

XI. Fin de la démonstration.

(a) *Cas du théorème 1.* En regroupant les formules (2), (6), (12), (15), (23) et (40) on obtient:

$$E^2(Q) \ll MQ \{MN^2Q^{-1}(\log X)^{-2A-2} + N^{5/2}Q^{-1}X^{7\epsilon} + N^{11/4}Q^{-1}X^{3\epsilon} + MNX^{\epsilon/2}\}$$

soit encore, pour ϵ suffisamment petit par rapport à η

$$E^2(Q) \ll M^2N^2(\log X)^{-2A-2} + MN^{11/4}X^{3\epsilon} \ll M^2N^2(\log X)^{-2A-2}$$

d'après la condition (iii), pourvu que ϵ soit suffisamment petit par rapport à δ_0 . La formule (1) est démontrée.

(b) *Cas du théorème 2.* De même avec les formules (2), (6), (12), (15), (26) et (40), on a:

$$E^2(Q) \ll MQ \{L^2MN^2Q^{-1}(\log X)^{-2A-2} + L^3N^{5/2}Q^{-1}X^{7\epsilon} + L^{11/4}N^3Q^{-1}X^{5\epsilon} + LMNX^{\epsilon/2}\}$$

$$\ll L^2M^2N^2(\log X)^{-2A-2}$$

sous la condition (iii) et ϵ suffisamment petit par rapport à η et δ_0 , ce qui termine la démonstration du théorème 2.

(c) *Cas du théorème 3.* De même avec les formules (2), (6), (12), (15), (36) et (40), on a:

$$E^2(Q) \ll MQ \{MN^2Q^{-1}(\log X)^{-2A-2} + N^{29/10}Q^{-1}X^{9\epsilon}\} \ll M^2N^2(\log X)^{-2A-2}$$

sous la condition (iii) et ϵ suffisamment petit. Le théorème 3 est démontré.

Bibliographie

- [1] J. R. Chen, *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica (1973), p. 157-176.
- [2] E. Fouvry and H. Iwaniec, *On a theorem of Bombieri-Vinogradov type*, Mathematika 27 (1980), p. 135-152.
- [3] G. Greaves, *A weighted sieve of Brun's type*, Acta Arith. 40 (1982), p. 297-332.
- [4] C. Hooley, *On the greatest prime factor of a cubic polynomial*, J. Reine Angew. Math. 303/304 (1978), p. 21-50.
- [5] M. Laborde, *Buchstab's sifting weights*, Mathematika 26 (1979), p. 250-257.
- [6] R. C. Vaughan, *On the estimation of trigonometric sums over primes and related questions*, Institut Mittag-Leffler, Report n°9 (1977).

U.E.R. DE MATHÉMATIQUES ET D'INFORMATIQUE
UNIVERSITÉ DE BORDEAUX I
F 33405 Talence Cedex

Reçu le 21. 10. 1980

et dans la forme modifiée le 2. 2. 1981

(1228)

Erweiterung eines Satzes von Schinzel über Potenzreste

von

VOLKER SCHULZE (West Berlin)

Es sei K ein algebraischer Zahlkörper und $n \in \mathbb{N}$ eine natürliche Zahl. Für eine ganze Zahl $a \in K$, $a \neq 0$, wird mit $P_K(a, n)$ die Menge aller Primideale \mathfrak{p} von K bezeichnet, für die die Kongruenz

$$X^n \equiv a \pmod{\mathfrak{p}}$$

lösbar ist. In einer Reihe von Arbeiten (siehe [1] bis [8]) wird untersucht, wann $P_K(a, n) \supseteq P_K(b, m)$ bzw. $P_K(a, n) \subseteq P_K(b, m)$ gilt; d.h. $P_K(a, n) = P_K(b, m)$ bzw. $P_K(a, n) \subseteq P_K(b, n)$ bis auf endlich viele Ausnahmen. Ein einfaches notwendiges und hinreichendes Kriterium ist bisher nur in Spezialfällen bekannt, und zwar für $P_K(a, n) \subseteq P_K(b, m)$ unter der Voraussetzung $n|m$ durch Schinzel [4] und für $P_Q(a, n) \supseteq P_Q(b, m)$ durch Schulze [7]. Die übrigen bisher bekannten Resultate sind Spezialfälle hiervon.

In der vorliegenden Arbeit werden diese Ergebnisse durch die Sätze 2 und 3 erweitert. Beim Beweis von Satz 3 wird zurückgegriffen auf die Arbeit von Schinzel. Für $g \in \mathbb{N}$ bezeichne ζ_g eine primitive g -te Einheitswurzel. Dann gilt

SATZ 1 (Schinzel [4]). *Es sei K ein algebraischer Zahlkörper und τ die größte natürliche Zahl derart, daß $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$. Ferner seien n, m aus \mathbb{N} mit $n|m$. Dann ist*

$$P_K(a, n) \subseteq P_K(b, m)$$

genau dann, wenn es eine Zahl $s \in \mathbb{N}$ und ein $d \in K$ gibt derart, daß wenigstens eine der folgenden Bedingungen erfüllt ist:

