

Werk

Titel: Mathematische Zeitschrift

Ort: Berlin

Jahr: 1918

Kollektion: Mathematica

Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen

Werk Id: PPN266833020_0001

PURL: http://resolver.sub.uni-goettingen.de/purl?PPN266833020_0001

LOG Id: LOG_0020

LOG Titel: Zur arithmetischen Untersuchung der Polynome

LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN266833020

PURL: <http://resolver.sub.uni-goettingen.de/purl?PPN266833020>

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Zur arithmetischen Untersuchung der Polynome.

Von

Georg Pólya in Zürich.

§ 1.

Es sei $f(x)$ eine ganze rationale Funktion mit ganzen rationalen Koeffizienten, n eine Zahl der Folge $0, 1, 2, 3, \dots$ und P_n der größte Primfaktor der Zahl $f(n)$. Ein längst bekannter, elementarer Satz¹⁾ der Zahlentheorie läßt sich auf folgende Form bringen: für jede nicht-konstante ganze rationale Funktion $f(x)$ ist

$$(1) \quad \lim_{n \rightarrow \infty} P_n = \infty.$$

Herr Störmer²⁾ hat (1) für drei spezielle Funktionen $f(x)$, nämlich für

$$(2) \quad x(x+1), \quad x(x+2), \quad x^2+1$$

bedeutend verschärft, indem er es durch

$$(3) \quad \lim_{n \rightarrow \infty} P_n = \infty$$

ersetzen konnte.

Herr Thue³⁾ hat mit Hilfe seines bekannten, wichtigen Satzes über Diophantische Gleichungen das Resultat von Herrn Störmer, in-

¹⁾ Dies kommt bei dem bekannten elementaren Beweis für die Existenz unendlich vieler Primzahlen in arithmetischen Progressionen mit dem Anfangsgliede $+1$ vor. Vgl. etwa J. Schur, Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen. Sitzungsberichte der Berliner Math. Gesellschaft, 11. Jahrg. (1912), S. 40 bis 50.

²⁾ Carl Störmer, Sur une équation indéterminée, C. R. 127 (1898), S. 752 bis 754.

³⁾ Axel Thue, I. Bemerkungen über gewisse Näherungsbrüche algebraischer Zahlen. Skrifter af Videnskabs-Selskabet i Christiania 1908, Nr. 3. — II. Om en general i store hele tal uløslar ligning, ebendasselbst, Nr. 7. — III. Über Annäherungswerte algebraischer Zahlen. Journ. für Mathematik 135 (1909), S. 284 bis 305.

soweit es die beiden ersten Polynome (2) betrifft, weitgehend verallgemeinert. Sein Resultat läßt sich so aussprechen:

Satz I. *Ist $f(x)$ das Produkt zweier wesentlich verschiedenen, d. h. nicht nur um eine multiplikative Konstante verschiedenen rationalen Linearfaktoren, so gilt (3).*

Ist $f(x)$ das Produkt zweier nur unwesentlich verschiedenen Linearfaktoren, oder hat es allgemeiner die Form

$$(4) \quad c(ax + b)^m,$$

so ist (3) offenbar ungültig. [Den Fall $b = 0$ beiseite gelassen, kann

$$(a, b) = 1, \quad a \geq 1, \quad b > a$$

vorausgesetzt werden. Setzt man

$$n = \frac{b}{a} (b^{v(a)^v} - 1),$$

wo $v = 1, 2, 3, \dots$, so wird P_n die größte in bc aufgehende Primzahl sein, also für unendlich viele n denselben Wert behalten.]

Welche Polynome sind es, für die (3), und welche sind es, für die nur (1) gültig ist? Ich will nicht auf naheliegende Vermutungen eingehen, ich begnüge mich heute damit, zu der aufgeworfenen Frage mit dem Beweise folgenden Satzes beizutragen:

Satz II. *Ist $f(x)$ ein irreduzibles Polynom vom zweiten Grade, so gilt (3).*

Satz II enthält das Resultat von Herrn Störmer über das letzte der Polynome (2).

§ 2.

Man verdankt Herrn Thue⁴⁾ den folgenden wichtigen Satz:

„Es sei $F(x, y)$ eine irreduzible homogene binäre Form vom dritten oder höheren Grade mit ganzen rationalen Koeffizienten. Dann hat die Diophantische Gleichung

$$(5) \quad F(x, y) = c$$

nur endlich viele verschiedene ganzzahlige Lösungen.“

Demselben Satze hat Herr Thue⁵⁾ noch die folgende Fassung gegeben:

„Ist $c \geq 0$ und hat die Diophantische Gleichung (5) unendlich viele ganzzahlige Lösungen, so muß die binäre Form $F(x, y)$ Potenz einer

⁴⁾ Vgl. loc. cit. ³⁾ III, Theorem IV, S. 303.

⁵⁾ Vgl. loc. cit. ³⁾ II, S. 3.

