Über die Zahlen der Form (n) - n und n - (n)

übertragen, wo er über alle Grenzen hinweg Kontakte fördern konnte. Die hohe Wertschätzung, die ihm von allen Seiten entgegengebracht wurde, kam sehr deutlich zum Ausdruck, als einmal an einer Topologie-Tagung im Mathematischen Forschungsinstitut in Oberwolfach in einer Art Gesellschaftsspiel der bedeutendste lebende Mathematiker ermittelt werden sollte; die Wahl fiel einmütig auf Heinz Hopf.

Wenn man sich fragt, worin das Wesen dieses grossen Mannes bestand, so wird man an seine warme Menschlichkeit denken, an seine Offenheit anderen gegenüber, gepaart mit vornehmer Zurückhaltung, an seine humorvoll-pfiffige Art, mit der er sich über gute Lösungen freuen konnte, an seine überlegene Persönlichkeit, mit der er die Dinge ins richtige Verhältnis brachte. Aber irgendwo entzieht sich dies alles einer Beschreibung. Wir stossen auf das Geheimnis eines Menschen, bei dem der volle Einsatz für die Wissenschaft nicht mit einer Deformation erkauft war, bei dem die Mathematik den richtigen Platz in einem harmonischen Ganzen hatte, das Geheimnis eines Mannes, der nicht nur in der Mathematik, sondern als ganzer Mensch schöpferichs war. Die Impulse, die von ihm auf die Wissenschaft ausgegangen sind, werden weiter wirken; aber darüber hinaus hat er seinen Freunden und Schülern ein menschliches Vorbild gegeben, an dem sich zu messen und das weiterzutragen Herausforderung und Aufgabe bleibt.

Konrad Voss

Über die Zahlen der Form $\sigma(n) - n$ und $n - \varphi(n)$

Dem Andenken von Waclaw Sierpiński gewidmet

Ich traf Professor Sierpiński zuerst im August 1955 bei einer mathematischen Tagung in Prag. Sierpiński war damals schon mehr an der elementaren Zahlentheorie interessiert als an der Mengenlehre. Wir diskutierten über die Eulersche φ-Funktion und vermuteten, dass für unendlich viele m die Gleichung

$$n - \varphi(n) = m \tag{1}$$

unlösbar ist. Diese Vermutung ist noch immer unentschieden, ich werde aber zeigen, dass für unendlich viele Werte von m

$$\sigma(n) - n = m \tag{2}$$

unlösbar ist. Wir beweisen einen etwas stärkeren

Satz I. Die untere Dichte[1]) der Zahlen m, für welche (2) unlösbar ist, ist positiv.

Bevor wir unseren Satz beweisen, wollen wir einige Besonderheiten unserer Vermutung besprechen. Es sei $n = p\,q$, wo p und q verschiedene ungerade Primzahlen sind. Offenbar ist

$$n - \varphi(n) = p + q - 1\,.$$

[1]) Ist $a_1 < a_2 < a_3 < \ldots$ eine unendliche Folge natürlicher Zahlen und $A(n)$ die Anzahl der $a_i \leq n$, so ist für $n \to \infty$ $\underline{d} = \underline{\lim}\, A(n)/n$ die untere und $\bar{d} = \overline{\lim}\, A(n)/n$ die obere Dichte der Folge. Ist $\underline{d} = \bar{d} = d$, so wird d die (asymptotische) Dichte der Folge genannt.

Wenn die (leicht modifizierte[2])) Goldbachsche Vermutung wahr ist, so ist jede ungerade Zahl in der Form (1) darstellbar, und jede ungerade Zahl $\neq 5$ ist in der Form (2) darstellbar. Van der Corput, Esterman und Tchudakoff zeigten, dass die geraden Zahlen, die nicht Summe zweier Primzahlen sind, die Dichte 0 haben, daher sind fast alle ungeraden Zahlen in der Form (1) und (2) darstellbar. Die kleinste gerade Zahl, die nicht in der Form $n - \varphi(n)$ darstellbar ist, ist 14. 2 und 4 sind nicht in der Form $\sigma(n) - n$ darstellbar. Man könnte ohne grosse Mühe alle Zahlen bis 10^6 bestimmen, die nicht in der Form (1) und (2) darstellbar sind. I. Ruzsa vermutete, dass die Dichte der Zahlen, die nicht in der Form (1) darstellbar sind, 0 ist, es ist aber nicht einmal bekannt, ob die obere Dichte dieser Zahlen grösser als $^1/_2$ ist oder ob die Dichte der in der Form (1) und (2) darstellbaren Zahlen überhaupt existiert.

