung quadratischer Congruenzen

Autor: Tonelli, Alberto

Jahr: 1891

PURL: https://resolver.sub.uni-goettingen.de/purl?252457072_1891 | log50

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

✉ info@digizeitschriften.de

Hiermit ist die oben ausgesprochene Behauptung dargethan. Ich bemerke übrigens, daß man auf Grund der vorstehenden Entwicklungen auch den im Eingang dieser Note angegebenen Satz selbst erweisen kann. Man überzeugt sich nämlich leicht, daß die $(\cdot, \cdot)$ Lösungssysteme des s ten Gleichungssystems in allen Fällen linear unabhängig sind, und daß weitere von einander linear unabhängige Lösungen nicht existiren können. Zu letzterem Behuf könnte man übrigens auch die von Herrn Hilbert für jeden Modul angegebene charakteristische Function $\chi(R)$ benutzen. Da nämlich offenbar jede Form der R ten Ordnung nach dem Modul $(x_1 \dots x_n)$ der Null congruent ist, so ist $\chi(R) = 0$; andererseits kann der allgemeinen Gestalt von $\chi(R)$, deren Beschaffenheit sich auf Grund des allgemeinen Theorems III direct angeben läßt, nur durch diejenigen Coefficienten genügt werden, welche mit den im obigen Satz figurirenden Zahlen identisch sind. Dies ist auch dann noch der Fall, wenn der Grad R der bezüglichen Formen kleiner als n ist; in diesem Fall bricht zwar die Kette der abgeleiteten Gleichungen vor dem n ten Gleichungssystem ab, die auf dasselbe bezüglichen Schlüsse werden aber dadurch in keiner Weise tangirt.

Bemerkung über die Auflösung quadratischer Congruenzen.

Von

Alberto Tonelli in Rom.

(Vorgelegt von Ernst Schering am 7. November.)

Auszug aus Briefen vom 18. April und 15. Juni 1891.

Das bekannte Verfahren zur allgemeinen Auflösung einer quadratischen Congruenz für einen Modul, welcher eine von der Form $4h+1$ verschiedene Primzahl ist, habe ich in der Weise verallgemeinert, daß es auch auf Primzahlen dieser letzteren Form anwendbar wird.

Wenn die Congruenz

$$xx \equiv c \pmod{p}$$

zur Auflösung vorgegeben ist und noch ein beliebiger quadratischer Nichtrest $g \pmod{p}$ bekannt ist, so besteht dies Verfahren im Folgenden.

Es sei $p = \alpha 2^s + 1$, worin α ungerade $s \geq 1$ ist, dann wird nach dem Eulerschen Satze

$$c^{\alpha 2^{s-1}} \equiv +1, \quad g^{\alpha 2^{s-1}} \equiv -1 \pmod{p}.$$

Wenn noch $s \geq 2$ ist, folgt aus der ersteren dieser beiden Congruenzen die neue

$$c^{\alpha 2^{s-2}} \equiv \pm 1 \pmod{p}.$$

Es sei nun $\varepsilon_0 = 0$ wenn das obere (+)Zeichen, $\varepsilon_1 = 1$ wenn das untere (—)Zeichen stattfindet, so daß immer

$$g^{\varepsilon_0 \alpha 2^{s-1}} c^{\alpha 2^{s-2}} \equiv +1 \pmod{p}$$

wird. Wenn nun noch $s \geq 3$ ist, so folgt hieraus

$$g^{\varepsilon_0 \alpha 2^{s-2}} c^{\alpha 2^{s-3}} \equiv \pm 1 \pmod{p}.$$

Gilt hier das obere (+)Zeichen, so setze ich $\varepsilon_1 = 0$, gilt das untere (—)Zeichen, so setze ich $\varepsilon_1 = 1$, so daß immer

$$g^{\varepsilon_1 \alpha 2^{s-1}} g^{\varepsilon_0 \alpha 2^{s-2}} c^{\alpha 2^{s-3}} \equiv +1 \pmod{p}$$

