MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 9|1970

Zahlentheorie

15.3. bis 21.3.1970

Unter der Leitung von Herrn Professor Dr. Th.Schneider fand in der Woche vom 15.3. bis 21.3.1970 eine Zahlentheorietagung im Mathematischen Forschungsinstitut Oberwolfach statt, die sich u.a. mit Fragen der rationalen, elementaren und analytischen Zahlentheorie, diophantischen Approximationen und transzendenten Zahlen beschäftigte. Das Interesse an dieser Tagung äußerte sich in der Teilnahme zahlreicher bedeutender Zahlentheoretiker aus dem In- und Ausland und nicht zuletzt in einem sehr umfangreichen Vortragsprogramm. Alle Teilnehmer waren von der Oberwolfacher Atmosphäre sehr angetan. So kam ein reger Gedankenaustausch innerhalb und außerhalb des offiziellen Programms zustande, und wir sind sicher, daß Oberwolfach sich viele neue Freunde erworben hat.

Teilnehmer

W.W.Adams, College Park
R.Ayoub, Pennsylvania
D.Bode, Braunschweig
P.Bundschuh, Freiburg/Br.
K.Burde, Braunschweig
D.A.Burgess, Nottingham
H.Delange, Bures-sur-Yvette
F.Dress, Bordeaux
W.Fleischer, Salzburg
J.H.Goguel, Marburg
E.Härtter, Gießen
H.Harborth, Braunschweig
O.S.Içen, Freiburg/Br.
H.Jager, Amstelveen
H.-J.Kanold, Braunschweig
L.Kuipers, Carbondale
W.J.LeVeque, Ann Arbor
E.Lutz, Grenoble
H.L.Montgomery, Cambridge
S.Monteferrante, St. James
L.J.Mordell, Cambridge
W.Nöbauer, Wien
P.A.B.Pleasants, Cardiff
R.A.Rankin, Glasgow
B.Saffari, Nottingham
W.Schaal, Marburg
P.G.Schmidt, Marburg
T.Schneider, Freiburg/Br.

W.Schwarz, Frankfurt/M.
F.Schweiger, Wien
H.Siebert, Marburg
H.M.Stark, Göttingen
A.Stöhr, Berlin
J.Surányi, Budapest
P.Szüsz, Stony Brook
V.Turan, Budapest
R.C.Vaughan, Nottingham
B.Volkmann, Stuttgart
R.Wallisser, Freiburg/Br.
C.Whyburn, Mainz
J.M.Wills, Berlin
E.Wirsing, Marburg
D.Wolke, Marburg

Vortragsauszüge

ADAMS, W.W. : **Asymptotic Diophantine Approximations**

Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be a vector of real numbers. Let $\psi(t)$ be a decreasing positive function. Set $\lambda_B(\alpha)$ = number of solutions in ingers $q>0$, $p_1, \ldots, p_n$ of the inequalities $|q\alpha_i - p_i| < \psi(q)$ $(1 \leq q \leq n)$, $1 \leq q \leq B$. The metrical result of W.M. Schmidt states that

$\lambda_B(\alpha) \sim 2^n \int_1^B \psi(t)^n \, dt$ $(B \to \infty)$ for almost all α. Now suppose that for the given α the inequality $|q_1\alpha_1 + \ldots + q_n\alpha_n - p| \geq Q^{-n} g(Q)^{-1}$ is valid for all Q sufficiently large with g a positive increasing function.

Then if $\psi(t) t^{\frac{1}{n}} g(t)^{-\frac{n+2}{n+1}} \to \infty (t \to \infty)$ we have again that

$\lambda_B(\alpha) \sim 2^n \int_1^B \psi(t)^n \, dt$. The question remains as to what happens if ψ does not go that slowly to zero. This problem is solved in the following cases

a) $n=1$, α = quadratic irrational, $g(t) =$ constant (S. Lang)
b) $n=1$, $\alpha = e$ (or more generally any Hurwitz continued fraction), $g(t) = 2 \frac{\log t}{\operatorname{loglog} t}$
c) $n=2$; $1, \alpha_1, \alpha_2$ are the basis of a cubic number field, $g(t) =$ constant.

BUNDSCHUH, P. : Über die Approximation gewisser transzendenter Zahlen

Ist β eine algebraische Irrationalität und $R(x,y) \in Z[x,y]$ irreduzibel und hängt wirklich von x und y ab, so sind die von 0 und 1 verschiedenen Nullstellen der Funktion $R(z,z^\beta)$ nach dem Gelfond-Schneiderschen Satz transzendent. N.I.Feldmann (Vestnik Moskov.Univ. Ser.I Mat.-Mekh. (1) no. 1 (1964), 13-20) hat die Approximation solcher transzendenter Nullstellen von $R(z,z^\beta)$ durch rationale Zahlen untersucht. Hier wird die analoge Frage für die Nullstellen meromorpher Funktionen des Typs $R(z,\wp(z))$ aufgeworfen und eine Antwort gegeben, die wie folgt lautet :

Satz. Die Invarianten g_2, g_3 der Weierstraßschen $\wp$-Funktion seien algebraisch; $R(x,y) \in Z[x,y]$ möge sowohl von x wie von y abhängen, jedoch möge es keinen nur von x und keinen nur von y abhängigen Teiler besitzen. Ist $\eta \neq 0$ Nullstelle von $R(z,\wp(z))$, so gibt es zu beliebigem $\varepsilon > 0$ ein nur von g_2, g_3, η, ε und der natürlichen Zahl d abhängiges $c > 0$ derart, daß für alle algebraischen α eines Grades $\leq d$ und der Höhe H gilt :

$$|\eta-\alpha| \geq \exp\left(-c\, e^{(\log H)^{2+\varepsilon}}\right).$$

Aus diesem Approximationsmaß für η läßt sich sofort ein Transzendenzmaß für η gewinnen. Ferner kann man eine von H und d explizit abhängige untere Schranke für $|\eta-\alpha|$ erhalten. Beim Beweis wird eine Gelfondsche Methode benutzt (A.O. Gelfond, Dokl.Akad.Nauk SSSR (N.S.) 1935 II, 177-179 (russ.), 180-182 (franz.)).