Linearform oder einer indefiniten quadratischen Form sein, oder sie unterscheidet sich nur um eine multiplikative Konstante von einer solchen Potenz.“

Diese zweite Fassung ist leicht aus der ersten herzuleiten. —

Der Beweis des Satzes I erfolgt nun so ⁶⁾: die beiden linearen Funktionen $ax + b$ und $cx + d$ seien wesentlich verschieden, d. h. es sei

$$(6) \quad \frac{b}{a} \neq \frac{d}{c}.$$

Man bezeichne mit P_n den größten Primfaktor der beiden Zahlen $an + b$ und $cn + d$. Wäre (3) falsch, so könnte man gewisse endlich viele Primzahlen

$$(7) \quad p_1, p_2, \dots, p_l$$

und unendlich viele Werte n finden, für welche $(an + b)(cn + d)$ durch keine von den Primzahlen (7) verschiedene Primzahl teilbar wäre. Für diese n wäre

$$(8) \quad an + b = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}, \quad cn + d = p_1^{c_1} p_2^{c_2} \dots p_l^{c_l}.$$

Man reduziere $a_1, \dots, a_l, c_1, \dots, c_l \pmod{3}$. Aus (8) folgt dann

$$an + b = p_1^{r_1} p_2^{r_2} \dots p_l^{r_l} x^3, \quad cn + d = p_1^{s_1} p_2^{s_2} \dots p_l^{s_l} y^3$$

$$(r_1, \dots, r_l, s_1, \dots, s_l = 0, 1 \text{ oder } 2),$$

wo für das Zahlensystem $r_1, \dots, r_l, s_1, \dots, s_l$ nur endlich viele [nämlich 3^{2l}] Möglichkeiten bestehen.

Jedes n der fraglichen Art liefert uns eine Lösung x, y einer Diophantischen Gleichung von der Form

$$a p_1^{s_1} p_2^{s_2} \dots p_l^{s_l} y^3 - c p_1^{r_1} p_2^{r_2} \dots p_l^{r_l} x^3 = ad - bc.$$

Die rechte Seite ist nach (6) von 0 verschieden. Die linke Seite ist nicht die dritte Potenz einer Linearform von x, y . Die Annahme, daß unendlich viele n der fraglichen Art existieren, führt also auf einen Widerspruch mit der zweiten Fassung des Thueschen Satzes, und somit ist Satz I bewiesen.

Dieses Beweisverfahren von Herrn Thue bedarf nur einiger Modifikation, um auch den Satz II mit seiner Hilfe zu erhalten.

§ 3.

Wäre der Satz II für das Polynom

$$f(x) = ax^2 + bx + c$$

⁶⁾ Vg. loc. cit. ⁵⁾ I, Satz 12, S. 30.

falsch, so wäre er auch für das Polynom

$$f^*(x) = x^2 + bx + ac$$

falsch, wegen der Identität

$$af(x) = f^*(ax).$$

Ich kann also von vornherein den höchsten Koeffizienten von $f(x)$ als 1 annehmen, d. h.

$$f(x) = (x - \alpha)(x - \alpha')$$

setzen, wo α und α' konjugierte ganze algebraische Zahlen zweiten Grades bedeuten. Ich will ferner beim Beweise den Fall vor Augen behalten, wo α und α' reell sind. [Dieser Fall ist etwas verwickelter, wegen der unendlich vielen Einheiten im reellen quadratischen Körper.]

Ich habe einen Widerspruch aus der Annahme abzuleiten daß es unendlich viele rationale ganze n gibt, für welche $f(n) = (n - \alpha)(n - \alpha')$ außer den Primzahlen

$$(9) \quad p_1, p_2, \dots, p_r$$

keine andere Primfaktoren hat.

Die Wurzeln α und α' von $f(x)$ sollen im Körper liegen, der durch $\sqrt{D}$ erzeugt ist. Es seien in diesem Körper:

$1, \omega$ eine Basis der ganzen Zahlen,

h die Klassenanzahl,

ε die Grundeinheit,

$p_1, p_2, \dots, p_l$ sämtliche Primidealteiler der Primzahlen (9).

Konjugierte Größen werden durch Akzent unterschieden: α und α' , β und β' , p und p' usw.

