Mh. Math. 124, 337–342 (1997)

Monatshefte für
Mathematik

Über die Verteilung der primen quadratischen Reste und Nicht-Reste mod p

Von

Jan-Christoph Puchta und **Dieter Wolke,** Freiburg

(Received 3 November 1995; revised 6 November 1996)

Abstract. On the Distribution of Prime and Nonprime Residues mod p. Let P be an odd prime, denote by p_n (q_n) the n^{th} prime $\neq P$ with $\left(\frac{p_n}{P}\right) = 1 (= -1), d_n = q_n - p_n$. We discuss the question whether d_n changes sign infinitely often or not. Without using Turán's power sum method the following theorem is proved. Suppose that the L-function L(s, χ), defined by the real primitive character mod P, has no real root σ with $\frac{1}{2} < \sigma < 1$. Then the numbers d_n change sign infinitely often. The hypothesis is known to be true for all P with $2 < P \leqslant 227$ (J. B. Rosser. J. of Research of the Nat. Bureau of Standards 45, 505–514 (1950)).

1. Einleitung

In der sogenannten vergleichenden Primzahltheorie ("comparative prime number theory") werden Unregelmäßigkeiten der Verteilung der Primzahlen in verschiedenen Restklassen zu einem Modul m untersucht. Zahlreiche Ergebnisse hierzu sind vor allem Knapowski und Turán zu verdanken, überwiegend mit der Turánschen Potenzsummen-Methode erzielt (siehe TURÁN [5], §§ 48–56). Die folgende Fragestellung und ebenso die Grundidee zum Beweis des Satzes wurde vom ersten Autor im Rahmen des Wettbewerbs "Jugend forscht" entwickelt.

Sei $P > 2$ eine ungerade Primzahl, bezeichne p_n die n-te Primzahl $\neq P$ mit $\left(\frac{p_n}{P}\right) = 1, q_n$ die n-te Primzahl $\neq P$ mit $\left(\frac{q_n}{P}\right) = -1$,

$$d_n = q_n - p_n.$$

Ist es möglich, daß d_n ab einer Stelle stets dasselbe Vorzeichen hat?

Für beliebige P scheint dies nicht ohne weiteres mit den Knapowski-Turánschen Ergebnissen beantwortbar zu sein. Im Folgenden soll unter Verwendung einer analytischen Hypothese, die in ähnlicher Form auch bei Knapowski-Turán auftritt, aber ohne Verwendung der Potenzsummen-Methode, eine negative Antwort auf die obige Frage gegeben werden.

1991 Mathematical Subject Classification: 11N13, 11M20
Key words: Prime quadratic residues and non-residues, Comparative prime number theory

Sei $\chi(n) = \left(\frac{n}{P}\right)$ der primitive reelle Charakter mod P, $L(s,\chi)$ die zugehörige L-Reihe, und bezeichne (Hp) die folgende Hypothese:

$$(Hp)\ L(\sigma,\chi) \neq 0 \text{ für } \frac{1}{2} < \sigma < 1.$$

Ziel dieser Arbeit ist der

Satz. *Sei $P > 2$ eine Primzahl, für die (Hp) gilt. Dann wechselt d_n unendlich oft das Vorzeichen.*

Bemerkung 1. Wie der Beweis zeigen wird, funktioniert die Schlußweise auch, wenn nur vorausgesetzt wird: Falls $\beta_0 \in \left(\frac{1}{2}, 1\right)$ eine reelle Nullstelle von $L(s,\chi)$ ist, dann existiert eine Nullstelle $\rho = \beta + i\gamma$ von $L(s,\chi)$ mit $\beta > \beta_0$.

Bemerkung 2. Nach ROSSER [3] ist (Hp) für alle $2 < P \leqslant 227$ erfüllt. Durch direktes Ausrechnen der L-Reihen läßt sich dies auf alle $P < 3533$ ausdehnen.

Die Primzahl P, für die (Hp) angenommen wird, sei im Folgenden festgehalten. Die O- und $\ll$ Konstanten, sowie die c_j können von P abhängen.

2. Bemerkungen zum Fall der Gültigkeit der Riemannschen Vermutung für $L(s,\chi)$.

Nimmt man beispielsweise $d_n > 0\ \forall n \geqslant n_0$ an, dann folgt unmittelbar

$$\eta(x) = \sum_{p \leqslant x} \chi(p) \geqslant 0 \quad \forall x \geqslant x_0. \tag{2.1}$$

Mit der Littlewoodschen Methode (Siehe LITTLEWOOD [1], PRACHAR [2]) kann

$$\eta(x) = \Omega \pm (x^{1/2} \ln \ln \ln x) \tag{2.2}$$

gezeigt werden. Hierbei spielt es keine Rolle, ob $s = \frac{1}{2}$ Nullstelle von $L(s,\chi)$ ist oder nicht. (2.2) ist mit (2.1) offenbar nicht verträglich.