BURDE, K. : Verteilungseigenschaften von Potenzresten

Ist p eine ungerade rationale Primzahl, so ordnen wir jedem vom Hauptcharakter ε verschiedenen Restklassencharakter χ modulo p die p-reihige quadratische Matrix

$$A(\chi) = \left(a_{ik} = \frac{1}{\gamma(\chi)} \cdot \chi(k-i) + \frac{1}{p} \right)_{i,k=0,1,\ldots,p-1}, \qquad \gamma(\chi) = \sum_{\nu \bmod p} \chi(\nu) e^{2\pi i \nu/p} \; ; \; \chi \neq \varepsilon$$

und dem Hauptcharakter ε die p-reihige Einheitsmatrix zu. Dann ist

durch : $\chi \to A(\chi)$ eine p-dimensionale unitäre Darstellung der Charaktergruppe modulo p, also auch der primen Restklassengruppe modulo p gegeben.

Die Betrachtung der Komponentenzerlegung gewisser Vektoren bezüglich der durch $A(\chi)$ gegebenen unitären Basis liefert in einfacher Weise Aussagen über die Verteilung der Charakterwerte $\chi(\nu)$; $\nu=1,\ldots,p-1$.

Unter Ausnutzung der vollen Darstellungseigenschaft der Matrizen $A(\chi)$ lassen sich die bisher nur für die quadratischen Charaktere bekannten Sequenzanzahlen für die Sequenzen zur Länge 2 bei kubischen und biquadratischen Charakteren berechnen. Diese Methode dürfte aber auch noch bei Charakteren höherer Ordnung, möglicherweise ganz allgemein zum Ziel führen.

BURGESS, D.A. : <u>A Form of the Large Sieve</u>

The basic Large Sieve inequality can be expressed in the form that if $x_1,\ldots x_R$ are real numbers for which

$$|| x_i - x_j || \geq \delta \qquad \forall i \neq j$$

and if $\alpha_1,\ldots,\alpha_N$ are complex numbers, then

$$\sum_{r=1}^{R} \left| \sum_{n=1}^{N} \alpha_n \exp(2\pi i x_r n) \right|^2 \ll (R+\delta^{-1}) \sum_{n=1}^{N} |\alpha_n|^2 .$$

This inequality can be used to show that if S is a subset of cardinality Q of the integers in $[1,x]$ then

$$\left[\sum_{q \in S} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| \sum_{n=1}^{N} \alpha_n \exp\left(2\pi i \frac{an}{q}\right) \right| \right]^2 \ll xQ\,(N+xQ) \sum_{n=1}^{N} |\alpha_n|^2 .$$

The latter inequality is required for the proof of the theorem that if $g(p)$ denotes the least primitive root mod. p^2 then

$$\pi(x)^{-1} \sum_{p \leq x} g(p) \ll (\log x)^3 \, (\log\log x)^6 .$$

DELANGE, H. : La distribution modulo 1 des fonctions additives

Soit f une fonction additive réelle.
A chaque entier positif n on associe une mesure μ_n sur la circonférence $\gamma = \{\zeta \in \mathbb{C} \mid |\zeta| = 1\}$, définie par

$$\mu_n(E) = \frac{1}{n} \text{ nombre des } m \leq n \text{ tels que } \exp[2\pi i f(m)] \in E.$$

On dit que f possède une distribution limite modulo 1 si la suite $\{\mu_n\}$ converge vers une mesure limite μ. Celle-ci est dite uniforme si sa valeur pour tout arc de γ est $\frac{1}{2\pi}$ fois la longueur de cet arc. Dans ce cas, on dit que f est uniformément distribuée modulo 1 (u.d.mod 1).

Nous donnons des conditions nécessaires et suffisantes portant sur les f (p), où p est premier, pour que f soit u.d.mod 1, ou pour que f possède une distribution limite mod 1 non uniforme.

Nous montrons que les f qui ne sont pas u.d.mod 1 forment un espace vectoriel sur Q. De même les f qui possèdent une distribution limite non uniforme. (Q est le corps des nombres rationnels).

DRESS, F. : Intersection d'ensembles normaux

Soit E un sous-ensemble de $R - \{0\}$. On dit que E est un ensemble normal s'il existe une suite (λ_n) de nombres réels telle que E soit l'ensemble de tous les x pour lesquels la suite $(x\lambda_n)$ est équirépartie modulo 1. Nous démontrons que l'intersection d'un nombre fini ou d'une infinité dénombrable d'ensembles normaux est un ensemble normal. En particulier, on retrouve ainsi le résultat connu que les nombres transcendants forment un ensemble normal.

FLEISCHER, W. : Über einen Satz von E. Hlawka

In der Theorie der Gleichverteilung kann man sich die Frage stellen,

"wie viele" Funktionen über den nichtnegativen reellen Zahlen gleichverteilt mod 1 sind. Bezeichnet μ_W das Wienersche Maß über dem Raum der obigen Funktionen, dann gilt

Satz 1 : μ_W - fast alle Funktionen aus $C[0,\infty]$ sind gleichverteilt mod 1. Bei einem Versuch der Verallgemeinerung dieses Satzes wird man auf eine Ungleichung von Bernstein geführt, welche einen sehr einfachen Beweis eines Satzes von E. Hlawka (1956) liefert, der als unmittelbare Folgerung des folgenden Satzes auftritt; Beweis mit Bernstein von .

Satz 2 : Ist X ein kompakter Raum, C(X) der Raum der stetigen Funktionen über X, μ ein Wahrscheinlichkeitsmaß auf X und μ_P das zugehörige Produktmaß über dem Folgenraum P zu X, dann gilt für eine Funktion $f \in C(X)$ mit $\mu(f)=0$, $\mu(f^2)=1$ die Beziehung :

$$\lim_{n\to\infty} \sum_{h=1}^{\infty} a_{nh} f(x_h) = 0 \text{ für } \mu_P \text{ - fast alle } W=(X_1,X_2,\ldots) \text{ aus } P.$$

Dabei ist $A=(a_{nh})$ eine Toeplitzmatrix mit $\sum_{n=1}^{\infty} e^{-\delta^2/\alpha_n} < +\infty$ für alle $\delta > 0$,

wobei $\alpha_n = \sum_{h=1}^{\infty} a_{nh}^2$ gesetzt wird.