wird. Auf diese Weise erhält man die Congruenz

$$g^{\alpha 2^{s-k} (\varepsilon_0 + \varepsilon_1 2 + \dots + \varepsilon_{k-1} 2^{k-1})} c^{\alpha 2^{s-k-1}} \equiv 1 \pmod{p}$$

so lange noch $k < s$ ist; also für $k = s - 1$ wird

$$g^{\alpha 2 (\varepsilon_0 + \varepsilon_1 2 + \dots + \varepsilon_{s-2} 2^{s-2})} c^{\alpha} \equiv 1 \pmod{p}$$

und demnach

$$x \equiv \pm g^{\alpha (\varepsilon_0 + \varepsilon_1 2 + \dots + \varepsilon_{s-2} 2^{s-2})} c^{\frac{\alpha+1}{2}} \pmod{p}$$

gesetzt, gibt die Wurzeln der Congruenz

$$xx \equiv c \pmod{p}.$$

Aus dieser Lösung erhält man durch

$$x_1 \equiv x^{\frac{p^{\lambda-1}}{c} \frac{p^{\lambda} - 2p^{\lambda-1} + 1}{2}} \pmod{p^{\lambda}}$$

eine allgemeine Auflösung der Congruenz

$$x_1 x_1 \equiv c \pmod{p^{\lambda}},$$

wie man sich leicht mit Anwendung des verallgemeinerten Fermatschen Satzes und des Satzes überzeugt, daß wenn

$$a \equiv b \pmod{p} \quad \text{ist, auch} \quad ap^{\lambda-1} \equiv bp^{\lambda-1} \pmod{p^{\lambda}}$$

wird.

Diese Formeln für die Wurzeln sind nicht nur theoretisch bemerkenswerth, sondern sie können auch in Fällen, wo andere besondere Methoden ihren Dienst versagen, von praktischer Bedeutung zur Berechnung der Wurzel der quadratischen Congruenzen sein.

Ueber die Fluorescenzwirkungen stehender Lichtwellen.

Von

P. Drude und W. Nernst.

Es bietet ein erhebliches Interesse, die bekannten Untersuchungen Hrn. Wiener's¹⁾ über die photographische Wirksamkeit stehender Lichtwellen auch auf andere Erscheinungen, durch welche Lichtbewegung objektiv zur Darstellung gebracht werden kann, auszudehnen, und für möglichst verschiedene Arten derselben folgende beiden Fragen zu beantworten:

1) Giebt es bei stehenden Lichtwellen Maxima und Minima der Wirkungsweise?

2) Fallen bei ein und derselben stehenden Lichtwelle die Maxima der Wirkung für die verschiedenen, zur Untersuchung gelangten Erscheinungsklassen zusammen?

Wirkungen des Lichtes sind auf vielen, recht verschiedenartigen Gebieten beobachtet; außer der durch Belichtung hervorgerufenen Erwärmung, Fluorescenz, und der Erscheinung der Hauchbilder, wie von Wiener erwähnt ist, möchten wir hier noch die durch Belichtung hervorgerufene Entladung negativ elektrisch geladener Körper, die Widerstandsänderungen des Selen's oder Chlorsilbers²⁾, den Einfluß des Lichtes auf elektrische Funkenentladung³⁾ und die photoelektrischen (Becquerel'schen⁴⁾) Ströme nennen.

Die Schwierigkeit der Untersuchung stehender Lichtwellen beruht hauptsächlich in zwei Punkten: einmal muß der Körper, durch dessen Verhalten die Wirkung der Bäuche und Knoten der stehenden Lichtwelle untersucht werden soll, dünn sein im Vergleich

1) O. Wiener, Wied. Ann. 40, p. 203, 1890.

2) Sr. Arrhenius, Wiener Ber. 96, p. 831. 1887.

3) H. Hertz, Wied. Ann. 31, p. 983, 1887.

4) Ed. Becquerel, La lumière, T. 2, p. 121, Paris 1868.