- (1) $a^{\frac{m}{n} \cdot s} \cdot b = d^m$;
- (2) $m \not\equiv 0 \pmod{2^\tau}$, $a^{\frac{m}{n} \cdot s} \cdot b = -d^m$, $\prod_{2|n} a^l = -c^2$ für ein $c \in K$, $l \in \mathbb{N}$;
- (3) $m \equiv 2^\tau \pmod{2^{\tau+1}}$, $a^{\frac{m}{n} \cdot s} \cdot b = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{m/2} \cdot d^m$,
 $\prod_{2|n} a^l = -c^2$ für ein $c \in K$, $l \in \mathbb{N}$;
- (4) $m \equiv 0 \pmod{2^{\tau+1}}$, $a^{\frac{m}{n} \cdot s} \cdot b = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{m/2} \cdot d^m$.

Eine Erweiterung von Satz 1 auf alle n, m , für die ein $d \in N$ existiert mit $(d, m) = 1$ und $n \mid m \cdot d$ liefert der einfach zu beweisende

SATZ 2. Für jedes $d \in N$ mit $(d, n) = 1$ gilt

$$P_K(a, n) = P_K(a^d, n \cdot d).$$

Beweis. Trivialerweise gilt $P_K(a, n) \subseteq P_K(a^d, n \cdot d)$. Im Fall $a \equiv 0 \pmod{p}$ sind $x^n \equiv a \pmod{p}$ und $x^{n \cdot d} \equiv a^d \pmod{p}$ lösbar. Es gelte also $a \not\equiv 0 \pmod{p}$ und für eine ganze Zahl $b \in K$

$$b^{n \cdot d} \equiv a^d \pmod{p}.$$

Für λ, μ aus Z mit $\lambda n + \mu d = 1$ folgt dann

$$(a^\lambda \cdot b^{d\mu})^n \equiv a^{d\lambda + \mu n} \equiv a \pmod{p},$$

wobei die Inversenbildung beim Auftreten negativer Exponenten im Restklassenkörper mod p erfolgt.

Insgesamt ergibt sich die Behauptung.

Eine weitere Verallgemeinerung von Satz 1 liefert die folgende Aussage. Für $g \in \mathcal{O}$ bezeichne $v_p(g)$ den Exponenten der Primzahl p in der kanonischen Primfaktorzerlegung von g . Dann gilt

SATZ 3. Es seien n, m natürliche Zahlen mit $v_2(n) \leq v_2(m)$ und n' das Produkt aller Primzahlen p mit $0 < v_p(m) < v_p(n)$. Es bezeichne $v = [n, m]$ den kgV von n und m . Ferner sei K ein algebraischer Zahlkörper, w die Anzahl der Einheitswurzeln in K und τ die größte natürliche Zahl derart, daß $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$. Weiter sei w_p die Anzahl der Einheitswurzeln in $K(\zeta_p)$. Es seien a, b aus K , $a \neq 0$, $b \neq 0$ und r der kleinste Teiler von n derart, daß ein $a_1 \in K$ existiert mit

$$a = a_1^{n/r}.$$

Die Wurzel $\sqrt[n]{a}$ sei so gewählt, daß $\sqrt[n]{a^r} = a_1$ ist. Erfüllt nun K die Bedingung

$$(5) \quad (w, r, n') = 1,$$

so ist $P_K(a, n) \subseteq P_K(b, m)$ gleichwertig mit der folgenden Aussage: Es existieren Zahlen $s \in N$, $d \in K$, eine Wurzel $\sqrt[m]{b}$ und primitive Einheitswurzeln ζ_{2^m}, ζ_k mit

$$(6) \quad k \mid n,$$

$$(7) \quad v_p(k) \leq \max\{v_p(m), v_p(w_p)\}, \text{ falls } p \mid n',$$

$$(8) \quad v_p(r) \leq v_p(s), \text{ falls } \max\{v_p(m), v_p(w_p)\} + v_p(s) < v_p(n) \text{ und } p \mid n'$$

derart, daß wenigstens eine der folgenden Aussagen gilt:

$$(9) \quad \zeta_k \sqrt[n]{a^s} \sqrt[m]{b} = d,$$

$$(10) \quad m \not\equiv 0 \pmod{2^\tau}, \zeta_{2^m} \zeta_k \sqrt[n]{a^s} \sqrt[m]{b} = d, \prod_{2 \mid n} a^l = -c^2 \text{ für ein } c \in K, l \in N,$$

$$(11) \quad m \equiv 2^\tau \pmod{2^{\tau+1}}, \zeta_{2^m} \zeta_k \sqrt[n]{a^s} \sqrt[m]{b} = \sqrt{\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2} \cdot d, \prod_{2 \mid n} a^l = -c^2 \text{ für ein } c \in K, l \in N,$$

$$(12) \quad m \equiv 0 \pmod{2^{\tau+1}}, \zeta_k \sqrt[n]{a^s} \sqrt[m]{b} = \sqrt{\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2} \cdot d.$$

Ein Nachteil von Satz 3 besteht darin, daß zur Beschreibung der Beziehung $P_K(a, n) \subseteq P_K(b, m)$ Eigenschaften der Nullstellen von $x^n - a$ und $x^m - b$ herangezogen werden. In Spezialfällen läßt sich dies vermeiden.