HÄRTTER, E. : Rekursiv definierte Mengenfolgen .

Eine Folge von Mengen nichtnegativer ganzer Zahlen $\mathfrak{A}_1,\mathfrak{A}_2,\ldots,\mathfrak{A}_n,\ldots$ sei durch eine Rekursionsgleichung r-ter Ordnung $\mathfrak{A}_{n+r} = f(\mathfrak{A}_{n+r-1},\ldots,\mathfrak{A}_n)$ $(n=1,2,\ldots;\ r\geq 1)$ bei gegebenen $\mathfrak{A}_1,\ldots,\mathfrak{A}_r$ definiert. Von besonderem Interesse sind die rekursiv definierten Mengenfolgen, die gegen eine Grenzmenge $\mathfrak{A}$ konvergieren (vgl. Ostmann, Ergebn.d.Math. 1). Durch geeignete Wahl der Rekursionsvorschrift möchte man erreichen, daß $\mathfrak{A}$ bestimmte Eigenschaften erfüllt. Wir definieren weiter : Eine Menge $\mathfrak{B}$ nichtnegativer ganzer Zahlen heißt Basis (2. Ordnung), wenn jede ganze Zahl z darstellbar ist als (*) $z=b_1+b_2$ $(b_i \in \mathfrak{B})$. - Ferner heißt $\mathfrak{B}$ Minimalbasis, wenn $\mathfrak{B}$ Basis, aber kein $\mathfrak{B}' \subset \mathfrak{B}$ Basis ist. - Entsprechend definiert man Differenzbasen (man verlangt statt (*) $z=b_1-b_2$) und Differenzminimalbasen. - Durch rekursive Konstruktion wird u.a. gezeigt : (1) Zu jeder Menge $\mathfrak{A}=\{a_1,\ldots,a_t,\ldots\}$ natürlicher Zahlen mit $a_{t+1} \geq 4a_t$ für alle $t \geq t_o \geq 1$ gibt es eine Minimalbasis $\mathfrak{B}$ mit $\mathfrak{A} \subseteq \mathfrak{B}$. (2) Zu jeder Menge $\mathfrak{A}$ natürlicher Zahlen mit $a_{t+1} > 2a_t+1$ für alle $t \geq t_o \geq 1$ gibt es eine Differenz-Minimalbasis $\mathfrak{B}$ mit $\mathfrak{A} \subseteq \mathfrak{B}$.

HARBORTH, H. : Sequenzen ganzer Zahlen

Es wird die folgende Aussage A betrachtet: In jeder Sequenz von n aufeinanderfolgenden ganzen Zahlen gibt es mindestens k Zahlen so, daß jede von ihnen mit jeder der restlichen n-k(>0) Zahlen einen größten gemeinsamen Teiler $\leqq$ t hat. Gilt A für alle $n < \eta(k,t)$ und gilt A für alle $n \geqq h(k,t)$ nicht, so wird gezeigt : $\eta(k,t) \geqq \max(k+1, 2t+2)$; $h(k,t) \leqq k+t+1$, wenn $k > t$; $h(k,t) \leqq 3(1+\varepsilon)(2t-k)\{\log(2t-k)+\operatorname{loglog}(2t-k)\}$, wenn $k \leqq t$ und $2t-k \geqq e^{2+\frac{6}{\varepsilon}}$ mit $0 < \varepsilon \leqq 2$. Als exakte Werte werden $\eta(t+1,t) = h(t+1,t) = 2t+2$, $\eta(1,1) = h(1,1) = 17$, $\eta(1,2) = h(1,2) = 25$, $\eta(2,2) = 20$, $h(2,2) = 25$ angegeben.

JAGER, H. : Decimals and Mixing

Let $\omega \in [0,1)$, $\omega = .a_1a_2a_3\ldots$ its decimal expansion. Let b be an integer, $0 \leq b \leq g$. Let m be such, that $a_m = b$, $a_\mu \neq b$, $1 \leq \mu < m$. Define the transformation $T_b : [0,1) \to [0,1)$ by $T_b\omega = .a_{m+1}a_{m+2}\ldots$ if such an m exists, $T_b\omega = 0$ otherwise. Then take a fixed sequence $b_1, b_2, \ldots$ of integers, $0 \leq b_n \leq 9$, $n = 1,2,\ldots$ and define $\Pi_n : [0,1) \to [0,1)$ by $\Pi_n = T_{b_n} T_{b_{n-1}} \ldots T_{b_1}$, $n = 1,2,\ldots$. Then one has:

Theorem 1 : For every pair A,B of Borel sets in [0,1) :

$\lim_{n\to\infty} \lambda(\Pi_n^{-1} A \cap B) = \lambda(A)\,\lambda(B)$ where λ denotes the ordinary Lebesgue measure. I.e., the sequence $\{\Pi_n^{-1} A\}_{n=1}^{\infty}$ is strongly mixing with density $\lambda(A)$.

Theorem 2 : If $J = [\alpha,\beta]$, $0 \leq \alpha < \beta \leq 1$, χ_J the characteristic function of J, then for every $\varepsilon > 0$ one has with probability 1 :

$$n^{-1} \sum_{j=1}^{n} \chi_J(\Pi_j\omega) = (\beta-\alpha) + o(n^{-\frac{1}{2}} \log^{1,5+\varepsilon} n), \quad n \to \infty .$$

Hence, for almost all ω the sequence $\{\Pi_n\omega\}_{n=1}^{\infty}$ is uniformly distributed mod 1.

KANOLD, H.-J. : Über eine spezielleKlasse diophantischer Gleichungen

Mit elementaren Methoden wird eine Klasse von diophantischen Gleichungen untersucht, die früher u.a. auch von Nagell, Ljunggren, Mordell, Siegel, Baker behandelt worden sind. Bereits 1921 befaßte sich Nagell mit der Gleichung (*) $p(x) = \sum_{v=0}^{2m} x^{2m-v} = y^2$.

Man kann die Resultate von Nagell in etwas verschärfter Gestalt so formulieren :

Satz 1. Besitzt (*) eine ganzzahlige Lösung x,y mit $x \geq \frac{2^{2m-1}}{\sqrt{3(m+1)}}$,

dann folgt $m = 2$, $x = 3$, $y = \pm 11$.