3. Zwei Hilfssätze

Im Hinblick auf den Fall der Nicht-Gültigkeit der Riemannschen Vermutung für $L(s,\chi)$ werde nun (Hp) und $\forall n \geqslant n_0 : d_n > 0$ (bzw. < 0) vorausgesetzt.

Lemma 1. *Es existieren $c_1 \in \left(0, \frac{1}{2}\right)$ und $c_2 > 0$, so daß für jedes $x > c_2$ das Intervall $(x, x + x^{1-c}]$ ein ξ mit*

$$\left|\sum_{p \leqslant \xi} \chi(p)\right| \leqslant x^{1-c_1} \tag{3.1}$$

enthält.

Beweis. Es werde wieder OBdA $d_n > 0$ $(n \geqslant n_0)$ und somit

$$\eta(x) = \sum_{p \leqslant x} \chi(p) \geqslant 0 \quad (x \geqslant x_0(P)) \tag{3.2}$$

vorausgesetzt. Wir nehmen an, daß für ein (später festzulegendes, hinreichend kleines) $c_1 \in \left(0, \frac{1}{2}\right)$ und ein hinreichend großes $\tilde{x} \geqslant x_0$

$$\eta(y) > \tilde{x}^{1-c_1} \text{ für alle } y \in (\tilde{x}, \tilde{x} + \tilde{x}^{1-c_1}] \tag{3.3}$$

gilt. Dann folgt mit $x = \tilde{x}^{1+c_1}$ und $k = \left[\frac{1}{2} c_1 \ln x\right]$

$$\begin{aligned} F_k(x) &:= \frac{1}{x} \int_{x_0}^{x} dx_{k-1} \cdots \frac{1}{x_1} \int_{x_0}^{x_1} dt\, \eta(t) \\ &= \frac{1}{x} \int_{x_0}^{x} dt\, \eta(t) \int_{t}^{x} dx_1 \frac{1}{x_1} \cdots \frac{1}{x_{k-2}} \int_{x_{k-2}}^{x} dx_{k-1} \frac{1}{x_{k-1}} \\ &= \frac{1}{(k-1)!\, x} \int_{x_0}^{x} dt\, \eta(t) \ln^{k-1}\left(\frac{x}{t}\right). \end{aligned} \tag{3.4}$$

Daraus ergibt sich mit (3.3)

$$\begin{aligned} F_k(x) &\geqslant \frac{1}{x(k-1)!} \tilde{x}^{2(1-c_1)} \ln^{k-1}\left(\frac{x}{2\tilde{x}}\right) \\ &\geqslant x^{1-5c_1}. \end{aligned} \tag{3.5}$$

Andererseits ist

$$F_k(x) \leqslant \frac{\ln^{k-1} x}{(k-1)!} + \frac{1}{x} \int_{x^{1/2}}^{x} dx_{k-1} \cdots \frac{1}{x_1} \int_{x^{1/2}}^{x_1} dt\, \eta(t)$$

Mit der expliziten Formel

$$\sum_{n \leqslant t} \chi(n) \Lambda(n) = - \sum_{|\rho| \leqslant x^{1/2}} \frac{t^\rho}{\rho} + O(t x^{-1/2} \ln^2 x)$$

($x^{1/2} \leqslant t \leqslant x$, und ρ durchläuft die nichttrivialen Nullstellen von $L(s, \chi)$) ergibt sich daraus

$$F_k(x) \leqslant - \sum_{|\rho| \leqslant x^{1/2}} \frac{1}{x} \int_{x^{1/2}}^{x} dx_{k-1} \cdots \frac{1}{x_1} \int_{x^{1/2}}^{x_1} dt \int_{x^{1/2}}^{t} dv \frac{v^{\rho-1}}{\ln v} + O\left(\frac{\ln^{k+1} x}{(k-1)!} x^{1/2}\right). \tag{3.6}$$