Ist K reeller Zahlkörper, so kann $\sqrt[n]{a}$ offenbar immer so gewählt werden, daß $\sqrt[n]{a}$ reell ist, falls $a > 0$, oder $\zeta_{2^{v_2(n)}} \sqrt[n]{a}$ reell ist, falls $a < 0$. Durch geeignete Wahl der Wurzel $\sqrt[m]{b}$ kann dann immer erreicht werden, daß ζ_k reell ist, also auch $k = 1$. Im Fall $\frac{n}{r} \mid w$ kann in Satz 3 die Wurzel $\sqrt[n]{a}$ beliebig gewählt werden, also auch so, daß $k = 1$ ist. Damit ergibt sich aus Satz 3 der folgende Spezialfall:

FOLGERUNG 1. Es sei K reell oder $\frac{n}{r} \mid w$. Mit den Bezeichnungen aus Satz 3 ist dann

$$P_K(a, n) \subseteq P_K(b, m)$$

gleichwertig damit, daß ein $d \in K$ und ein $s \in N$ existiert mit

$$(13) \quad v_p(r) \leq v_p(s), \text{ falls } \max\{v_p(m), v_p(w_p)\} + v_p(s) < v_p(n) \text{ und } p \mid n' \text{ derart, daß wenigstens eine der folgenden Aussagen gilt:}$$

$$(14) \quad a^{\frac{v}{n} \cdot s} \cdot b^{\frac{v}{m}} = d^v,$$

$$(15) \quad m \not\equiv 0 \pmod{2^\tau}, a^{\frac{v}{n} \cdot s} \cdot b^{\frac{v}{m}} = -d^v, \prod_{2 \mid n} a^l = -c^2 \text{ für ein } c \in K, l \in N,$$

$$(16) \quad m \equiv 2^\tau \pmod{2^{\tau+1}}, a^{\frac{v}{n} \cdot s} \cdot b^{\frac{v}{m}} = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{v/2} \cdot d^v, \prod_{2 \mid n} a^l = -c^2 \text{ für ein } c \in K, l \in N,$$

$$(17) \quad m \equiv 0 \pmod{2^{\tau+1}}, a^{\frac{v}{n} \cdot s} \cdot b^{\frac{v}{m}} = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{v/2} \cdot d^v.$$

Offenbar ist $n' = 1$ genau dann, wenn ein $d \in N$ existiert mit $(d, m) = 1$ und $n | m \cdot d$. Wird die s einschränkende Bedingung (13) in Folgerung 1 fortgelassen, so erhält man eine Aussage, welche nach Satz 3 unter der Voraussetzung $n' = 1$ für alle algebraischen Zahlkörper K gilt. Dieselbe Aussage erhält man offenbar mit Hilfe von Satz 2' aus Satz 1. Satz 3 ist also tatsächlich eine Verallgemeinerung von Satz 1.

Im folgenden soll nun Satz 3 bewiesen werden. Zur Vorbereitung werden zunächst einige Hilfssätze zusammengestellt. Nach den bekannten Gesetzen über die Zerlegung der Primideale in algebraischen Zahlkörpern gilt

HILFSSATZ 1. *Es sei E eine endliche Körpererweiterung von K , in der $(X^n - a) \cdot (X^m - b)$ in Linearfaktoren zerfällt. Dann ist $P_K(a, n) \subseteq P_K(b, m)$ gleichwertig damit, daß jeder Automorphismus von $E : K$ mit einer Nullstelle von $X^n - a$ auch eine von $X^m - b$ auf sich abbildet.*

HILFSSATZ 2. *Es sei a eine ganze Zahl aus K , $\sqrt[n]{a}$ eine beliebige Nullstelle von $X^n - a$ und δ ein Automorphismus des Zerfällungskörpers von $X^n - a$ über K mit*

$$\delta(\zeta_n) = \zeta_n^{1+j}, \quad \delta(\sqrt[n]{a}) = \zeta_n^g \sqrt[n]{a}.$$

Dann läßt δ eine Nullstelle von $X^n - a$ fest genau dann, wenn $(j, n) | g$.

Beweis. Genau dann gibt es eine Nullstelle $\zeta_n^l \sqrt[n]{a}$ ($l \in \mathbb{Z}$) von $X^n - a$ mit

$$\delta(\zeta_n^l \sqrt[n]{a}) = \zeta_n^{l+j} \zeta_n^g \sqrt[n]{a} = \zeta_n^l \sqrt[n]{a},$$

wenn es ein $l \in \mathbb{Z}$ gibt mit $l \cdot j + g \equiv 0 \pmod{n}$. Hieraus ergibt sich die Behauptung.

