REVUE DE MATHÉMATIQUES
PURES ET APPLIQUÉES
Tome I, 1956, N° 3

ÜBER ARITHMETISCHE EIGENSCHAFTEN DER SUBSTITUTIONSWERTE EINES POLYNOMS FÜR GANZZAHLIGE WERTE DES ARGUMENTS *)

VON

P. ERDÖS

(Budapest)

Es sei $f(x)$** ein irreduzibles Polynom mit ganzzahligen Koeffizienten, $\nu(p)$ bedeute die Anzahl der Lösungen der Kongruenz

$$f(n) \equiv 0 \pmod{p} \quad , \quad 0 \leqslant n < p \qquad (p \text{ Primzahl}).$$

Man kann bekanntlich den Primidealsatz in folgender Form aussprechen:

$$\sum_{p<x} \nu(p) = (1 + o(1)) \frac{x}{\log x} . \tag{1}$$

Wenn $f(x) = x$, so ist $\nu(p) = 1$ für alle p, also ist (1) eine Verallgemeinerung des Primidealsatzes ***). Im folgenden will ich einige Probleme und Resultate diskutieren, dit mit (1) zusammenhängen.

Natürlich erhebt diese Arbeit keineswegs Anspruch auf Vollständigkeit, ich diskutiere hier nur diejenigen Probleme, mit denen ich mich in den letzten zehn Jahren beschäftigt habe. Am Ende der Arbeit betrachte ich auch einige Fragen, die mit (1) nicht zusammenhängen.

1. HARDY und RAMANUJAN ****) haben folgenden Satz bewiesen:

---

*) Vortrag auf dem IV. rumänischen Mathematikerkongress. Bukarest. 27. Mai – 4. Juni 1956.

**) In dieser Arbeit wird $f(x)$ immer ein irreduzibles Polynom mit ganzzahligen Koeffizienten bedeuten.

***) Vor einigen Jahren bewies SHAPIRO, mit Selbergs und meiner Methode, den Primidealsatz elementar. SHAPIROS Beweis benützt aber, wie jeder andere Beweis von (1), die Idealtheorie. Es wäre interessant (1) nicht nur ohne analytische Methoden, sondern auch ohne Idealtheorie zu beweisen. Vielleicht ist dies aber nicht möglich (SHAPIRO, Communications on pure and applied Mathematics, 1949, **2**, S. 309–323).

****) S. RAMANUJAN, *Collected Papers*, S. 262–275.

Es sei $V(n)$ die Anzahl der verschiedenen Primfaktoren von n, dann strebt für fast alle Zahlen n $V(n)/\log\log n$ gegen 1, oder präziser ausgedrückt: Es sei $g(n)\to\infty$ eine beliebige Funktion, dann ist die Anzahl der Zahlen $n\leqslant x$ für welche entweder

$$V(n) < \log\log n - g(n)\ (\log\log n)^{1/2},$$

oder

$$V(n) > \log\log n + g(n)\ (\log\log n)^{1/2}$$

gilt, $o(x)$.

TURAN *) fand einen sehr einfachen Beweis für diesen Satz. In einer späteren Arbeit bewies er folgende Verallgemeinerung **):

Die Anzahl der Zahlen $n\leqslant x$ für welche entweder

$$V(f(n)) < \log\log n - g(n)(\log\log n)^{1/2},$$

oder

$$V(f(n)) > \log\log n + g(n)(\log\log n)^{1/2}$$

gilt, ist $o(x)$.

Ich bewies ***), daß die Anzahl der Primzahlen $p<x$, für welche

$$V(p-1) < (1-\varepsilon)\log\log p,$$

oder

$$V(p-1) > (1+\varepsilon)\log\log p$$

gilt, $o\left(\frac{x}{\log x}\right)$ ist.

M. KAC und ich ****) bewiesen mit Hilfe der Brunschen Methode und des zentralen Grenzwertsatzes der Wahrscheinlichkeitsrechnung, daß die Dichte der Zahlen $n<x$, für welche

$$V(n) < \log\log n + c\sqrt{\log\log n}$$

gilt, $\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{c} e^{-x^2/2}\,dx$ ist. Offenbar enthält unser Satz den Satz von Hardy und Ramanujan. KAC und ich bewiesen einen viel allgemeineren Satz, aber darüber wollen wir hier nicht sprechen.