Zu vorgegebenem (am Ende hinreichend groß gewähltem) $c_3 > 1$ kann $c_4 = c_4(P)$ so gewählt werden, daß für alle ρ mit $\operatorname{Re} \rho > 1 - c_4$ die Ungleichung $|\rho + 1| \geqslant c_3$ erfüllt ist. Die ρ werden durch 1) $\operatorname{Re} \rho \leqslant 1 - c_4$, 2) $\operatorname{Re} \rho > 1 - c_4$ in zwei Klassen eingeteilt. Für ein ρ gemäß 1) ist

$$\int_{x^{1/2}}^{t} dv \frac{v^{\rho-1}}{\ln v} \ll \frac{x^{1-c_4}}{|\rho| \ln x},$$

der Beitrag dieser ρ zu (3.6) somit $\ll x^{1-c_4} \ln x$. Für die übrigen ρ wird mehrfach

partiell integriert

$$\int_{x^{1/2}}^{t} dv \frac{v^{\rho-1}}{\ln v} = \frac{t_\rho}{\rho \ln t} + \cdots + \frac{(k-1)! t^\rho}{\rho^k \ln^k t} + O\left(\frac{k!}{|\rho|^k} \frac{t}{(\ln x^{1/2})^{k+1}}\right) + O\left(\frac{x^{1/2}}{|\rho|} \max_{0 \leqslant v \leqslant k-1} \frac{v!}{(\ln x^{1/2})^{v+1}}\right).$$

Weiteres Integrieren wie in (3.6) ergibt, wie man sich induktiv überzeugt,

$$\begin{aligned} F_k(x) \leqslant & - \sum_{\substack{|\rho| \leqslant x^{1/2} \\ \mathrm{Re}\rho > 1-c_4}} \left\{ \frac{x^\rho}{\rho(\rho+1)^k} \left(\frac{k!}{k! \ln x} + \frac{(k+1)!}{\rho k! \ln x} + \cdots + \frac{(2k-1)!}{\rho^{k-1} k! \ln^k x} \right) \right. \\ & \left. + O\left(\frac{(2k)!}{|\rho|^k k!} \frac{x}{(\ln x^{1/2})^{k+1}} \right) + O\left(\frac{x^{1/2}}{|\rho|} \max_{0 \leqslant v \leqslant k-1} \frac{v!}{(\ln x^{1/2})^{v+1}} \right) \right\} \\ & + O(x^{1-c_4} \ln x) + O\left(\frac{\ln^{k+1} x}{(k-1)!} x^{1/2} \right) \\ \ll & \, x c_3^{-k} + x \frac{(2k)!}{k!} \left(\frac{1}{2} \ln x \right)^{-k} \\ & + x^{1/2} \ln^2 x + x^{1-c_4} \ln x + x^{1/2} \frac{(\ln x)^{k+1}}{(k-1)!}, \end{aligned} \tag{3.7}$$

und, da $k = \left[\frac{1}{2} c_1 \ln x\right]$ gewählt war,

$$\ll \ln^2 x \left(x^{1-1/2c_1 \ln c_3} + x^{1+1/2c_1 \ln(4e^{-1}c_1)} + x^{1-c_4} + x^{1+1/2c_1 \ln(3ec_1^{-1})-1/2} \right).$$

Verglichen mit (3.5) besagt dies

$$5c_1 \geqslant \min\left(\frac{1}{2} c_1 \ln c_3, \frac{1}{2} c_1 \ln(e(4c_1)^{-1}), c_4, \frac{1}{2} - \frac{1}{2} c_1 \ln(3ec_1^{-1}) \right). \tag{3.8}$$

Nimmt man $c_3 > e^{10}$ und $c_1 \leqslant \frac{1}{6} c_4$, dann kann schließlich c_1 so klein gewählt werden, daß (3.8) widersprüchlich wird. Damit ist Lemma 1 gezeigt.

Die Idee, die Nullstellensumme mehrfach zu integrieren, geht auf TURÁN [4] zurück.

Lemma 2. *Es existiert ein $c_5 > 0$, so daß für alle n $d_n \ll p_n^{1-c_5}$ gilt.*

Beweis. Es kann angenommen werden, daß für das c_1 aus Lemma 1 der Hoheisel-Inghamsche Primzahlsatz Gültigkeit hat:

$$\pi(x+y, P, a) - \pi(y, P, a) \sim \frac{y}{(P-1)\ln x} \tag{3.9}$$

für $x^{1-c_1} \leqslant y \leqslant x$ und (a, P) = 1. Für hinreichend großes x sei $I = (x, x + x^{1-c_1}]$,