HILFSSATZ 3 (Schinzel [6]). *Es sei $n \in N$. Gilt für ein $a \in K$*

$$a = \vartheta^n, \quad \vartheta \in K(\zeta_n),$$

so gibt es ein $\gamma \in K$ mit

$$a = \gamma^n,$$

wobei

$$\sigma = (w', \text{kgV} [K(\zeta_n):K])$$

$q | n$,
 q Primzahl
oder $q=4$

und w' die Anzahl der n -ten Einheitswurzel in K ist.

HILFSSATZ 4. *Es sei $n \in N$, $a \in K$ und w die Anzahl der Einheitswurzeln in K . Ferner sei r der kleinste Teiler von n derart, daß ein $b \in K$ existiert mit*

$$a = b^{n/r}$$

und s der kleinste Teiler von n derart, daß ein $c \in K$ existiert mit

$$a^s = c^n.$$

Dann gilt $s | r$, und jeder Primteiler von r/s teilt w .

Beweis. Die Gültigkeit von $s | r$ ist klar. Nach Voraussetzung gilt für eine geeignete Einheitswurzel $\zeta \in K$

$$a = c^{n/s} \cdot \zeta.$$

Wegen $\frac{n}{r} \mid \frac{n}{s}$ ist $\zeta^{\frac{n}{r}}$ $\frac{n}{r}$ -te Potenz einer Zahl $\zeta' \in K$. Dabei muß ζ' w -te

Einheitswurzel sein. Ist p nun eine Primzahl mit $p \mid \frac{r}{s}$, $p \nmid w$, so gilt für Zahlen $\lambda, \mu \in \mathbb{Z}$ mit $\lambda p + \mu w = 1$

$$\zeta' = \zeta'^{1-\mu w} = \zeta'^{\lambda p},$$

also

$$a = (c^{\frac{r}{s} p} \cdot \zeta'^{\lambda})^{\frac{n}{r} p}, \quad c \in K, \zeta' \in K.$$

Die letzte Gleichung steht im Widerspruch zur Definition von r . Benötigt werden ferner die folgenden bekannten Aussagen.

HILFSSATZ 5 (Flanders [2]). *Ist p Primzahl und $a \in K$, $\zeta_p \in K$, $\sqrt[p]{a} \notin K$, so gilt $[K(\sqrt[p]{a}):K] = p$.*

HILFSSATZ 6 (Flanders [2]). *Es sei $p \neq 2$ Primzahl, $a \in N$ und $\zeta_{p^a} \in K$, $\zeta_{p^{a+1}} \notin K$. Dann ist*

$$[K(\zeta_{p^{a+1}}):K] = p.$$

HILFSSATZ 7 (Schulze [7]). *Es seien n, m natürliche Zahlen mit $m | n$. Ein Automorphismus σ von $K(\zeta_n)$ mit $\sigma(\zeta_n) = \zeta_n^{1+j}$ läßt ζ_m invariant genau dann, wenn $m | j$.*

Beweis von Satz 3. Wir nehmen zunächst $P_K(a, n) \subseteq P_K(b, m)$ an. Da jede Nullstelle von $X^m - b$ auch Nullstelle von $X^v - b^{v/m}$ ist, folgt nach Hilfssatz 1 $P_K(a, n) \subseteq P_K(b^{v/m}, v)$ und daraus nach Satz 1 von

Schinzel die Existenz von Zahlen $s \in N$, $d \in K$, einer Wurzel $\sqrt[s]{b}$ und primitiven Einheitswurzeln ζ_{2m}, ζ_k mit $k | n$ derart, daß eine der Beziehungen (9), (10), (11) oder (12) gilt. Nachzuweisen bleibt noch die Gültigkeit von (7) und (8). Nach Hilfssatz 1 müssen dazu die Automorphismen

des Körpers $E = K(\zeta_{2v}, \sqrt[s]{a}, \sqrt[s]{b})$ über K untersucht werden. Es sei im folgenden $\zeta_{2v}, \zeta_v, \zeta_n, \zeta_m$ fest gewählt, und zwar so, daß gilt

$$\zeta_{2v}^{2v/k} = \zeta_k, \quad \zeta_v = \zeta_{2v}^2, \quad \zeta_n = \zeta_{2v}^{2v/n}, \quad \zeta_m = \zeta_{2v}^{2v/n}.$$

Bei geeigneter Wahl von $\sqrt[m]{b}$ läßt sich offenbar immer erreichen, daß gilt

$$\zeta_{2m} = \zeta_{2v}^{2v/2m}.$$

Wir nehmen zunächst an, daß (7) nicht gilt. Es gelte also für eine Primzahl q

$$(18) \quad v_q(k) > \max\{v_q(m), v_q(w_q)\}, \quad q|n'.$$

Hieraus wird ein Widerspruch hergeleitet, indem ein Automorphismus σ von $E:K$ konstruiert wird, welcher eine Nullstelle von $X^n - a$ festläßt, jedoch keine Nullstelle von $X^m - b$. Es bezeichne r_1 den kleinsten Teiler von r derart, daß