Satz 2. Besitzt (*) eine ganzzahlige Lösung x,y mit $x > 1$, so muß einer der folgenden drei Fälle eintreten:

a) $2m+1 = p > 3$; p Primz.; $x \not\equiv 1 \ (p)$.

b) $2m+1 = p^2$; $p > 3$ Primz.; $x \equiv 1 \ (p)$; $m \equiv 0 \ (12)$.

c) $2m+1 = p_1^2 p_2$; p_1, p_2 Primz.; $x \equiv 1 \ (p_1)$; $m \equiv 0 \ (12)$; $211 \leq p_1 < p_2 < \frac{1}{8} p_1^2$; $p_2 \equiv 1 \ (24 p_1)$; $m > 10^8$.

Durch Verfeinerung der Methoden können wir die Schranke in Satz 1 ersetzen durch 2^m. Nun wollen wir eine etwas allgemeinere Klasse von Gleichungen betrachten. Das Ergebnis dieser Untersuchungen wird im wesentlichen gegeben durch

Satz 3. Es sei $\mathbb{Z}$ der Ring der ganzen ration. Zahlen. Für die Lösungen $x,y \in \mathbb{Z}$ von

$$(**) \quad p(x) = a_o^2 x^{2m} + \sum_{v=1}^{2m} a_v x^{2m-v} = y^2 \ ; \quad a_o, a_1, \ldots, a_{2m} \in \mathbb{Z} \ ; \ (a_o \geq 1)$$

können zwei Fälle eintreten:

I. $p(x) \equiv q_o^2(x)$ ist das Quadrat eines Polynoms $q_o(x) \in \mathbb{Z}[x]$. Dann existiert zu jedem $x \in \mathbb{Z}$ ein Lösungspaar (x,y); (x,-y) mit $y \in \mathbb{Z}$ (oder die Lösung (x,o)).

II. Für jede Lösung $x,y \in \mathbb{Z}$ gilt die Abschätzung $|x| < \frac{1}{m^2} \cdot H^{2m} \cdot 2^{(4+\frac{2}{3})m}$. Dabei ist H die Höhe von p (x), d.h. $H = \max \{a_o^2, |a_1|, \ldots, |a_{2m}|\}$.

In vielen Sonderfällen kann die Schranke verbessert werden.

KUIPERS, L. : A general form of the Weyl criterion in the theory of asymptotic distribution

In the paper we (Professor A.J. Stam, Groningen, Netherlands, and I) apply a (classic) result on the convergence of a class of distribution functions in order to find a very general form of the Weyl criterion covering even the case of the Niven-Uchiyama criterion in the theory of distribution of sequences of integers modulo m, and also the case of some summability-procedure distribution of sequences of real numbers.

MONTGOMERY, H.L. : The problem of Schinzel and Zassenhaus

P.E. Blanksby and I have recently proved the following sharpening of a well-known theorem of Kronecker.

Theorem. Let α be an algebraic integer of degree $n > 1$ over the rationals with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$. If

$$\max_{1 \le j \le n} |\alpha_j| \le 1 + \frac{1}{30\, n^2 \log 6n} \qquad (*)$$

then α is a root of unity.

Schinzel and Zassenhaus have asked whether (*) can be weakened to

$$\max_{1 \le j \le n} |\alpha_j| \le 1 + \frac{c}{n}$$

for some $c > 0$. This would be best possible because of the example $\alpha = 2^{\frac{1}{n}}$. The problem is treated as one of Diophantine approximation. Our basic technique is analytic, and permits one to give many results in Diophantine approximation. Our joint paper will appear in the Davenport volume of Acta Arithmetica.

MONTEFERRANTE, S. - SZÜSZ, P.

: On the digits of an algorithm connected with continued fractions

Let α be a positive irrational number with the continued fraction expansion

$$\alpha = [o;a_1,a_2,..].$$

Set $\frac{A_n}{B_n} = [o;a_1,..,a_n]$, $((A_n,B_n) = 1)$, $D_n = B_n\alpha - A_n$.

It is known that every real t satisfying $-D_o \leqq t \leqq 1 - D_o$ permits a representation

$$(*) \quad t = \sum_{k=o}^{\infty} c_{k+1} D_k,$$

where $o \leqq c_1 < a_1$, $o \leqq c_{k+1} \leqq a_{k+1}$ and $c_{k+1} = a_{k+1}$ implies $c_k = o$. If we exclude $c_{2k+1} = a_{2k+1}$ $(k = 1,2,...)$ with some l, then the representation $(*)$ is unique.

It was proved that for a certain class of the α's analogues of a classical theorem of Borel holds, which states that for almost all t 's the asymptotical density of every digit of the dyadic expansion exists. More precisely, for a class of α (which includes all α except a set of measure zero) we have the existence of the limit

$$(**) \quad \lim_{n\to\infty} \frac{1}{n} \sum_{\substack{k\leqq n \\ c_k=r}} 1 = \gamma_r$$

for almost all t; the limit $(**)$ is for almost all t depending only on α and r and independent of t. Further we investigated the asymptotic behaviour of the difference

$$\sum_{\substack{k\leqq n \\ c_k=r}} 1 - n\gamma_r$$

for almost all t. In particular we showed that if α is a quadratic irrational number, then there is a positive constant K such that for almost all t we have

$$\overline{\lim_{n\to\infty}} \left(\sum_{\substack{k\leqq n \\ c_k=r}} 1 - \gamma_r n \right) \frac{1}{\sqrt{kn \log\log n}} = 1 .$$

MORDELL, L.J. : Cubic congruences in two variables

Let f(x,y) be a cubic polynomial with integer coefficients. Necessary and sufficient conditions are given so that if either variable is given, the congruence $f(x,y) \equiv o \pmod p$, p a prime has a solution for the other variable.

