MATH. SCAND. 45 (1979), 168–176

ÜBER LIPSCHITZ-FOLGEN

G. J. RIEGER

Aussagen der Gestalt $F(\alpha)-F(\beta)=O(\alpha-\beta)$ sind für die Analysis wie für die Zahlentheorie gleichermassen wichtig. Wir möchten darauf vom zahlentheoretischen Standpunkt näher eingehen. § 1 bringt die Konstruktion vieler F. Diese werden in § 2 zu Ringen zusammengefasst. In § 3 beweisen wir ein Gegenstück zu einem bekannten Satz von Lagrange über Polynome. § 4 bringt die Verallgemeinerung auf beliebige algebraische Zahlkörper. § 5 enthält einen Satz über Gleichverteilung auf Restklassen; die dortige Voraussetzung $F_i \in W(\mathsf{N},1)$ stellt den Zusammenhang zum Vorhergehenden her. In § 6 werden obere und in § 7 schliesslich untere Siebabschätzungen herangezogen.

Kleine lateinische Buchstaben bedeuten ganzrationale Zahlen.

1.

SATZ 1. *Es sei M eine unendliche Teilmenge von $\mathbf{Z}$; ferner sei $k>0$; dann gibt es überabzählbarviele $F\colon M \to \mathbf{Z}$ mit*

$$(1.1)\qquad F(a) \equiv F(b) \bmod (a-b)^k \qquad (a \in M,\ b \in M)$$

und

$$(1.2)\qquad F(a) > 2^{|a|} \qquad (a \in M)\,.$$

BEWEIS. Wir gehen aus von irgendeiner Abzählung von $M=\{a_1,a_2,a_3,\ldots\}$. $F(a_1),F(a_2),\ldots,F(a_{n-1})$ seien bereits konstruiert $(n>1)$, und es gelte

$$(1.3)\qquad F(a_i) \equiv F(a_j) \bmod (a_i-a_j)^k \qquad (0<i<j<n)\,.$$

Wir suchen ein $F(a_n) \in \mathbf{Z}$ mit

$$(1.4)\qquad F(a_n) \equiv F(a_j) \bmod (a_n-a_j)^k \qquad (0<j<n)\,.$$

Dieses System von Kongruenzen für $F(a_n)$ ist nach dem chinesischen Restsatz genau dann lösbar, wenn gilt

$$(1.5)\qquad F(a_i) \equiv F(a_j) \bmod ((a_n-a_i)^k, (a_n-a_j)^k) \qquad (0<i<j<n)\,.$$

Eingegangen am 18. Dezember, 1978.

Nun gilt

$$(a^k, b^k) = (a,b)^k, \ (a,b) \mid (a-b), \ c \mid d \ \Rightarrow \ c^k \mid d^k;$$

mit $a = a_n - a_i$, $b = a_n - a_j$ folgt

$$((a_n - a_i)^k, (a_n - a_j)^k) \mid (a_i - a_j)^k \qquad (0 < i < j < n)\,.$$

Wegen (1.3) ist also (1.5) erfüllt. $F(a_n)$ kann daher beliebig in einer bestimmten Restklasse $\bmod\,[(a_n - a_1)^k, (a_n - a_2)^k, \ldots, (a_n - a_{n-1})^k]$ gewählt werden. Alles weitere ist klar.

Wegen (1.2) ist ein F aus Satz 1 sicherlich nicht die Einschränkung eines $F(X) \in \mathbf{Z}[X]$ auf M. Statt (1.2) hätte man auch andere Bedingungen wie

$$(1.6) \qquad (-1)^j F(a_j) > 0 \qquad (j > 0)$$

verlangen können, und wieder ist F kein Polynom.

2.