$$(19) \quad \sqrt[n]{a^{r_1}} \in K(\zeta_n)$$

ist. Zunächst wird

$$(20) \quad q \nmid [K(\sqrt[n]{a^{r_1}}):K]$$

nachgewiesen. Wegen $\sqrt[n]{a^{r_1}} = a_1 \in K$ genügt es zu zeigen, daß r/r_1 nur Primteiler p mit $p|w$ enthält; denn dann ergibt sich durch wiederholte Anwendung von Hilfssatz 5, daß

$$[K(\sqrt[n]{a^{r_1}}):K]$$

nur Primteiler von r/r_1 und damit auch nur von (r, w) enthalten kann, woraus wegen (5) sofort (20) folgt. Nach (19) ist a^{r_1} n -te Potenz eines Elementes aus $K(\zeta_n)$. Bezeichnet r_2 den kleinsten Teiler von n derart, daß ein $a_2 \in K$ existiert mit

$$a^{r_2} = a_2^n,$$

so ist $r_2|r_1 w$ nach Hilfssatz 3, also

$$\frac{r}{r_1} \mid \frac{r}{r_2} \cdot w.$$

Nach Hilfssatz 4 besitzt r/r_2 nur Primteiler p mit $p|w$. Damit ist (20) bewiesen.

Für jede Primzahl p wird die Abkürzung

$$m_p = \max\{v_p(m), v_p(w_p)\}$$

verwendet. Dann ist $m_q \geq 1$ und damit nach Hilfssatz 6

$$[K(\zeta_q^{m_q+1}):K(\zeta_q^{m_q})] = q.$$

Zusammen mit (20) ergibt sich hieraus die Existenz eines Automorphismus σ mit

$$(21) \quad \sigma(\zeta_q^{m_q}) = \zeta_q^{m_q},$$

$$(22) \quad \sigma(\zeta_q^{m_q+1}) \neq \zeta_q^{m_q+1},$$

$$(23) \quad \sigma(\sqrt[n]{a_1})^{r_1} = \sqrt[n]{a_1}^{r_1}.$$

Wegen (23) folgt

$$(24) \quad \sigma(\sqrt[n]{a}) = \sqrt[n]{a} \zeta_v^{\lambda v} = \sqrt[n]{a} \zeta_n^{\lambda n} \quad \text{für ein } \lambda \in \mathbf{Z}.$$

Wegen (19) gibt es für beliebiges $\lambda_1 \in \mathbf{Z}$ einen Automorphismus σ' von $E:K$ mit

$$\begin{aligned} \sigma'(\zeta_n) &= \zeta_n, \\ \sigma'(\sqrt[n]{a}) &= \sqrt[n]{a} \cdot \zeta_n^{\lambda_1 n}. \end{aligned}$$

Es sei $\lambda_1 = -\lambda$.

Betrachtet man anstelle von σ den Automorphismus $\sigma' \circ \sigma$, so erkennt man, daß ohne Einschränkung der Allgemeinheit σ so gewählt werden kann, daß neben (21) und (22) gilt

$$(25) \quad \sigma(\sqrt[n]{a}) = \sqrt[n]{a}.$$

Offenbar läßt σ dann eine Nullstelle von $X^n - a$ fest. Es wird andererseits nun gezeigt, daß σ keine Nullstelle von $X^m - b$ festlassen kann. Es gelte $\sigma(\zeta_{2v}) = \zeta_{2v}^{1+j}$, also $\sigma(\zeta_m) = \zeta_m^{1+j}$. Wegen (21) und (22) folgt nach Hilfssatz 7

$$(26) \quad v_q(j) = m_q,$$

nach Definition von m_q also

$$(27) \quad v_q(j, m) = v_q(m).$$

Da (25) gilt und eine der Gleichungen (9), (10), (11) oder (12) kommt für $\sigma(\sqrt[m]{b})$ nur eins der folgenden vier Elemente in Frage:

$$\sqrt[m]{b} \zeta_m^{-\frac{m}{k} \cdot j}, \quad \sqrt[m]{b} \zeta_m^{-\left(\frac{m}{k} \cdot j + \frac{m}{2}\right)}, \quad \sqrt[m]{b} \zeta_m^{-\left(\frac{m}{k} \cdot j + \frac{j}{2}\right)}, \quad \sqrt[m]{b} \zeta_m^{-\left(\frac{m}{k} \cdot j + \frac{j+m}{2}\right)}.$$

Der Exponent von ζ_m ist dabei immer ganzzahlig. Wegen (18) und (26) ist

$$v_q\left(\frac{m}{k} \cdot j\right) < v_q(m).$$

Da q als Primteiler von n' ungerade ist, gilt

$$(28) \quad v_q(m/2) = v_q(m),$$

und nach (27) außerdem

$$(29) \quad v_q(j/2) \geq v_q(m).$$

Zusammen ergibt sich nach Hilfssatz 2, daß σ keine Nullstelle von $X^m - b$ festlassen kann. Damit ist die Gültigkeit von (7) nachgewiesen.