NÖBAUER, W. : Darstellung von Permutationen durch Polynome und rationale Funktionen

Es sei $\mathfrak{K}$ ein kommutativer Ring mit Einselement. Die Permutation Π der Elemente von $\mathfrak{K}$ wird dargestellt durch das Polynom f(x) über $\mathfrak{K}$, wenn gilt $\Pi\, a = f(a)$ für alle $a \in \mathfrak{K}$. Ein Polynom f(x) über $\mathfrak{K}$ heißt Permutationspolynom von $\mathfrak{K}$, wenn es eine Permutation der Elemente von $\mathfrak{K}$ darstellt. Es werden hi er zwei Möglichkeiten der Verallgemeinerung dieser Definition und die sich daraus ergebenden Probleme und Resultate behandelt :

1) Verallgemeinerung auf rationale Funktionen : Die Permutation Π der Elemente von $\mathfrak{K}$ wird dargestellt durch die rationale Funktion $r(x) = \frac{u(x)}{v(x)}$, wenn v(a) für jedes $a \in \mathfrak{K}$ eine Einheit von $\mathfrak{K}$ ist, und wenn gilt $\Pi\, a = u(a)v(a)^{-1}$ für jedes $a \in \mathfrak{K}$. Eine rationale Funktion r(x) über $\mathfrak{K}$ heißt Permutationsfunktion von $\mathfrak{K}$, wenn sie eine Permutation der Elemente von $\mathfrak{K}$ darstellt.

2) Verallgemeinerung auf Polynome in mehreren Unbestimmten. Hier gibt es drei Möglichkeiten :

a) Eine Permutation Π der Elemente des n-fachen Cartesischen Produkts $\mathfrak{K} \times \ldots \times \mathfrak{K}$ wird dargestellt durch den "Polynomvektor" (= n-Tupel von Polynomen) $(f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n))$, wenn gilt $\Pi\,(a_1,\ldots,a_n) \equiv (f_1(a_1,\ldots,a_n),\ldots,f_n(a_1,\ldots,a_n))$ für alle $(a_1,\ldots,a_n) \in \mathfrak{K} \times \ldots \times \mathfrak{K}$. Ein Polynomvektor heißt Permutationspolynomvektor, wenn er eine Permutation von $\mathfrak{K} \times \ldots \times \mathfrak{K}$ darstellt.

b) Jede Permutation Π von $\mathfrak{K} \times \ldots \times \mathfrak{K}$ läßt sich mit Hilfe der Funktionen $\varphi_i : \mathfrak{K} \times \ldots \times \mathfrak{K} \to \mathfrak{K}$ darstellen in der Form $\Pi\,(a_1,\ldots,a_n) = (\varphi_1(a_1,\ldots,a_n),\ldots,\varphi_n(a_1,\ldots,a_n))$. Eine Funktion $\varphi_i : \mathfrak{K} \times \ldots \times \mathfrak{K} \to \mathfrak{K}$ heiße "Permutationsteil", wenn sie in der Darstellung einer Permutation in obiger Gestalt als Komponente auftritt. Das Polynom $f(x_1,\ldots x_n)$

heiße Permutationspolynom, wenn die ihm entsprechende Funktion ein Permutationsteil ist. Es gilt : $f(x_1,..,x_n)$ ist genau dann Permutationspolynom, wenn die Kardinalzahl der Lösungsmenge der Gleichung $f(x_1,...,x_n) = u$ für jedes $u \in \mathfrak{K}$ den Wert $|\mathfrak{K}|^{n-1}$ hat.

c) Das Polynom $f(x_1,...,x_n)$ heiße starkes Permutationspolynom, wenn es in irgendeinem Permutationspolynomvektor als Komponente auftritt. Es gilt : Jedes starke Permutationspolynom ist auch Permutationspolynom (die Umkehrung konnte bisher nur für bestimmte Typen von Ringen, insbesondere Galoisfelder, bewiesen werden).

Es werden verschiedene Resultate und Probleme erwähnt, die mit diesen Definitionen in Zusammenhang stehen, wobei über $\mathfrak{K}$ vorausgesetzt wird, daß es ein Galoisfeld oder ein Restklassenring $\mathbb{Z}|(n)$ der ganzen rationalen Zahl ist. Diese betreffen insbesondere die kleinstmöglichen Grade der Polynome bzw. rationalen Funktionen, die eine gegebene Permutation darstellen, sowie Aussagen der Art, daß ein Polynom oder eine rationale Funktion von bestimmter Gestalt Permutationspolynom bzw. Permutationsfunktion ist.

NOVÁK, Břetislav$^+$: Über Gitterpunkte in mehrdimensionalen Ellipsoiden

Sei $Q(u) = \sum_{1 \le j,j' \le r} a_{j,j'} u_j u_{j'}$ eine positiv definite quadratische Form in $r \ge 2$ Variablen; α_j, b_j seien reelle, M_j positive Zahlen $(j=1,...,r)$. Die positiven Werte von $Q(M_j m_j + b_j)$ für ganze m_j $(j=1,...,r)$ seien mit $0<\lambda_1<\lambda_2<...$ bezeichnet; sei $\lambda_0 = 0$.

An LANDAU und JARNIK anknüpfend untersucht der Verfasser für $\rho \ge 0$ die Funktion

$$A_\rho(x) = \frac{1}{\Gamma(\rho+1)} \sum_{\lambda_m \le x} (x-\lambda_m)^\rho \sum_{\substack{u_j \equiv b_j \bmod M_j \\ Q(u) = \lambda_m}} \exp(2\pi i \Sigma \alpha_j u_j).$$

Für den Fehler $\{A_\rho(x) - \text{Hauptglied}\}$ und das Quadrat-Integral dieses Fehlers werden O-Abschätzungen und Ω-Abschätzungen angegeben, und zwar in folgenden Fällen :

a) Die Koeffizienten $a_{j,j'}$, die b_j und die M_j sind ganz.

Auszug aus dem der Tagung übersandten Manuskript

b) $M_j = 1$, $\alpha_j = b_j = 0$ und $Q(u) = \sum_{j=1}^{\sigma} a_j Q_j(u_{1,j},\ldots,u_{r_j,j})$

ist Summe positiv definiter quadratischer Formen Q_j in genügend vielen Variablen mit ganzen Koeffizienten; hierbei sind die a_j positive reelle Zahlen.

PLEASANTS, P.A.B. : Cubic forms over $\wp$-adic fields

A simple proof of other well known result that a cubic form in n variables over a $\wp$-adic field has a non-singular zero if $n \geq 10$. Also some remarks about forms of higher degree.