HALBERSTAM *****) bewies kürzlich mit anderen Methoden folgende allgemeinere Sätze: Die Dichte der Zahlen $n\leqslant x$, für welche

$$V(f(n)) < \log\log n + c\sqrt{\log\log n}$$

gilt, ist $\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{c} e^{-x^2/2}dx$.

Die Anzahl der Primzahlen $p<x$, für welche

$$V(f(p)) < \log\log p + c\sqrt{\log\log p} \quad (f(x)\neq cx)$$

gilt, ist $\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{c} e^{-x^2/2}\,dx\,(1+o(1))\frac{x}{\log x}$.

*) Journal London Math. Soc., 1934, **9**, S. 274–276.
) *Ibid.*, 1936, **11, S. 125–133.
***) Quarterly Journal of Math., 1935, **6**, S. 205–213.
****) American Journal of Math., 1940, **42**, S. 738–742.
*****) Journal London Math. Soc., 1955, **30**, S. 43–53; *ibid.*, 1956, **31**, S. 1–27. HALBERSTAM verschärft ein früheres Resultat von PRACHAR *(ibid.*, 1953, **28**, S. 236–239).

2. VAN DER CORPUT *) bewies, daß ($d(n)$ ist die Anzahl der Teiler von n)

$$\sum_{n=1}^{x} d(f(n)) < c_1 x (\log x)^{c_2}.$$

Es wurde vermutet, daß

$$c_3 x \log x < \sum_{n=1}^{x} d f(n) < c_4 x \log x. \tag{2}$$

Die linke Seite von (2) ist eine leichte Konsequenz von (1), aber der Beweis der rechten Seite bereitete Schwierigkeiten. BELLMAN und SHAPIRO **) zeigten, daß wenn $f(x)$ von zweitem Grad ist, so gilt

$$\sum_{n=1}^{x} d(f(n)) = (2 + o(1)) x \log x. \tag{3}$$

Später gelang es mir (2) zu beweisen ***); der Beweis ist ziemlich kompliziert.

Es ist wohl anzunehmen, daß für Polynome $f(x)$ vom Grad k

$$\sum_{n=1}^{x} d(f(n)) = (c_k + o(1)) x \log x \tag{4}$$

ist, wo c_k vom Grade und vielleicht auch vom Polynom $f(x)$ abhängt [für $k = 2$ ist nach (3) $c_k = 2$]. Die größten Schwierigkeiten beim Beweis von (4) scheinen die großen Primfaktoren von $f(n)$ (d. h. die Primfaktoren, größer als x) zu bereiten, jedenfalls ist (4) bis heute nicht bewiesen.

Mit Hilfe der Brunschen Methode und der meinigen, mit welcher ich (2) bewies, kann ich zeigen****), daß

$$\sum_{p<x} d(f(p)) < c_5 x$$

gilt.

$$\sum_{p<x} d(f(p)) > c_6 x \quad (f(x) \neq c x)$$

ist bis jetzt unbewiesen selbst im Falle $f(x) = x - 1$ ****).

3. Eine alte Vermutung der Primzahltheorie besagt, daß der Ausdruck n^2+1 unendlich viele Primzahlen darstellt. Eine noch allgemeinere Vermutung besagt, daß es zu jedem $f(x)$ eine nur vom Grade abhängige Konstante c_k gibt, derart daß $f(n)=c_k p$ unendlich viele Lösungen hat. [$f(x)= x^2 + x+2$, welche für jedes n gerade ist, zeigt, daß man c_k nicht weglassen kann, da gewisse Polynome

*) Proc. K. Neder. Akad. van Wet., Amsterdam, 1939, **42**, S. 547–553.

**) Der Beweis wurde nicht veröffentlicht.

***) Journal London Math. Soc., 1952, **27**, S. 7–15.

****) Das beste Resultat in dieser Richtung stammt von HASELGROVE. Er bewies, daß $\sum_{p<x} d(p-1) > c\, x \log\log x$ gilt. (Journal London Math. Soc.). Aus der Riemannschen Hypothese würde $\sum_{p<x} d(p-1) > c\, x$ folgen (PITCHMASCH, Rend. del Circ. Mat. di Palermo, 1930, **54**, S. 414–419, siehe auch P. ERDÖS, Quarterly Journal of Math., 1935, **6**, S. 205–213.

konstante Primfaktoren besitzen können; es ist aber bekannt, daß ein derartiger konstanter Primfaktor ein Teiler von $k!$ sein muß, wo k den Grad des Polynoms $f(x)$ bezeichnet].

