

Werk

Titel: Über die Nichtprimteiler von $abx + c$.

Autor: Trost, E.; Jaeschke, G.

Jahr: 1966

PURL: https://resolver.sub.uni-goettingen.de/purl?378850199_0021 | log15

Kontakt/Contact

[Digizeitschriften e.V.](#)
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

✉ info@digizeitschriften.de

Analog kann der Beweis für die Gerade $M \mathfrak{L}$ bzw. für Hyperbeln mit gemeinsamem Krümmungselement geführt werden. Die hier angegebene Konstruktionsvorschrift \mathfrak{B} dürfte wohl gleichzeitig eine bisher unbekannte Erzeugungsweise von Steinerzykloiden sein.

J. HOSCHEK, TH Darmstadt

LITERATURVERZEICHNIS

- [1] J. HOSCHEK, *Über Kegelschnitte mit gemeinsamem Krümmungselement*, erscheint demnächst in *Elemente der Mathematik*.
- [2] W. KICKINGER, *Einfacher Beweis eines Satzes von F. Laurenti über Parabeln mit gemeinsamem Krümmungselement*, *Elemente der Mathematik* 18, S. 28–29, 1963.
- [3] F. LAURENTI, *Sopra una proprietà dell'ipocicloide tricuspidata*, *Periodico Mat. IV. Ser. 38*, 155–158, (1960).
- [4] F. LAURENTI, *Sopra una proprietà dell'ipocicloide tricuspidata*, *Archimede* 12, 253–256, (1960).
- [5] J. STEINER, *Vorlesungen über synthetische Geometrie*, Leipzig 1898.
- [6] H. SCHMIDT, *Ausgewählte höhere Kurven*, Wiesbaden 1949.

Über die Nichtprimteiler von $a b^x + c$

Die Primzahl p wird Primteiler der ganzwertigen Funktion $g(x)$ genannt, wenn die Kongruenz $g(x) \equiv 0 \pmod{p}$ eine ganzzahlige Lösung n mit $g(n) \neq 0$ hat. Ist die Kongruenz nicht lösbar, so heisst p Nichtprimteiler (NP) von $g(x)$.

PÓLYA [1] hat gezeigt, dass für ganze a, b, c mit $a c \neq 0, b \geq 2$ die Funktion $g_0(x) = a b^x + c$ unendlich viele Primteiler besitzt. Für die NP von $g_0(x)$ gibt es keine so allgemeine Aussage. Beispielsweise sind nach dem Fermatschen Satz die Primteiler von b die einzigen NP von $b^x - 1$. Für die Existenz von unendlich vielen NP von $g_0(x)$ ist somit eine Zusatzbedingung notwendig, die im Fall $a = 1$ nach SCHINZEL [2] $-c \neq b^k$ lautet. Eine Aussage über die Form der NP gibt der

Satz 1. Ist $(a c, b) = 1, b \geq 2$ und $|a c| \neq u^2$, so ist die Anzahl der NP von $a b^x + c$ in jeder der Restklassen $\pm 1 \pmod{4}$ unendlich¹⁾.

Wird der Definitionsbereich von $g_0(x)$ auf die ungeraden Zahlen beschränkt, so gilt der

Satz 2. Ist $(a c, b) = 1, b \geq 2$ und $b \neq b_1^2$, so ist die Anzahl der NP von $a b^{2x+1} + c$ in jeder der Restklassen $\pm 1 \pmod{4}$ unendlich.

Ohne Einschränkung von b ist Satz 2 nicht richtig. Jede Primzahl $p \equiv 3 \pmod{4}$ ist nämlich Primteiler von

$$4^{2x+1} - 1 = (2^{2x+1} + 1) (2^{2x+1} - 1) = (2^{(p-1)/2} + 1) (2^{(p-1)/2} - 1).$$

Lemma 1. $p \neq 2, (p, a b c) = 1, (b/p) = 1, (-a c/p) = -1 \Rightarrow p = \text{NP von } g_0(x)$.
Beweis indirekt (Kongruenzen mod p):

$$b \equiv b_0^2, a b^n + c \equiv 0 \Rightarrow a^2 b_0^{2n} + a c \equiv 0, -a c \equiv (a b_0^n)^2, (-a c/p) = 1 \text{ Widerspruch!}$$

¹⁾ Sind b und $a c$ Quadratzahlen, so ist (nach Lemma 1) jedes $a b c$ nicht teilende $p \equiv -1 \pmod{4}$ ein NP von $g_0(x)$. Ist b ein Quadrat, so ist die Bedingung $(a c, b) = 1$ überflüssig, da Satz 1 sofort aus Lemma 1 und Lemma 3 folgt. Ebenso erhält man für $a c = u^2$ und beliebiges $b \geq 2$ unendlich viele NP der Form $4m + 3$

Lemma 2 (Verallgemeinerter chinesischer Restsatz). Das Kongruenzsystem $x \equiv r_i \pmod{m_i}$ ($i = 1, 2, \dots, s$) ist dann und nur dann lösbar, wenn $r_i \equiv r_j \pmod{(m_i, m_j)}$ ($j = 1, 2, \dots, s$). Zwei Lösungen sind mod $\{m_1, m_2, \dots, m_s\}$ kongruent ($\{\} =$ k.g. V.).

Beweis: Siehe [3].