Es sei M eine unendliche Teilmenge von $\mathbf{Z}$; ferner sei $k \geqq 0$; die Menge der $F\colon M \to \mathbf{Z}$ mit (1.1) bezeichnen wir mit $W(M,k)$. Es ist

$$W(M,0) \supsetneqq W(M,1) \supsetneqq W(M,2) \supsetneqq W(M,3) \supsetneqq \ldots;$$

denn: »$\supset$« ist klar; für »$\neq$« wählen wir als a_1, a_2 irgendwelche Elemente von M mit $|a_1 - a_2| > 1$ und setzen $F(a_2) := F(a_1) + (a_1 - a_2)^k$, woraus sich mit Hilfe des Beweises von Satz 1 sofort $F \in W(M,k)$, $F \notin W(M,k+1)$ ergibt. Es ist

$$\bigcap_{k \geqq 1} W(M,k) = \mathbf{Z} \ (= \text{Menge der konstanten Folgen auf } M);$$

denn für $F \in W(M,k) \setminus \mathbf{Z}$ wählen wir zunächst $a \in M$, $b \in M$ mit $F(a) \neq F(b)$ und dann l mit

$$|F(a) - F(b)| < |a-b|^l$$

und erhalten $F \notin W(M,l)$. $F_1, \ldots, F_s$ $(s \geqq 0)$ aus $W(M,k)$ seien algebraisch unabhängig über $\mathbf{Z}$; wie bei Satz 1 konstruieren wir F_{s+1} aus $W(M,k)$ mit

$$\log |F_{s+1}(x)| > |x| + |F_1(x)| + \ldots + |F_s(x)| \qquad (x \in M);$$

dann sind auch $F_1, \ldots, F_s, F_{s+1}$ algebraisch unabhängig über $\mathbf{Z}$. Es seien $M_1 \subsetneqq M_2$ unendliche Teilmengen von $\mathbf{Z}$; ferner sei $k > 0$; dann ist $W(M_1,k) \supsetneqq W(M_2,k)$; dann: »$\supset$« ist klar; für »$\neq$« lässt es sich leicht einrichten, dass (1.1) für ein Paar $a \in M_1$, $b \in M_2 \setminus M_1$ verletzt wird. Es seien M, M' unendliche Teilmengen von $\mathbf{Z}$; ferner sei $k > 0$, $l > 0$, $F \in W(M,k)$, $F(M) \subseteqq M'$, $G \in W(M',l)$; dann ist $G \circ F \in W(M; kl)$.

SATZ 2. *Es sei M eine unendliche Teilmenge von $\mathbf{Z}$; ferner sei $k>0$; vermöge $(F \dotplus G)(a) := F(a) \dotplus G(a)$ wird $W(M,k)$ zu einem nullteilerfreien kommutativen Ring mit Einselement.*

BEWEIS. Wegen

$$F(x+y)G(x+y)-F(x)G(x)$$
$$= F(x+y)(G(x+y)-G(x))+(F(x+y)-F(x))G(x)$$

führt Multiplikation aus $W(M,k)$ nicht heraus. Für jedes $F \neq 0$ aus $W(M,k)$ gibt es höchstens endlichviele $n \in M$ mit $F(n)=0$; denn sonst wähle man ein $a \in M$ mit $F(a) \neq 0$, und für die unendlichvielen $n \in M$ mit $F(n)=0$ wäre $(n-a)^k \mid F(a)$ nach (1.1), was ungereimt ist; folglich hat auch das Produkt zweier $F_1 \neq 0$, $F_2 \neq 0$ aus $W(M,k)$ höchstens endlichviele Nullstellen, und es gibt keine Nullteiler. Alles weitere ist klar.

Es sei $k>1$; unter eine k-Lipschitz-Folge verstehen wir ein Element von $W(\mathbf{N},k)$. Eine 1-Lipschitz-Folge nennt man auch ein Quasi-Polynom (vgl. [3]). Für jedes $F(x) \in \mathbf{Z}[X]$ ist $(F(n)\colon n>0)$ eine 1-Lipschitz-Folge wegen $(a-b) \mid (a^r-b^r)$ für $r>0$; zusammen mit Satz 1 kann man schreiben