Bekanntlich bewies DIRICHLET, dass jede arithmetische Progression $ax+b$, mit $(a, b) = 1$ (also jedes irreduzible Polynom ersten Grades) unendlich viele Primzahlen darstellt. Es ist aber bis heute kein einziges Polynom vom Grade größer als 1 bekannt, welches unendlich viele Primzahlen darstellt.

Es ist bekannt, daß jedes irreduzible Polynom vom Grade k $(k>1)$ unendlich viele Zahlen darstellt, die durch keine k-te Potenz teilbar sind, und daß die Menge der Zahlen n, für welche $f(n)$ diese Eigenschaft hat, von positiver Dichte ist. Es wurde vermutet, daß jedes kubische Polynom $f(x)$ unendlich viele quadratfreie Zahlen darstellt. Vor einigen Jahren gelang es mir, diese Vermutung zu beweisen *). Allgemeiner bewies ich, daß jedes Polynom $f(x)$ vom Grade k $(k>2)$ unendlich viele Zahlen darstellt, die durch keine $(k-1)$-te Potenz teilbar sind. [Für $k = 2^l$ kann es vorkommen, dass $f(x)$ den konstanten Primfaktor 2^{k-1} hat, in diesem Falle gilt aber, daß $f(x)$ unendlich viele Zahlen von der Form $2^{k-1}u$ darstellt, wo u eine ungerade Zahl ist, die durch keine $(k-1)$-te Potenz teilbar ist. Mein Beweis ist ziemlich kompliziert, die eigentliche Schwierigkeit verursachen wieder die „grossen" Primzahlen (nämlich die Primzahlen $n < p < n^{1+1/k-1}$).

Man könnte vermuten, daß die Dichte der Zahlen n, für welche $f(n)$ durch keine $(k-1)$-te Potenz teilbar ist, positiv ist. Dies konnte ich aber nicht beweisen. Eine andere Vermutung wäre die Existenz von unendlich vielen Primzahlen p, für welche $f(p)$ durch keine $(k-1)$-te Potenz teilbar ist. Der Beweis ist mir ebenfalls nicht gelungen.

Es wurde auch mehrmals vermutet, daß jedes Polynom $f(x)$ [wenn man von den konstanten Primfaktoren absieht] unendlich viele quadratfreie Zahlen darstellt, aber schon für $k = 4$ scheinen meine Methoden ganz unbrauchbar zu sein.

4. TCHEBYCHEFF **) bewies folgenden Satz: P_x sei der größte Primfaktor des Produktes $\prod_{k=1}^{x} (1 + k^{\xi})$. Dann gilt $\lim P_{x/x} = \infty$. Später bewiesen NAGELL und RICCI ***) folgenden Satz: Es sei $g(x)$ ein nicht notwendig irreduzibles Polynom, welches nicht das Produkt von lauter linearen Faktoren ist, dann gilt $\left[P_x \text{ ist der größte Primfaktor von } \prod_{k=1}^{x} g(k)\right]$

$$P_x > c_6 x \log x.$$

Ich bewies, daß ****)

$$P_x > c_7 x (\log x)^{c_8 \log\log\log x}$$

*) Journal London Math. Soc., 1953, **28**, S. 417–425.

**) EDMUND LANDAU, *Verteilung der Primzahlen*, Vol. 1, 1909, S. 559–561.

***) NAGELL, Abh. Math. Sem. Hamburg, 1922, **1**, S. 179–194. Siehe auch G. RICCI, Annali de Mat., 1934, **12**, *4*, S. 295–303.

****) Journal London Math. Soc., 1952, **27**, S. 379–384.

gilt und mit ähnlichen aber komplizierteren Methoden kann ich

$$P_x > c_8 x e^{(\log x)^\alpha} \tag{5}$$

zeigen, wo $0 < \alpha < 1$ eine absolute Konstante ist. Den Beweis von (5) habe ich bis jetzt nicht publiziert.

Der sehr komplizierte Beweis von (5) könnte vereinfacht werden, wenn man folgenden kombinatorischen Satz beweisen könnte: zu jeder Konstante c_1 gibt es eine Konstante $c_2 (c_2$ unabhängig von $k)$, derart daß wenn $[c_2^k]$ Mengen $A_1, A_2, \ldots, A_t$, $t = [c_2^k]$, beliebig gegeben sind, wo jedes A k Elemente hat, wir immer c_1 Mengen $A_{i_1} \ldots A_{i_{c_1}}$ finden können, derart daß die Durchschnitte $A_{i_r} \cap A_{i_l}$, $1 \leqslant i < r \leqslant c_1$ alle gleich sind, RADO und ich konnten nur $k!\,(c_1-1)^k + 1$ anstatt $[c_2^k]$ beweisen.