SAFFARI, Bahman : On some connexions between Riemann hypothesis and Dirichlet's divisor problem

The purpose of this talk is to study the average behaviour of some arithmetical functions related to the divisor function d(n), and to give some results which <<naturally>> lead to a <<general conjecture>> yielding, as particular cases, both the Riemann hypothesis and the Hardy-Landau hypothesis on the divisor problem.

SCHAAL, Werner : Das große Sieb in algebraischen Zahlkörpern

Eine Ungleichung von Bombieri und Davonport aus der Theorie des großen Siebes wird auf algebraische Zahlkörper von endlichem Grade über dem Körper der rationalen Zahlen verallgemeinert. Diese Verallgemeinerung wird zusammen mit einer Identität von Montgomery benutzt, um obere Abschätzungen für die Anzahl der Primzahlen in Parallelepipeden und eine Ausdehnung des Satzes von Brun-Titchmarsh auf Zahlkörper zu erzielen.

SCHMIDT, P.G. : Beiträge zur Theorie stark multiplikativer Funktionen

Sei f eine der Bedingung $\sum_p f(p) < \infty$ genügende nichtnegative stark multiplikative Funktion, ω_n die Anzahl der verschiedenen Primteiler von n und h eine nichtnegative zahlentheoretische Funktion, für die

$H(z) := \sum_{k=o}^{\infty} \frac{h(k)}{k!} z^k$ einen positiven Konvergenzradius R besitzt.

Zunächst wird eine elementare Methode skizziert zur Herleitung asymptotischer Beziehungen zwischen der Summe $\sum_{n \leq x} h(\omega_n) f(n)$ und dem Integral $\frac{1}{2\pi i} \int_{|z|=r} H(z) \prod_p (1+ \frac{f(p)}{\log p} \frac{\log x}{z}) \frac{dz}{z}$ $(o<r<R)$.

Einige Sätze werden notiert.

Anschließend wird das Verhalten der summatorischen Funktion $\sum_{n \leq x} f(n)$ genauer diskutiert. Unter der Voraussetzung

$$(*) \quad \sum_{n \leq x} f(n) \sim \frac{1}{2\pi i} \int_{|z|=r>o} e^z \prod_p (1+ \frac{f(p)}{\log p} \frac{\log x}{z}) \frac{dz}{z}$$

wird gezeigt :

I. Eine Zufallsvariable ω mit der Verteilungsfunktion

$$P(\omega<y) := \frac{\sum_{\substack{n \leq x \\ \omega_n < y}} f(n)}{\sum_{n \leq x} f(n)}$$

ist bei geeigneter Normierung asymptotisch normal verteilt, sofern Erwartungswert E und Dispersion D für $x \to \infty$ den Bedingungen $D \to \infty$, $E = o(D^3)$ genügen.

II. Besitzt die Menge $\mathfrak{N}$ nichtnegativer ganzer Zahlen die positive asymptotische Dichte δ, und gilt für das Restglied

$\Delta(x) := \left(\sum_{\substack{o \leq k \leq x \\ k \in \mathfrak{N}}} 1 \right) - \delta \cdot x$ entweder $\Delta(x) = o(\sqrt{x})$ oder $\Delta(x) - \Delta(y) = o(|x-y|)$,

so folgt

$$\sum_{\substack{n\leq x \\ \omega_n \in \mathfrak{N}}} f(n) \sim d \sum_{n\leq x} f(n)$$

Die Voraussetzung (*) trifft zu, wenn $\sum_p f(p) < \infty$ gilt.

SCHNEIDER, Th. : <u>Über rationale Punkte auf algebraischen Kurven</u>

Sei f(x) eine algebraische Funktion qten Grades, d.h. $F(x,f(x)) = \sum_{k=o,\lambda=o}^{l,q} a_{k\lambda} x^k f(x)^\lambda \equiv o$ mit ganzrationalen Koeffizienten ist bezüglich q minimal.

Sei f(z) regulär in einer Umgebung um $z = o$, dann gilt der Satz :

Sei 1. f(o) eine rationale Zahl,
2. $f(\frac{r}{t})$ eine rationale Zahl für rationales, gekürztes $\frac{r}{t} \neq o$,
so ist 3. $|\frac{r}{t}| > t^{-(\frac{1}{q} + \epsilon)}$ bei $\epsilon > o$ für $t > t_o(\epsilon)$.

Hierzu existiert eine p-adische Verallgemeinerung bzw. Verschärfung :

Ist zu einem p : $\Sigma a_\nu x^\nu = f(x)$ p-adisch konvergent, schreibe

$f_p(x) = \Sigma_p a_\nu x^\nu$ und für rationales $x = \frac{r}{t}$, sowie für $x = o$

$(\Sigma a_\nu x^\nu = \sum_p a_\nu x^\nu)_{x=\frac{r}{t}}$ die gleiche rationale Zahl;

dies ist, wenn $\Sigma a_\nu x^\nu /_{x=\frac{r}{t}}$ rational ist, eine Bedingung für p,

und ich bezeichne solche p mit $p = p^*$, so gilt unter den obigen Bedingungen

1. und 2. anstelle von 3.

$$3' \quad |\tfrac{r}{t}| \cdot \prod_{p^*} |\tfrac{r}{t}|_{p^*} > t^{-(\frac{1}{q} + \epsilon)} .$$

Beide Behauptungen 3. und 3' sind bezüglich der rechten Seite (des Exponenten) scharf, wie man an den Beispielen

$$\frac{t_1-1}{t_1} = \left(1-\frac{r_1}{t_1^q}\right)^{\frac{1}{q}} \quad \text{zu } \underline{3}.$$

und $\frac{s}{t_1} = \left(1-\frac{r_2}{t_1^q}\right)^{\frac{1}{q}}$ und $t_1^q = s^q + r_2$ zu $\underline{3}'$.

erkennen kann.

Beim Beweis wird der Satz von Eisenstein über die Entwicklung algebraischer Funktionen und eine geeignete Interpolationsreihenentwicklung einer zu konstruierenden Funktion

$$\Phi(x,f(x)) = \sum_{k=o,\lambda=o}^{k,q-1} {}_{k\lambda}x^k\, f(x)^\lambda$$ benutzt. Der Beweis ist indirekt.

