Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 38 (1983)
Heft: 6

Artikel: Über eine Formel für primitive Kongruenzwurzeln
Autor: Bergmann, Horst
DOI: https://doi.org/10.5169/seals-37197

Die Gleichungen der Steinerellipsen sind
Umellipse: $7x^2-3xy+3y^2=25$,
Inellipse: $28x^2-12xy+12y^2=25$
Man verifiziert leicht, dass die Punkte A, B und C auf der Umellipse und die Seitenmitten auf der Inellipse liegen. Die Dreiecksmatrix

$$U=\begin{pmatrix} \sqrt{6} & 0 \\ \frac{1}{2}\sqrt{6} & \frac{5}{2}\sqrt{2} \end{pmatrix}$$

erfüllt die Gleichung $S=UU'$, und $\vec{x}=U^{-1}\vec{y}$ transformiert das Dreieck auf

$$A^*\left(\frac{\sqrt{6}}{6},\frac{\sqrt{2}}{2}\right),\qquad B^*\left(\frac{\sqrt{6}}{6},-\frac{\sqrt{2}}{2}\right),\qquad C^*\left(-\frac{\sqrt{6}}{3},0\right).$$

Dieses Dreieck ist gleichseitig und hat die Seitenlänge $\sqrt{2}$.

Peter Nüesch, Département de Mathématiques, ETH-Lausanne

LITERATURVERZEICHNIS

1 A.P. Dempster: Elements of continuous multivariate Analysis. Addison-Wesley, Reading, Mass., 1969.
2 J. Steiner: Gesammelte Werke. Herausgegeben von K. Weierstrass, 2. Auflage. Chelsea Publishing Co., New York, N.Y., 1971.

 0013-6018/83/060137-06$1.50+0.20/0

Über eine Formel für primitive Kongruenzwurzeln

Zu jeder ungeraden Primzahlpotenz p^a gibt es genau $\phi(\phi(p^a))$ Primitivwurzeln $\bmod p^a$, wobei $\phi(n)$ die Eulersche ϕ-Funktion ist. Kennt man eine Primitivwurzel ω für die ungerade Primzahl p, so lässt sich eine Primitivwurzel $\bmod p^a$ sofort explizit angeben: Die Zahl

$$\omega^*=\omega^{p^{a-1}}(1+p)$$

ist dann Primitivwurzel $\bmod p^a$.
Zur Ermittlung von Primitivwurzeln $\bmod p$ schreibt H. Hasse ([2], S. 68): «Ein systematisches Rechenverfahren zur Bestimmung einer primitiven Wurzel $\bmod p$, etwa der kleinsten, ist nicht bekannt. Man ist dazu auf Probierverfahren angewiesen.» – Nach der Angabe eines Probierverfahrens zur Gewinnung von

Primitivwurzeln mod p bemerkt D. Shanks ([4], S. 79): "Gauss, and others, have devised more efficient techniques, but no general, *explicit*, *nontentative* method has been devised, and this, like a good criterion for primality, remains an important unsolved problem."
Für spezielle Primzahlen p von besonderer Gestalt lassen sich dagegen Primitivwurzeln mod p explizit angeben. Beispielsweise[1]) ist ± 6 Primitivwurzel mod p für alle Primzahlen der Form $p = 8q + 1$ mit ungerader Primzahl q.
Analog zu der Frage nach einer Formel[2]) für die n-te Primzahl p_n stellt sich die Aufgabe, eine Formel für Primitivwurzeln mod p zu finden.
Es soll jetzt gezeigt werden:

Satz. *Für jede ungerade Primzahl p stellt die ganze Zahl*

$$\omega_p = \sum_{r=2}^{p-1} r P_r \prod_{s=1}^{r-1} (1 - P_s) \quad mit \quad P_t = \prod_{\mu=1}^{p-2} (t^\mu - 1) \tag{1}$$

stets eine Primitivwurzel mod p *dar.*

Beweis: Für ganze Zahlen a und ungerade Primzahlen p sei das Symbol $(a)_p$ definiert durch:

$$(a)_p = \left\{ \begin{array}{l} 1, \text{ wenn } p \nmid a \text{ und } a \text{ Primitivwurzel mod } p \\ 0, \text{ wenn } p \nmid a \text{ und } a \text{ nicht Primitivwurzel mod } p \\ -1, \text{ wenn } p \mid a \end{array} \right\}.$$

Unter Heranziehung des Wilsonschen Satzes

$$(p-1)! \equiv -\prod_{k=2}^{p-1} (k-1) \equiv -1 \bmod p \qquad (p > 2)$$

lässt sich damit das Primitivwurzel-Kriterium

$$(a)_p \equiv \prod_{\mu=1}^{p-2} (a^\mu - 1) \bmod p \qquad (p > 2) \tag{2}$$

herleiten.
Man betrachtet jetzt die zahlentheoretische Funktion

$$F(r) = \frac{1}{2} (r)_p \prod_{s=0}^{r-1} \left(1 - (s)_p\right) \qquad (r \geqq 1). \tag{3}$$

1) Vergleiche dazu [1].
2) Man vergleiche etwa [3], S. 12 und 165.

Bezeichnet man mit $\tilde{\omega}_p$ die kleinste positive Primitivwurzel mod p, so gilt offensichtlich

$$F(r)=\begin{Bmatrix} 0, \text{ wenn } 1 \leqq r \leqq \tilde{\omega}_p - 1 \\ 1, \text{ wenn } r = \tilde{\omega}_p \\ 0, \text{ wenn } \tilde{\omega}_p + 1 \leqq r \leqq p \end{Bmatrix}.$$

Daraus folgt aber

$$\tilde{\omega}_p = \sum_{r=2}^{p-1} r F(r). \tag{4}$$

Aus (2), (3) und (4) ergibt sich schliesslich die Behauptung des Satzes.
Zur *praktischen* Berechnung einer Primitivwurzel mod p ist die Formel (1) nicht geeignet. Vom *theoretischen* Standpunkt aus betrachtet, kann aber aufgrund von (1) die Frage nach der Existenz eines systematischen Rechenverfahrens zur Bestimmung einer Primitivwurzel mod p im positiven Sinne entschieden werden.

Horst Bergmann, Hamburg

LITERATURVERZEICHNIS

1 A. Ecker: On primitive roots. El. Math. *37*, 103–108 (1982).
2 H. Hasse: Vorlesungen über Zahlentheorie. Springer, Berlin, Göttingen, Heidelberg 1950.
3 K.-H. Indlekofer: Zahlentheorie. Birkhäuser, Basel, Stuttgart 1978.
4 D. Shanks: Solved and unsolved Problems in Number Theory, Vol. I. Washington 1962.

 0013-6018/83/060142-03$1.50+0.20/0

Integralungleichungen aus der Hilbertraum-Theorie

In [3], S. 62, wird folgende Aufgabe gestellt:
Die Funktion $f:[0,1]\to\mathbf{R}$ sei stetig differenzierbar, und es gelte $f(0)=f(1)=0$. Man zeige

$$\left(\int_0^1 f(x)\,dx\right)^2 \leq \frac{1}{12}\int_0^1 [f'(x)]^2\,dx.$$

Wann genau gilt Gleichheit?
Der Aufgabensteller verallgemeinert das Problem in [4], S. 380–381, Aufgabe P. 326: Es sei f eine reellwertige n-mal stetig differenzierbare Funktion auf $[0,1]$ mit $f^{(k)}(0) = f^{(k)}(1) = 0\,(k=0,1,\ldots,n-1)$. Man zeige

$$\left(\int_0^1 f(x)\,dx\right)^2 \leq (n!)^2 (2n+1)^{-1} \left((2n)!\right)^{-2} \int_0^1 [f^{(n)}(x)]^2\,dx$$