Die Zahlen der Form $\varphi(n)$ und $\sigma(n)$ sind viel leichter zu studieren. $A_\varphi(x)$ sei die Anzahl der Zahlen $m \leq x$, die sich in der Form $\varphi(n)$ darstellen lassen, und $A_\sigma(x)$ sei analog für $\sigma(n)$ definiert. Pillai zeigte, dass $A_\varphi(x) = o(x)$ ist, und ich zeigte, dass für jedes ε und $x > x_0(\varepsilon)$

$$A_\varphi(x) < \frac{x}{\log x} (\log x)^\varepsilon \tag{3}$$

gilt (P. Erdös, Quarterly Journal of Math. 1935). Kürzlich zeigten R.R. Hall und ich, dass

$$A_\varphi(x) < \frac{x}{\log x} \exp c(\text{loglog } x)^{0,5} \tag{4}$$

ist; unser Beweis ist noch nicht veröffentlicht. Weiter zeigte ich (Bull. Amer. Math. Soc. 1945)

$$A_\varphi(x) > \frac{c\,x}{\log x} \text{loglog } x\,. \tag{5}$$

(5) lässt sich wohl noch auf $A_\varphi(x) > (c\,x/\log x)\,(\text{loglog } x)^k$ für jedes k und $x > x_0(k)$ verschärfen.

Weiter zeigte ich (Quarterly Journal 1935), dass ein $c > 0$ existiert, so dass für unendlich viele m die Gleichung $\varphi(n) = m$ mehr als m^c Lösungen hat. Sicherlich gilt dies für jedes $c > 1$, aber wir sind weit entfernt davon, dies zeigen zu können.

Die hier erwähnten Sätze gelten alle auch für $\sigma(n)$. Ich weiss aber nicht, ob $A_\varphi(x) - A_\sigma(x)$ unendlich viele Zeichenwechsel hat und ob $\lim_{x=\infty} A_\varphi(x)/A_\sigma(x)$ existiert und 1 ist; diese Fragen sind wahrscheinlich recht schwierig. Ich weiss auch nicht, ob $\varphi(n) = \sigma(m)$ unendlich viele Lösungen hat.

Nun beweisen wir unseren Satz. Es sei $P_k = 2.3 \ldots p_k$ das Produkt der ersten k Primzahlen. Wir beweisen den folgenden stärkeren

Satz II. Zu jedem $\varepsilon > 0$ gibt es ein k, so dass für alle $x > x_0(\varepsilon, k)$ die Anzahl $A(k, x)$ der Zahlen $n \neq p$, für welche

$$\sigma(n) - n \leq x\,, \quad \sigma(n) - n \equiv 0 \pmod{P_k} \tag{6}$$

gilt, kleiner als $\varepsilon\, x/P_k$ ist.

[2]) Jede gerade Zahl > 6 ist die Summe zweier *verschiedener* Primzahlen.

Aus Satz II folgt, dass die obere Dichte der Zahlen $m \equiv 0 \pmod{P_k}$ von der Form (2) höchstens $\varepsilon/P_k < 1/P_k$ ist. Wäre die untere Dichte der nicht in der Form (2) darstellbaren Zahlen 0, so wäre die obere Dichte der Zahlen der Form (2) 1 und die obere Dichte der durch P_k teilbaren unter ihnen $\geq 1/P_k$. Daher folgt Satz I aus Satz II.

Offenbar gilt

$$A(k, x) = A_1(k, x) + A_2(k, x) + A_3(k, x) , \tag{7}$$

wo $A_1(k, x)$ die Anzahl der Lösungen von (6) mit $n \equiv 1 \pmod 2$, $A_2(k, x)$ die Anzahl der Lösungen von (6) mit $n \equiv 0 \pmod 2$, $n \not\equiv 0 \pmod{P_k}$ und $A_3(k, x)$ die Anzahl der Lösungen von (6) mit $n \equiv 0 \pmod{P_k}$ bedeutet. Zuerst zeigen wir

$$A_1(k, x) = o(x) \tag{8}$$

und

$$A_2(k, x) = o(x) . \tag{9}$$

Aus $n \equiv 1 \pmod 2$, $\sigma(n) - n \equiv 0 \pmod 2$, folgt $\sigma(n) \equiv 1 \pmod 2$. Daher ist $n = t^2$. Wenn t Primzahl ist, folgt $\sigma(n) - n > \sqrt{n}$, also wegen $\sigma(n) - n \leq x$, $n < x^2$, $t < x$. Wenn t nicht Primzahl ist, gilt $\sigma(n) - n > n^{3/4}$ (da der kleinste Primfaktor eines quadratischen n nicht grösser als $n^{1/4}$ ist und daher $n p^{-1} \geq n^{3/4}$ gilt). Daher folgt aus $\sigma(n) - n \leq x$, dass $n < x^{4/3} < x^{3/2}$ und $t < x^{3/4}$. Also $A_1(k, x) \leq \pi(x) + x^{3/4} = o(x)$, womit (8) bewiesen ist.

Jetzt wollen wir (9) beweisen. Hier gilt $n \equiv 0 \pmod 2$, also ist $\sigma(n) \geq 3\, n/2$. Daher folgt aus $\sigma(n) - n \leq x$, dass $n \leq 2\, x$. Wir benötigen nun folgendes:

Lemma. Es sei p eine beliebige Primzahl. Die Dichte der Zahlen n mit $\sigma(n) \not\equiv 0 \pmod p$ ist 0.