Lemma 3. Ist die natürliche Zahl n kein Quadrat, so gibt es in jeder der Restklassen $\pm 1 \pmod{4}$ unendlich viele Primzahlen mit der Eigenschaft $(n/p) = e$ ($e = 1$ oder -1).

Beweis: $k(n) = 2^\alpha q_1 q_2 \dots q_s$ ($\alpha = 0$ oder 1) sei der «quadratfreie Kern» von n , das ist das Produkt der verschiedenen Primzahlen, die in n mit ungeraden Exponenten aufgehen.

a) $p \equiv 1 \pmod{4}$, $e = 1$. Wir wählen je einen quadratischen Rest $r_i \pmod{q_i}$. Für $\alpha = 1$ benutzen wir noch $(2/p) = 1$ für $p \equiv 1 \pmod{8}$. Das System

$$x \equiv r_i \pmod{q_i} \quad (i = 1, 2, \dots, s), \quad x \equiv 1 \pmod{8}, \quad x \equiv 1 \pmod{4}$$

ist nach Lemma 2 lösbar und die Lösungen sind die Elemente einer primen Restklasse mod $8 q_1 q_2 \dots q_s$ (mod $4 q_1 q_2 \dots q_s$ im Fall $\alpha = 0$). Nach dem Satz von DIRICHLET über die arithmetische Progression enthält diese Restklasse unendlich viele Primzahlen p^* . Aus dem quadratischen Reziprozitätsgesetz folgt nun

$$\left(\frac{n}{p^*}\right) = \left(\frac{2}{p^*}\right)^\alpha \left(\frac{q_1}{p^*}\right) \left(\frac{q_2}{p^*}\right) \dots \left(\frac{q_s}{p^*}\right) = \left(\frac{2}{p^*}\right)^\alpha \left(\frac{p^*}{q_1}\right) \left(\frac{p^*}{q_2}\right) \dots \left(\frac{p^*}{q_s}\right) = 1. \quad (1)$$

b) $p \equiv 1 \pmod{4}$, $e = -1$. Ist $k(n) \neq 2$, so wähle man anstelle von r_1 einen Nichtrest n_1 . Im Fall $k(n) = 2$ hat man das System $x \equiv 1 \pmod{4}$, $x \equiv 5 \pmod{8}$ zu erfüllen, was nach Lemma 2 möglich ist.

c) $p \equiv 3 \pmod{4}$, $e = 1$. Für $q_j \equiv 3 \pmod{4}$ ist jetzt in (1) $(q_j/p) = -(p/q_j)$. Das zu lösende System lautet also hier $x \equiv r_i \pmod{q_i}$ ($q_i \equiv 1 \pmod{4}$), $x \equiv n_j \pmod{q_j}$ ($q_j \equiv 3 \pmod{4}$), $x \equiv -1 \pmod{8}$, $x \equiv 3 \pmod{4}$.

d) $p \equiv 3 \pmod{4}$, $e = -1$. Ist $k(n) \neq 2$, so ersetze man r_1 bzw. n_1 durch n_1 bzw. r_1 . Im Fall $k(n) = 2$ hat man das lösbare System $x \equiv 3 \pmod{4}$, $x \equiv -5 \pmod{8}$.

Beweis von Satz 1: a) $p' \equiv 1 \pmod{4}$ bzw. $p'' \equiv 1 \pmod{4}$ sei je eine Lösung von $(b/p) = 1$ bzw. $(-a c/p) = (a c/p) = -1$ im Sinn von Lemma 3. Die Moduln M_1 bzw. M_2 der beiden Lösungsrestklassen haben wegen $(k(b), k(a c)) = 1$ höchstens 4 als gemeinsamen Faktor. Ferner ist $p' \equiv p'' \pmod{4}$. Somit hat das System $x \equiv p' \pmod{M_1}$, $x \equiv p'' \pmod{M_2}$ nach Lemma 2 eine prime Restklasse mod $\{M_1, M_2\}$ als Lösung. Damit sind unendlich viele NP der Form $4 m + 1$ von $g_0(x)$ gefunden.

b) $p' \equiv 3 \pmod{4}$ bzw. $p'' \equiv 3 \pmod{4}$ sei eine Lösung von $(b/p) = 1$ bzw. $(a c/p) = 1$. Wie in a) erhält man unendlich viele NP der Form $4 m + 3$ von $g_0(x)$.

Beweis von Satz 2. Im Fall $|a c| \neq u^2$ ist nichts zu beweisen, denn jeder NP von $g_0(x)$ ist erst recht NP von $g_1(x) = a b^{2x+1} + c$. Es sei also $|a c| = u^2$. Dann ist $|a b c| \neq v^2$, somit können wir Satz 1 auf $a b (b^2)^x + c$ anwenden (vgl. Fussnote 1). Ohne die Restklassenaussage lässt sich Satz 2 folgendermassen gewinnen: Wir nehmen an, dass $g_1(x)$ nur endlich viele NP besitze. Dann ist die Kongruenz

$$a b g_1(x) = a^2 b^{2x+2} + a b c \equiv 0 \pmod{p} \quad (2)$$

für «fast alle» p lösbar, das heisst die Menge der Ausnahmeprimzahlen ist endlich. Ist w eine Primitivwurzel mod p und $a \equiv w^\alpha$, $b \equiv w^\beta$, $-a b c \equiv w^\gamma$, so ergibt sich aus (2)

$$2\alpha + (2x+2)\beta \equiv \gamma \pmod{p-1}. \quad (3)$$