Wir nehmen nun an, daß (8) nicht gilt. Es sei also für einen Primteiler q von n'

$$(30) \quad v_q(r) > v_q(s)$$

und

$$(31) \quad m_q + v_q(s) < v_q(n).$$

Zu konstruieren ist wieder ein Automorphismus σ von $E:K$, welcher eine Nullstelle von $X^n - a$ festläßt, jedoch keine von $X^m - b$. Die Konstruktion erfolgt analog zum vorangegangenen Fall. Betrachtet wird ein Automorphismus σ , welcher (21), (22) und (24) erfüllt und anstelle von (25) die Kongruenzen

$$(32) \quad \lambda \frac{n}{r_1} \equiv 0 \pmod{p^{v_p(n)}}, \quad p \text{ Primteiler von } n, p \neq q,$$

$$(33) \quad \lambda \frac{n}{r_1} \equiv q^{v_q(n) - v_q(s) - 1} \pmod{q^{v_q(n) - v_q(s)}}.$$

Einen solchen Automorphismus σ gibt es, da nach dem chinesischen Restsatz ein λ_1 existiert mit

$$\lambda_1 \frac{n}{r_1} + \frac{\lambda n}{r_1} \equiv 0 \pmod{p^{v_p(n)}}, \quad p \text{ Primteiler von } n, p \neq q$$

und

$$\lambda_1 \frac{n}{r_1} + \frac{\lambda n}{r_1} \equiv q^{v_q(n) - v_q(s) - 1} \pmod{q^{v_q(n) - v_q(s)}}.$$

Die zur Anwendung des chinesischen Restsatzes hinreichende Bedingung

$$v_q\left(\frac{n}{r_1}\right) \leq v_q(n) - v_q(s) - 1$$

ist erfüllt wegen (30) und $v_q(r) = v_q(r_1)$. Die letzte Gleichung wurde bereits zum Nachweis von (20) hergeleitet. Wegen der Gültigkeit von (26), (31), (32) und (33) gilt

$$(34) \quad (j, n) \mid \lambda \frac{n}{r_1}.$$

Nach Hilfssatz 2 läßt σ also eine Nullstelle von $X^n - a$ fest.

Andererseits kommt für $\sigma(\sqrt[b]{b})$ nur eins der folgenden vier Elemente

in Frage:

$$\frac{m}{\sqrt[b]{b}} \cdot \zeta_m^{-\left(\frac{\lambda sm}{r_1} + \frac{m}{k} \cdot j\right)}, \quad \frac{m}{\sqrt[b]{b}} \cdot \zeta_m^{-\left(\frac{\lambda sm}{r_1} + \frac{m}{k} \cdot j + \frac{m}{2}\right)}, \quad \frac{m}{\sqrt[b]{b}} \cdot \zeta_m^{-\left(\frac{\lambda sm}{r_1} + \frac{m}{k} \cdot j + \frac{j}{2}\right)}, \quad \frac{m}{\sqrt[b]{b}} \cdot \zeta_m^{-\left(\frac{\lambda sm}{r_1} + \frac{m}{k} \cdot j + \frac{m}{2} + \frac{j}{2}\right)}.$$

Wie im vorigen Fall gilt wieder (28) und (29) und wegen (7) und (26) außerdem

$$v_q\left(\frac{m}{k} \cdot j\right) \geq v_q(j, m).$$

Weiter ist

$$v_q(\lambda sm/r_1) < v_q(m, j),$$

denn es gilt (27) und nach (33)

$$v_q(\lambda n/r_1) = v_q(n) - v_q(s) - 1.$$

Insgesamt folgt, daß σ keine Nullstelle von $X^m - b$ festlassen kann. Damit ist die Gültigkeit von (8) nachgewiesen.

Wir nehmen nun an, daß (6), (7) und (8) gilt und eine der Gleichungen (9), (10), (11) oder (12). Dann ist $P_K(a, n) \subseteq P_K(b, m)$ zu beweisen. Ein Automorphismus σ von $E:K$ läßt sich vollständig beschreiben durch zwei Gleichungen der Form

$$\sigma(\zeta_{2v}) = \zeta_{2v}^{1+j}, \quad \sigma(\sqrt[a]{a}) = \sqrt[a]{a} \cdot \zeta_v^{\lambda \frac{v}{r}} = \sqrt[a]{a} \zeta_n^{\lambda \frac{n}{r}}.$$

Ohne Einschränkung der Allgemeinheit sei wieder

$$\zeta_{2v}^{2v/k} = \zeta_k, \quad \zeta_v = \zeta_{2v}^2, \quad \zeta_n = \zeta_{2v}^{2v/n}, \quad \zeta_m = \zeta_{2v}^{2v/m}, \quad \zeta_{2m} = \zeta_{2v}^{2v/2m}.$$

Dann gilt

$$\sigma(\zeta_n) = \zeta_n^{1+j}, \quad \sigma(\zeta_m) = \zeta_m^{1+j},$$

$$(35) \quad \sigma(\sqrt[b]{b}) = \frac{m}{\sqrt[b]{b}} \cdot \zeta_v^{-\left(\frac{\lambda sv}{r} + \frac{v}{k} \cdot j\right)} = \frac{m}{\sqrt[b]{b}} \cdot \zeta_m^{-\left(\frac{\lambda sm}{r} + \frac{m}{k} \cdot j\right)},$$

falls (9) gilt oder (12) und $\sigma(\sqrt{\zeta_{2r} + \zeta_{2r}^{-1} + 2}) = \sqrt{\zeta_{2r} + \zeta_{2r}^{-1} + 2}$.