SCHWARZ, Wolfgang : <u>Über Teiler von n der Gestalt p-1</u>

PRACHAR zeigte 1955 für die Anzahl $\delta(n)$ der Teiler d von n der Gestalt $d = p-1$, p prim, unter anderem die asymptotische Formel

$$\sum_{n\leq x} \delta(n) = x\cdot\text{loglog } x + B\cdot x + O\ (x\ /\ \log x)\ ;$$

diese wird zu einer asymptotischen Entwicklung nach fallenden Potenzen von log x mit dem Fehlerglied

$O\{ x\cdot \exp(-c\sqrt{\log x})\}$

verschärft. Mit BOMBIERIs Primzahlsatz und der SELBERGschen Siebmethode wird

$$\sum_{p\leq x} \delta(p-1) = D\cdot\frac{x}{\log x}\cdot\{\text{loglog } x + O(\text{logloglog } x)\}$$

hergeleitet; schließlich wird auf einige offene Probleme hingewiesen.

SCHWEIGER, Fritz : Metrische Theorie kettenbruchähnlicher Ziffernentwicklungen

Zunächst wird eine Klasse kettenbruchähnlicher Ziffernentwicklungen betrachtet, welche ergodische Transformationen des Einheitswürfels induzieren. Tragend für die Theorie sind dabei eine Verallgemeinerung des Satzes von KUZMIN und ein Lemma von PHILIPP. Es wird auf einige Algorithmen verwiesen, die kein absolut stetiges invariantes Maß besitzen. Einige Bemerkungen zu dem noch ungelösten Problem der Normalität bezüglich verschiedener Ziffernentwicklungen werden angeschlossen.

SIEBERT, H. : Einige Analoga zum Satz von Siegel-Walfisz

Alle bisher bekannten Beweise des Satzes von BOMBIERI benutzen für kleine Moduln den Satz von Siegel-Walfisz, und es scheint so, daß sich dies nicht umgehen läßt. Die Frage nach Analoga zum Bombierischen Satz und andere Anwendungsmöglichkeiten begründen daher ein gewisses Interesse an gleichmäßigen Abschätzungen vom Siegel-Walfisz-Typ für andere Folgen, bzw. zahlentheoretische Funktionen. 1935 bewies DAVENPORT einen solchen Satz für $\mu(n)$, wir folgern hieraus analoge Sätze für $\lambda(n)$ und die Verteilung k-freier Zahlen. Abschließend geben wir eine Klasse multiplikativer Funktionen an, für die sich solche Sätze beweisen lassen.

STARK, H.M. : Sign Changes of Number Theoretic Functions

Let $\pi(x,k,a)$ denote the number of primes $\leq x$ that are $\equiv a \pmod k$. The problem to be considered is whether $\pi(x,k,a) - \pi(x,k,b)$ has infinitely many sign changes. Let

$$\Delta(x;k;a;K,A) = \frac{\phi(k)\,\pi(x,k,a) - \phi(K)\,\pi(x,K,A)}{\sqrt{x} / \log x} .$$

Most likely $\limsup_{x \to \infty} \Delta(x;k,a;K,A) = \infty$ but this seems beyond our reach if neither a nor A is 1. However, it seems to be possible to prove for any given k,a,K,A that

$$\limsup_{x \to \infty} \Delta(x;k,a;K,A) > 0 .$$

This requires a computation in general which can be carried out in two different ways. Both ways are illustrated for the case $k = K = 5$, $a = 4$, $a = 2$.

SURÁNYI, János : Gitterpunktfreie Rechtecke

Der Satz von Szekeres, - nach dem zu beliebigen Linearformen $L_i = a_i u + b_i v$ $i = 1,2$ mit $D = |a_1 b_2 - a_2 b_1| > 0$ positive Konstanten s_1, s_2 mit $s_1 s_2 \geq ((\sqrt{5}+1) / 2\sqrt{5})\, D$ gibt, so daß daß System der Ungleichungen $|L_i| < s_i$ $i = 1,2$ nur die triviale Lösung in ganzen Zahlen hat, - wird mit elementar-geometrischen Hilfsmitteln bewiesen. Der Beweis liefert auch das zweite Maximum $((\sqrt{3}+1) / 2\sqrt{3})\, D$. - Die Folge der sukzessiven Maxima wurde von A. Oppenheim mittels Kettenbrüchen bestimmt. - Es ergibt sich aus der hier angegebenen Behandlung des Problems ein wirkungsvoller gittergeometrischer Aufbau der Kettenbrüche ähnlich dem von F. Klein vorgeschlagenen.

VAUGHAN, R.C. : An application of the large sieve to a diophantine equation

Endös and Straus have conjectured that for every integer $n > 1$,

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

is soluble in positive integers x,y,z.

Schinzel has conjectured that for every $a > o$, if $n > n_o(a)$,

$$(1) \qquad \frac{a}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

is soluble in positive integers x,y,z.

If $E_a(N)$ is the number of $n \leq N$ for which (1) is insoluble, it can be shown, by an application of the large sieve, that

$$E_a(N) << N \exp \{ -c(a) (\log N)^{2/3} \} .$$

WALLISSER, R. : Zur Transzendenz gewisser Zahlen

In seiner Arbeit über Linearformen von Logarithmen algebraischer Zahlen (Mathematika 14 (1967), 102-107) hat A. Baker den folgenden Satz bewiesen : "Sind $\alpha_1, \ldots, \alpha_n$ von 0 und 1 verschiedene algebraische Zahlen und sind die algebraischen Zahlen $1, \beta_1, \ldots, \beta_n$ linear unabhängig über dem Körper der rationalen Zahlen Q, dann ist $\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$ transzendent."

Mit derselben Beweismethode läßt sich noch zeigen:

"Sind $\alpha_1, \ldots, \alpha_n$ von 0 und 1 verschiedene algebraische Zahlen, $\eta_1, \ldots, \eta_n$ algebraisch vom Grade $\leq s$ und einer Höhe $\leq H$, gilt bei beliebig großem H: $\max_i |\beta_i - \eta_i| < \exp(-(\log H)^{\varkappa})$ mit $\varkappa > 2n+3$ und sind $1, \beta_1, \ldots, \beta_n$ linear unabhängig über Q, dann ist $\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$ transzendent."