Das Lemma ist wohlbekannt. Der Vollständigkeit wegen werden wir es aber im Anhang beweisen. Aus unserem Lemma folgt sofort, dass die Anzahl der Zahlen $n \leq 2\, x$ mit $\sigma(n) \not\equiv 0 \pmod{P_k}$ $o(x)$ ist. Wegen (6) und $n \not\equiv 0 \pmod{P_k}$ folgt aber $\sigma(n) \not\equiv 0 \pmod{P_k}$, daher folgt (9) sofort aus $n \leq 2\, x$.

Schliesslich wollen wir $A_3(k, x)$ abschätzen. Wegen $n \equiv 0 \pmod{P_k}$ folgt

$$\sigma(n) \geq n \prod_{l=1}^{k} \left(1 + \frac{1}{p_l}\right) > \left(\frac{2}{\varepsilon} + 1\right) n$$

für $k > k_0(\varepsilon)$, da $\sum_{l=1}^{\infty} 1/p_l = \infty$. Daher folgt aus $\sigma(n) - n \leq x$, dass $n < \varepsilon\, x/2$, also

$$A_3(k, x) < \frac{\varepsilon}{2} \frac{x}{P_k} . \tag{10}$$

Satz II folgt sofort aus (8), (9) und (10). Leider lässt sich diese einfache Methode nicht auf $n - \varphi(n)$ anwenden.

Folgende Frage konnte ich weder für $\varphi(n)$ noch für $\sigma(n)$ beantworten. Ist es wahr, dass für jedes $c > 1$ und $t > 1$ Zahlen m_1 und m_2 existieren mit $\sigma(m_1) > c\, m_1$, $\varphi(m_2) < m_2/c$, so dass die Gleichungen

$$\sigma(n) - n = m_1 , \quad n - \varphi(n) = m_2$$

mindestens t Lösungen haben.

Anhang (Beweis des Lemmas). Es seien $q_1, q_2, \ldots$ die Primzahlen mit $q_i \equiv -1 \pmod{p}$. Nach dem Dirichletschen Satz gilt $\sum q_i^{-1} = \infty$. Somit divergiert die Reihe $\sum v_i$ mit $v_i = (q_i - 1)\, q_i^{-2}$. Das unendliche Produkt $\Pi (1 - v_i)$ strebt daher gegen Null. Man kann also $\eta > 0$ beliebig und r so gross wählen, dass

$$\prod_{i=1}^{r} (1 - v_i) < \eta/2 \,. \tag{11}$$

Wenn für irgend ein i $q_i \mid n$ und $q_i^2 \nmid n$ gilt, so folgt $\sigma(n) \equiv 0 \pmod{p}$. Nun sei $B_r = \prod_{i=1}^{r} q_i$. Wenn für ein u in $1 \leq u < B_r^2$ und ein $i \leq r$ $q_i \mid u$ und $q_i^2 \nmid u$ gilt, dann folgt aus $n \equiv u \pmod{B_r^2}$, dass $\sigma(n) \equiv 0 \pmod{p}$. Für die Anzahl der Restklassen $u \pmod{B_r^2}$, die diese Eigenschaft *nicht* haben, erhält man sofort aus dem Sieb des Eratosthenes den Ausdruck

$$B_r^2 \prod_{i=1}^{r} \left(1 - \frac{q_i - 1}{q_i^2}\right),$$

der nach (11) $< 0{,}5\, \eta\, B_r^2$ ist. Daher ist für $x > x_0(\eta, r)$ die Anzahl der Zahlen $n \leq x$ mit $\sigma(n) \not\equiv 0 \pmod{p}$ kleiner als

$$0{,}5\, \eta\, B_r^2 \cdot x\, B_r^{-2} + 0{,}5\, \eta\, B_r^2 < \eta x \,. \tag{12}$$

Da (12) für jedes $\eta > 0$ gilt, ist der Beweis fertig. P. Erdös

Irreduzible Polynome als kombinatorische Figuren

Der folgende Beitrag behandelt ein Abzählproblem aus der klassischen Algebra, das erstmals von Gauss gelöst worden ist. Gelegentlich taucht es auch in der neueren Literatur wieder auf (Vgl. [1] und [2]). Mit der Darlegung der folgenden Lösung soll ein Einblick in die modernen Methoden der abzählenden Kombinatorik vermittelt werden.

1. Die Problemstellung

Die endlichen Körper oder *Galois-Felder* werden in der algebraischen Literatur meist damit abgetan, dass an einer geeigneten Stelle ein kurzer und eleganter Existenzbeweis eingeflochten wird. Die neueren Entwicklungen in der sogenannten *finiten Mathematik*[1]) bringen es mit sich, dass die Galois-Felder mehr und mehr explizit benötigt werden. So kann zum Beispiel auf Grund einer Darstellung des Galois-Feldes $GF(p^n)$[2]) die endliche Desarguessche affine Ebene von der Ordnung $s = p^n$ leicht konstruiert werden. Damit im Zusammenhang steht die Aufgabe, orthogonale lateinische Quadrate von der Ordnung $s = p^n$ zu finden. An lateinischen Verteilungen

[1]) Im angelsächsischen Raum treffender als Combinatorial Mathematics bezeichnet.

[2]) p ist eine Primzahl, n eine beliebige natürliche Zahl.