$$(36) \quad \sigma(\sqrt[b]{b}) = \frac{m}{\sqrt[b]{b}} \cdot \zeta_m^{-\left(\frac{\lambda sm}{r} + \frac{m}{k} \cdot j + \frac{m}{2}\right)}, \quad \text{falls (12) gilt und}$$

$$\sigma(\sqrt{\zeta_{2r} + \zeta_{2r}^{-1} + 2}) = -\sqrt{\zeta_{2r} + \zeta_{2r}^{-1} + 2},$$

$$(37) \quad \sigma(\sqrt[b]{b}) = \frac{m}{\sqrt[b]{b}} \cdot \zeta_m^{-\left(\frac{\lambda sm}{r} + \frac{m}{k} \cdot j + \frac{j}{2}\right)}, \quad \text{falls (10) gilt oder (11) und}$$

$$\sigma(\sqrt{\zeta_{2r} + \zeta_{2r}^{-1} + 2}) = \sqrt{\zeta_{2r} + \zeta_{2r}^{-1} + 2},$$

$$(38) \quad \sigma(\sqrt[b]{b}) = \frac{m}{\sqrt[b]{b}} \cdot \zeta_m^{-\left(\frac{\lambda sm}{r} + \frac{m}{k} \cdot j + \frac{m}{2} + \frac{j}{2}\right)}, \quad \text{falls (11) gilt und}$$

$$\sigma(\sqrt{\zeta_{2r} + \zeta_{2r}^{-1} + 2}) = -\sqrt{\zeta_{2r} + \zeta_{2r}^{-1} + 2}.$$

Nach Hilfssatz 2 läßt σ eine Nullstelle von $X^n - a$ fest genau dann, wenn

$$(39) \quad (j, n) \left| \frac{\lambda n}{r} \right.$$

gilt und eine Nullstelle von $X^m - b$ genau dann, wenn

$$(40) \quad (j, m) \left| \frac{\lambda sm}{r} + \frac{m}{k} \cdot j, \quad \text{falls (35) gilt,} \right.$$

$$(41) \quad (j, m) \left| \frac{\lambda sm}{r} + \frac{m}{k} \cdot j + \frac{m}{2}, \quad \text{falls (36) gilt,} \right.$$

$$(42) \quad (j, m) \left| \frac{\lambda sm}{r} + \frac{m}{k} \cdot j + \frac{j}{2}, \quad \text{falls (37) gilt,} \right.$$

$$(43) \quad (j, m) \left| \frac{\lambda sm}{r} + \frac{m}{k} \cdot j + \frac{m}{2} + \frac{j}{2}, \quad \text{falls (38) gilt.} \right.$$

Es gelte (39). Dann ist zu zeigen, daß jeweils eine der Teilerbeziehungen (40), (41), (42) oder (43) gilt. Es sei p ein Primteiler von (j, m) . Dann gilt

$$(44) \quad v_p(j, m) \leq v_p\left(\frac{m}{k} \cdot j\right).$$

Dies ist klar, wenn $v_p(k) \leq v_p(m)$ ist. Wegen $k|n$ muß andernfalls $p|n'$ gelten und wegen (7)

$$v_p(k) \leq v_p(w_p).$$

Wegen $p|j$ folgt nach Hilfssatz 7 außerdem

$$(45) \quad v_p(j) \geq v_p(w_p).$$

Insgesamt ergibt sich (44).

Wir weisen nun die Ungleichung

$$(46) \quad v_p(j, m) \leq v_p(\lambda sm/r)$$

nach. Ist $m_p + v_p(s) < v_p(n)$, so muß $p|n'$ gelten und damit nach (8)

$$v_p(r) \leq v_p(s),$$

woraus (46) unmittelbar folgt. Im Fall $m_p + v_p(s) \geq v_p(n)$ ergibt sich aus (39)

$$(47) \quad v_p(j, p^{m_p}) \leq v_p\left(\frac{\lambda \cdot s \cdot p^{m_p}}{r}\right).$$

Ist $m_p = v_p(m)$, so erhält man (46) unmittelbar. Andernfalls ist

$$m_p = v_p(w_p) > v_p(m)$$

woraus zusammen mit (45) und (47) wieder (46) folgt.