WHYBURN, CLIFTON : Elimentary Estimates for the Distribution of r-th Power in a Finite Field

Let p be an odd prime, k a positive integer, and r a positive integer such that $r \mid (p^k - 1)$. Let $\varepsilon = 1$ or 2 such that $k \equiv \varepsilon \pmod 2$. GF $(p^k) = F$ is represented as $\mathbb{Z}_p[x]/P$ where P

is an irreducible element of $Z_p[x]$.

By completely elementary methods, L. Kuty and H. Stevens have been able to prove that there exist at least $(p^{\epsilon} - 1)/2$ non-r-th powers of degree $\leq [k/2]$ in F. By similar methods (indeed, the same basic lemma), it is shown that there are at least $(p^{k/2} + 1)(p^{\epsilon/2} - 1)(r-1)/r$ non r-th powers in F having degree $\leq [k/2]$. Some more general results may be obtained by the same methods

WILLS, J.M. : Zur simultanen diophantischen Approximation

In der linearen reellen diophantischen Approximation wird zu gegebenem $\alpha=(\alpha_{ij})$, $1 \leq i \leq n$, $1 \leq j \leq m$, $\alpha_{ij} \in R$ die Verteilung der Menge

$$Q(\alpha) = \{\eta \in R^n \,/\, \eta_i = \sum_{j=1}^{vn} \alpha_{ij} q_j - p_i \,,\; p_i, q_j \in Z,\; 1 \leq i \leq n,\; 1 \leq j \leq m\}$$

auf dem durch $\rho(\xi,\eta) = \max_{1 \leq i \leq n} ||\xi_i - \eta_i||$ metrisierten kompakten Torusraum T^n untersucht ($||x|| = \min_{g \in Z} |x-g|$). Kroneckers Approximationssatz lautet dann $\overline{Q}(\alpha) = M(\alpha)$; dabei ist $M(\alpha)$ eine lineare Mannigfaltigkeit. Im Anschluß an diesen Strukturssatz zwei Fragen :

1) Feinere Verteilung von $Q(\alpha)$ auf $M(\alpha)$? ("Innere Geometrie von $Q(\alpha)$");

2) Einbettung der $M(\alpha)$ in T^n ?

Die meisten bekannten Sätze gehören zu 1), z.B. Weyls Gleichverteilungssatz und der Satz von Dirichlet-Minkowski. Es werden einige Sätze zu ?) gebracht, die sich durch die oben eingeführte Metrik ganz natürlich ergeben.

Beweismethoden, verwandte Probleme und eine Anwendung auf die Funktionentheorie (Analytische Fortsetzung durch Limitierungsverfahren) werden skizziert.

WIRSING, Eduard : Über den Satz von Gauß-Kusmin

Entwickelt man die (irrationalen) Zahlen $\alpha \in [0,1]$ in regelmäßige Kettenbrüche $\alpha = \frac{1}{a_1+} \frac{1}{a_2+} \ldots = (0,a_1,a_2\ldots)$, so ist die Frage nach der Verteilungsfunktion für $a_n = a_n(\alpha)$ eng verwandt mit der Frage nach dem Maß

$$m_n(x) = \mu \{\alpha; \frac{1}{a_{n+1}} \dotplus \frac{1}{a_{n+2}} \dotplus \ldots < x\} .$$

In Fortführung und Vereinfachung von Ideen von Kusmin, P. Lévy, P. Szüsz wurde im Vortrag zunächst die Abschätzung

$$m_n(x) = \frac{\log(1+x)}{\log 2} + r_n(x), \quad c_1 5^{-n} x(1-x) \leq (-1)^{n+1} r_n(x) \leq c_2 2^{-n} x(1-x),$$

insbesondere $r_n(x) << 2^{-n}$ gezeigt. Dafür sind numerische Untersuchungen nicht nötig. Weiter wurde der folgende Satz angegeben :

$r_n(x) = (-1)^{n+1} \lambda^n \rho(x) + O(\mu)$.

Dabei ist $\lambda = 0{,}30366\ldots$ und $\mu < \lambda$; λ und $\rho(x)$ können mit Rechenautomaten berechnet werden. Geschlossene Ausdrücke sind jedoch nicht bekannt. Zum Existenzbeweis wurde der folgende Satz entwickelt :

Satz : Sind B,F lineare Abbildungen von $C[0,1]$ in sich bzw. in R, dabei $B \geq F \geq 0$ (d.h. $\forall_x (B\varphi)(x) \geq F\varphi \geq 0$ wenn $\forall_x \varphi(x) \geq 0$), hat man ferner eine streng positive Funktion φ_0, so daß

$s\varphi_0 \leq B\varphi_0 \leq t\varphi_0$ mit Konstanten s,t, für die gilt

$F\varphi_0 > (1-\frac{s}{t}) \sup_x (B\varphi_0)(x)$, dann hat B eine (streng) positive Eigenfunktion ϕ_0 mit einem Eigenwert $\lambda \in [s;t]$ und das restliche Spektrum von B liegt im Kreis um Null mit dem Radius

$$\mu = \lambda - t \left(\frac{F\varphi_0}{\sup B\varphi_0} - t + s\right) < \lambda .$$

WOLKE, Dieter : Das große Sieb mit Primzahlen

Der Beweis und einige Anwendungen zur folgenden Ungleichung werden diskutiert.

Sei $Q \geq 10$, $0 < \delta < 1$, $N \leq Q^{1+\delta}$. Seien

a_n $(M < n \leq M + N)$ komplexe Zahlen,

$$S(\alpha) = \sum_n a_n e^{2\pi i n\alpha}, \quad Z = \sum_n |a_n|^2 .$$

Dann gibt es eine absolute Konstante C, so daß

$$\sum_{\substack{p \leq Q \\ p \text{ prim}}} \sum_{b=1}^{p-1} \left| S\left(\frac{b}{p}\right) \right|^2 \leq \frac{C}{1-\delta} \frac{Q^2 \ln\ln Q \, Z}{\ln Q}$$

gilt.

P. Bundschuh (Freiburg)