Ich habe einen Widerspruch aus der Annahme zu folgern, daß für unendlich viele rationale ganze n das Ideal $(n - \alpha)$ eine Zerlegung der Art

$$(n - \alpha) = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$$

zuläßt. Ich setze

$$(n - \alpha) = p_1^{r_1} p_2^{r_2} \dots p_l^{r_l} r^{3h},$$

wo

$$0 \leq r_1 < 3h, \quad 0 \leq r_2 < 3h, \quad \dots \quad 0 \leq r_l < 3h.$$

r^{3h} ist die dritte Potenz eines gewissen Hauptideals $(x + \omega y)$. Daher ist

$$(10) \quad n - \alpha = \beta (x + \omega y)^3,$$

wo β eine gewisse ganze Zahl des Körpers ist. Für das Ideal (β) bestehen höchstens $3^l h^l$ verschiedene Möglichkeiten, denn dies ist die Anzahl der möglichen Zahlssysteme $r_1, r_2, \dots, r_l$. Ein bestimmtes Ideal (β)

muß in (10) nur durch 6 verschiedene Zahlen vertreten werden, nämlich durch die Zahlen

$$\beta, \varepsilon \beta, \varepsilon^2 \beta, -\beta, -\varepsilon \beta, -\varepsilon^2 \beta.$$

Kurzum, es genügt zu beweisen, daß für gegebenes β die Gleichung (10) nicht unendlich viele verschiedene Auflösungen in rationalen ganzen Zahlen n, x, y haben kann. Aus

$$n - \alpha = \beta (x + \omega y)^3$$

$$n - \alpha' = \beta' (x + \omega' y)^3$$

folgt aber

$$(11) \quad \frac{\alpha' - \alpha}{\omega' - \omega} = \frac{\beta (x + \omega y)^3 - \beta' (x + \omega' y)^3}{\omega' - \omega} = F(x, y),$$

wo $F(x, y)$ eine homogene binäre Form dritten Grades mit ganzen rationalen Koeffizienten bedeutet. $F(x, y)$ ist nicht die dritte Potenz einer Linearform, denn die drei Wurzeln der Gleichung

$$F(z, 1) = 0,$$

d. h. der Gleichung

$$\left(\frac{z + \omega}{z + \omega'} \right)^3 = \frac{\beta'}{\beta}$$

sind alle verschieden. So folgt aus dem Thueschen Satze, daß die Diophantische Gleichung (11) nicht unendlich viele Auflösungen haben kann, und damit die Richtigkeit unseres Satzes II.

Aus den Thueschen Resultaten über Diophantische Gleichungen ergibt sich noch, daß (3) auch für das Polynom $x^n - 1$ Gültigkeit behält, oder allgemeiner für solche Polynome, bei welchen eine gewisse Anzahl Koeffizienten, die dem höchsten Gliede folgen, $= 0$ sind⁷⁾. Die volle Entscheidung der im § 1 aufgeworfenen allgemeineren Frage ist aber wohl aus einer anderen Quelle zu schöpfen.

§ 4.

Ich will noch den Satz I in einer anderen Fassung aussprechen und daran einige Bemerkungen knüpfen.

Es seien

$$(12) \quad p_1, p_2, \dots, p_r$$

r gegebene Primzahlen, $r \geq 2$. Man erteile in dem Ausdruck

$$p_1^{x_1} p_2^{x_2} \dots p_r^{x_r}$$

$x_1, x_2, \dots, x_r$ alle mögliche nichtnegative ganzzahlige Wertsysteme. Die

⁷⁾ Vgl. loc. cit. *) III, S. 304.

so erhaltenen ganzen Zahlen, nach aufsteigender Größe geordnet, bezeichne man mit

$$(13) \quad \alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n, \dots$$

Satz I' ist dann äquivalent mit der Tatsache

$$(14) \quad \lim_{n=\infty} (a_{n+1} - a_n) = \infty.$$

Denn wäre $\lim_{n=\infty} \inf. (a_{n+1} - a_n) = k$, so wäre (3) für das Polynom $x(x+k)$ ungültig. Umgekehrt ist leicht einzusehen, daß Satz I nur für die Polynome $x(x+k)$ bewiesen zu werden braucht.

Nun lassen sich (14) noch folgende Eigenschaften der Zahlen $\alpha_0, \alpha_1, \alpha_2, \dots$ zur Seite stellen:

$$(15) \quad \lim_{n=\infty} \frac{\alpha_{n+1}}{\alpha_n} = 1,$$

$$(16) \quad \lim_{n=\infty} \frac{(\log \alpha_n)^r}{n} = 1 \cdot 2 \dots r \log p_1 \log p_2 \dots \log p_r.$$

Diese Eigenschaften tragen zur besseren Auffassung von (14) bei, liegen aber viel weniger tief. Die Gleichung (15) beruht darauf, daß die Linearform

$$x_1 \log p_1 + x_2 \log p_2 + \dots + x_r \log p_r$$

der ganzzahligen Variablen $x_1, x_2, \dots, x_r$ nie verschwinden kann (abgesehen von $x_1 = x_2 = \dots = x_r = 0$) und folglich beliebig kleine Werte annimmt. Die Formel (16) folgt aus der Abzählung der Gitterpunkte in dem durch die $r+1$ Ungleichungen

$x_1 \geq 0, x_2 \geq 0, \dots, x_r \geq 0, x_1 \log p_1 + x_2 \log p_2 + \dots + x_r \log p_r \leq \log \alpha_n$ abgegrenzten, abgeschlossenen, ebenwändigen, r -dimensionalen Bereich.

(Eingegangen am 4. August 1917.)