Wegen (44) und (46) bleibt nur noch aus der Gültigkeit von (39) zu beweisen, daß der Faktor 2 in (j, m) nicht häufiger aufgeht als in der jeweiligen rechten Seite der Teilerbeziehungen (40)–(43). Hierzu verwenden wir das Resultat aus Satz 1 von Schinzel. Da eine der Gleichungen (9)–(12) nach Voraussetzung gilt, folgt nach Satz 1

$$P_K(a, n) \subseteq P_K(b^{\frac{v}{m}}, v).$$

Der Automorphismus σ läßt also eine Nullstelle von $X^v - b^{\frac{v}{m}}$ fest. Nach Hilfssatz 2 ist dies der Fall genau dann, wenn

$$(j, v) \left| \frac{\lambda sv}{r} + \frac{v}{k} \cdot j, \quad \text{falls (35) gilt,} \right.$$

$$(48) \quad (j, v) \left| \frac{\lambda sv}{r} + \frac{v}{k} \cdot j + \frac{v}{2}, \quad \text{falls (36) gilt,} \right.$$

$$(49) \quad (j, v) \left| \frac{\lambda sv}{r} + \frac{v}{k} \cdot j + \frac{j}{2}, \quad \text{falls (37) gilt,} \right.$$

$$(50) \quad (j, v) \left| \frac{\lambda sv}{r} + \frac{v}{k} \cdot j + \frac{v}{2} + \frac{j}{2}, \quad \text{falls (38) gilt.} \right.$$

Nach Voraussetzung ist $v_2(m) = v_2(v)$. Aus (44) und (46) folgt also

$$v_2(j, v) \leq v_2\left(\frac{v}{2}\right), \quad \text{falls (36) gilt,}$$

$$v_2(j, v) \leq v_2\left(\frac{j}{2}\right), \quad \text{falls (37) gilt,}$$

$$(51) \quad v_2(j, v) \leq v_2\left(\frac{v}{2} + \frac{j}{2}\right), \quad \text{falls (38) gilt}$$

und damit

$$v_2(j, m) \leq v_2\left(\frac{m}{2}\right), \quad \text{falls (36) gilt,}$$

$$v_2(j, m) \leq v_2\left(\frac{j}{2}\right), \quad \text{falls (37) gilt.}$$

Die Ungleichung (51) ist nur möglich, wenn $v_2(v) = v_2(j)$ ist, also

$$v_2(j, m) \leq v_2\left(\frac{m}{2} + \frac{j}{2}\right).$$

Damit ist Satz 3 bewiesen.

Literaturverzeichnis

- [1] N. C. Ankeny and C. A. Rogers, *A conjecture of Chowla*, Ann. of Math. 53 (1951), pp. 541–550.
 [2] H. Flanders, *Generalisation of a theorem of Ankeny and Rogers*, *ibid.* 57 (1953), pp. 392–400.
 [3] I. Gerst, *On the theory of n -th power residues and a conjecture of Kronecker*, Acta Arith. 17 (1970), pp. 121–139.
 [4] A. Schinzel, *On power residues and exponential congruences*, *ibid.* 27 (1975), pp. 397–420.
 [5] — *A refinement of a theorem of Gerst on power residues*, *ibid.* 17 (1970), pp. 161–168.
 [6] — *Abelian binomials, power residues and exponential congruences*, *ibid.* 32 (1977), pp. 245–274.
 [7] V. Schulze, *Potenzreste*, *ibid.* 33 (1977), pp. 379–404.
 [8] E. Trost, *Zur Theorie der Potenzreste*, Nieuw. Arch. Wiskunde 18 (1934), pp. 58–61.

FREIE UNIVERSITÄT BERLIN
 II. MATH. INST. FB 19
 Königin-Luise-Str. 24/26
 D-1000 Berlin 33

Eingegangen am 4. 2. 1980
 und in revidierter Form am 28. 11. 1980

(1235)

Some asymptotic formulas on generalized divisor functions, III

by

P. ERDÖS and A. SÁRKÖZY (Budapest)

1. Throughout this paper, we use the following notation:

$c_1, c_2, \dots, X_0, X_1, \dots$ denote positive absolute constants. We denote the number of elements of the finite set S by $|S|$. We write $e^x = \exp(x)$. We denote the least prime factor of n by $p(n)$, while the greatest prime factor of n is denoted by $P(n)$. We write $p^a \parallel n$ if $p^a | n$ but $p^{a+1} \nmid n$. $\omega(n)$ denotes the number of all the prime factors of n so that $\omega(n) = \sum_{p^a \parallel n} a$ and we write

$$\omega(n, x, y) = \sum_{\substack{p^a \parallel n \\ x < p \leq y}} a.$$

The divisor function is denoted by $d(n)$:

$$d(n) = \sum_{d|n} 1.$$

Let A be a finite or infinite sequence of positive integers $a_1 < a_2 < \dots$. Then we write

$$N_A(x) = \sum_{\substack{a \in A \\ a \leq x}} 1, \quad f_A(x) = \sum_{\substack{a \in A \\ a | x}} \frac{1}{a}, \quad d_A(n) = \sum_{\substack{a \in A \\ a | n}} 1$$

(in other words, $d_A(n)$ denotes the number of divisors amongst the a_i 's) and

$$D_A(x) = \max_{1 \leq n \leq x} d_A(n).$$

The aim of this series is to investigate the function $D_A(x)$. (See [1] and [2]; see also Hall [4].) Clearly,

$$\sum_{1 \leq n \leq x} d_A(n) = x f_A(x) + O(x).$$

Thus if $f_A(x)$ is large then we have $D_A(x)/f_A(x) \gg 1$. In Part II of this