$x < p_{n_1} < \cdots < pn_k \leqslant x + x^{1-c_1}$ seien die $p_n \in I$. Nach (3.9) ist

$$k \sim \frac{1}{2}\frac{x^{1-c_1}}{\ln x}.$$

Wegen Lemma 1 gilt – wieder OBdA mit $d_n > 0 (n \geqslant n_o)$ –

$$0 \leqslant \eta(\xi) \leqslant x^{1-c_1} \text{ für ein } \xi \in I,$$

für beliebiges $y \in I$ also

$$0 \leqslant \eta(y) \leqslant \eta(\xi) + |\xi - y| \leqslant 2x^{1-c_1}. \tag{3.10}$$

Aus der Annahme

$$d_{n_j} = q_{n_j} - p_{n_j} > 5x^{1-c_1} \ln x \text{ für ein } j \in \{1, \ldots, k\} \tag{3.11}$$

folgt mit (3.9)

$$\#\{q_n \in (p_{n_j}, q_{n_j}]\} > 2x^{1-c_1}$$

und somit

$$\eta(p_{n_j}) = n_j - \#\{q_n \leqslant p_{n_j}\} > n_j - (n_j - 2x^{1-c_1}) = 2x^{1-c_1},$$

was (3.10) widerspricht. Es gilt daher die Behauptung des Lemmas mit $c_5 = c_1/2$.

4. Beweis des Satzes im Fall der Nicht-Gültigkeit der Riemannschen Vermutung für $L(s, \varkappa)$

Es werde wieder OBdA $d_n > 0$ für $n \geqslant n_0$ vorausgesetzt. $\log L(s, \chi)$ bezeichne den Zweig des Logarithmus, bei dem $\log L(s, \chi) \to 0$ für $\sigma \to +\infty$ gilt. $H_v(s)$ bezeichne Funktionen, die für $\sigma > \frac{1}{2}$ holomorph sind. Dann gilt für $\sigma > 1$

$$\begin{aligned}\log L(s, \chi) &= \sum_p \frac{\chi(p)}{p^s} + H_1(s) = \sum_{n \geqslant n_0} \left(\frac{1}{p_n^s} - \frac{1}{q_n^s}\right) + H_2(s) \\ &= s \sum_{n \geqslant n_0} \frac{d_n}{p_n^{s+1}} + \sum_{2 \leqslant k \leqslant c_6} (-1)^{k+1} \frac{s(s+1)\cdots(s+k-1)}{k!} \sum_{n \geqslant n_o} \frac{d_n^k}{p_n^{s+k}} + H_3(s).\end{aligned} \tag{4.1}$$

Die letzte Aussage wird ermöglicht durch Lemma 2, wonach die Reihe

$$G_k(s) = \sum_{n \geqslant n_o} d_n^k p_n^{-s-k}$$

für hinreichend großes k eine Konvergenzabszisse $\sigma_{0,k} \leqslant \frac{1}{2}$ hat. Nach Lemma 2 bestehen die Ungleichungen

$$1 > \sigma_{0,1} > \sigma_{0,2} > \cdots.$$

Es muß $\sigma_{0,1} > \frac{1}{2}$ sein, denn sonst wäre nach (4.1) $\log L(s, \chi)$ holomorph für $\sigma > \frac{1}{2}$, im Gegensatz zur Annahme einer Nullstelle von $L(s, \chi)$ mit Realteil $> \frac{1}{2}$.

Nach einem bekannten Satz von Landau hat wegen $d_n > 0\,(n \geqslant n_o)\, G_1(s)$ bei $s = \sigma_{0,1}$ eine Singularität, während $G_2(s), \ldots, G_{c_7}(s)$ in $\{\sigma > \sigma_{0,1} - c_8\}$ holomorph sind. Dies bewirkt nach (4.1) eine Singularität von $\log L(s, \chi)$ bei $s = \sigma_{0,1} > \frac{1}{2}$, was aber wegen (Hp) nicht möglich ist. Damit ist der Satz auch in diesem Fall bewiesen.

Literatur

[1] LITTLEWOOD JE (1914) Sur la distribution des nombres premiers. CR Acad Sci Paris **158**: 1869–1872
[2] PRACHAR K (1957) Primzahlverteilung. Berlin Göttingen Heidelberg: Springer
[3] ROSSER JB (1950) Real roots of real Dirichlet L-series. J of Research of the Natl Bureau of Standards **45**: 505–514
[4] TURÁN P (1938/40) Über die Primzahlen der arithmetischen Progression. II. Acta Sci Math Szeged **9**: 187–192
[5] TURÁN P (1984) On a New Method of Analysis and its Applications. New York: Wiley

J. C. PUCHTA and D. WOLKE
Mathematisches Institut
Eckerstr. 1
D-79104 Freiburg
Deutschland