Man würde wohl vermuten, daß $P_x > C_\varepsilon x^k$ ist, wo k das Maximum der Grade der in $g(x)$ aufgehenden irreduziblen Polynome ist, aber selbst der Beweis von

$$P_x > x^{1+\varepsilon}$$

scheint sehr schwierig zu sein. (5) ist wohl die „natürliche Grenze" meiner Methode.

(6) würde leicht folgen, wenn man zeigen könnte, daß die Anzahl der Zahlen $n \leqslant x$, für welche jeder Primfaktor von $f(n)$ kleiner als x ist, größer als cx ist. Dies scheint aber schon für den einfachsten Fall $g(x) = x^2+1$ sehr schwer zu sein *).

5. Es wäre vielleicht von Interesse, den grössten Primfaktor von einigen anderen Produkten zu untersuchen. Es sei z.B. Q_x der größte Primfaktor von $\prod_{p<x} (1+p)$ [wo p alle Primzahlen $p < x$ durchläuft]. Man würde wohl vermuten, daß $\lim Q_x\, x = \infty$ gilt. Ich konnte aber nicht einmal $\limsup Q_x / x = \infty$ beweisen **).

Bekanntlich enthält 2^n-1 für jedes $n>1$ mindestens einen Primfaktor $p \equiv 1 \pmod n$ ***). Daraus folgt, daß der größte Primfaktor p_n von 2^n-1 mindestens $n+1$ ist. Es ist wohl anzunehmen, daß mit Ausnahme von $n = 2,4,6$ $p_n > n+1$ ist, und daß $\lim p_n/n = \infty$ gilt. Diese beiden Vermutungen konnte ich aber nicht beweisen. Es ist leicht zu zeigen, daß für unendlich viele n $p_n > cn\log n \cdot \log\log n \cdot \log\log\log\log n \cdot (\log\log\log n)$ ist ****), wahrscheinlich ist aber diese Abschätzung sehr schlecht.

PÓLYA *****) bewies, daß der größte Primfaktor q_n von $g(n)$ gegen Unendlich strebt. MAHLER und CHOWLA ******) zeigten, daß der größte Primfaktor von n^2+1 größer als $c \log\log n$ ist, und NAGELL bewies dasselbe für einige spezielle Polynome höheren Grades. Es wird wohl sehr schwer sein, die wahre Größenordnung von q_n abzuschätzen, selbst im Falle $g(x) = x^2 + 1$.

*) Der sehr einfache Beweis ist unveröffentlicht.

) CHOWLA-PODD, Canadian Journal of Math., 1949, **1, S. 297–299.

***) Vergleiche S. KNAPOWSKI, Ann. Polon. Math., 1955, **2**, S. 55–63.

****) BANG, Tiddsskrift for Math., 1886, S. 130–137. Siehe auch BIRKHOFF-VANDIVER, Annals of Math., 1904.

*****) Math. Zeitschrift, 1918, **1**, S. 143–148.

******) Journal London Math. Soc.

Es seien $p_1, p_2, \ldots, p_k$ beliebige Primzahlen, $a_1 < a_2 < \ldots$ seien die Zahlen der Form $\prod_{i=1}^{k} p_i^{\alpha_i}$. PÓLYA *) bewies, daß $\lim_{i=\infty} (a_{i+1} - a_i) = \infty$ ist. Vor mehr als zehn Jahren stellte mir WINTNER **) folgendes Problem: Gibt es eine unendliche Folge von Primzahlen $q_1 < q_2 < \ldots$, derart daß wenn $b_1 < b_2 < \ldots$ die Zahlen der Form $\prod q_i^{\alpha_i}$ bedeuten, so $\lim_{i=\infty} (b_{i-1} b_i) = \infty$ gilt? Man würde glauben, daß die Antwort ohne Zweifel bejahend sein muß, aber, soviel ich weiß ist dieses Problem noch nicht erledigt.

*) Math. Zeitschrift, 1918,1, S. 143—148.
**) Mündliche Mitteilung.