$$\mathbf{Z}[X] \subsetneqq W(\mathbf{N},1)\,. \tag{2.1}$$

Wir betrachten noch zwei Beispiele aus $\mathbf{Q}[X]$; es ist $F(X)=\frac{1}{2}X(X+1) \notin W(\mathbf{N},1)$ wegen $2 \nmid (F(3)-F(1))$; est ist $F(X)=\frac{1}{2}X^2(X^2+1) \in W(\mathbf{N},1)$ da in

$$a^2(a^2+1)-b^2(b^2+1) = (a-b)(a^2+a^2b+ab^2+b^3+a+b)$$

die letzte Klamme stets durch 2 teilbar ist. Mittels Newton-Interpolation lassen sich leicht alle $F(X) \in \mathbf{Q}[X] \cap W(\mathbf{N},1)$ charakterisieren (vgl. [3, Corollary 1]).

SATZ 3. *Es sei $F(X) \in \mathbf{Z}[X]$; ferner sei $(F(n)\colon n>0) \in W(\mathbf{N},2)$; dann ist F eine Konstante.*

BEWEIS. Es sei $F(X)=b_0+b_1X+b_2X^2+\ldots+b_gX^g$. Für beliebige $n>0$, l müsste dann sein $F(n+l) \equiv F(l) \bmod n^2$. Binomische Entwicklung führt nach Weglassen der Potenzen $n^2,\ldots,n^g$ und nach Kürzen mit n auf

$$b_1+2b_2l+\ldots+gb_gl^{g-1} \equiv 0 \bmod n\,.$$

Für $n>|b_1|+2|b_2||g+\ldots+g|b_g|g^{g-1}$ folgt

$$b_1+2b_2l+\ldots+gb_gl^{g-1} = 0 \qquad (l=1,2,\ldots,g)\,.$$

Dieses lineare Gleichungssystem für $b_1, 2b_2, \ldots, gb_g$ führt nach Vandermonde auf $b_1 = 2b_2 = \ldots = gb_g = 0$.
Für $k > 0$ bezeichne $V(k)$ den Körper der Quotienten von $W(\mathbf{Z}, k)$. Wegen (2.1) (mit $\mathbf{Z}$ statt $\mathbf{N}$) und wegen (1.5) gilt

$$\mathbf{Z}[X] \subsetneqq V(1)\,.$$

Für $\alpha \in \mathbf{R}$ bezeichne $[\alpha]$ die durch $\alpha - 1 < [\alpha] \leqq \alpha$ eindeutig bestimmte ganzrationale Zahl.

SATZ 4. *Es sei* $G(n) > 0$ $(n > 0)$,

$$(G(n) : n > 0) \in W(\mathbf{N}, 1)\,, \tag{2.2}$$

$$n \mid G(n) \qquad (n > 0) \tag{2.3}$$

$$H(n) := \left(\sum_{r=0}^{\infty} \prod_{l=1}^{r} G(l)^{-1} \right) \prod_{j=1}^{n} G(j) \qquad (n > 0);$$

dann ist $([H(n)] : n > 0) \in W(\mathbf{N}, 1)$

BEWEIS. Für $n > 0$ ist

$$0 < \sum_{r > n} \prod_{l=1}^{r} G(l)^{-1} \leqq \sum_{r > 1} \frac{1}{r!} \text{ (termweise)} < 1\,. \tag{2.4}$$

Indem man in H die Terme der Reihe mit dem rechts stehenden Produkt multipliziert und die Reihe bei $r = n$ aufspaltet, kommt

$$H(n) = \sum_{r=0}^{n} \prod_{j=r+1}^{n} G(j) + \sum_{r > n} \prod_{j=n+1}^{r} G(j)^{-1}\,.$$

Wegen (2.4) folgt

$$[H(n)] = \sum_{r=0}^{n} \prod_{j=r+1}^{n} G(j)\,. \tag{2.5}$$

Es sei $0 < a < b$. Durch Aufspalten der Summe (2.5) für $n = b$ bei $r = b - a - 1$ kommt

$$[H(b)] - [H(a)] = \sum_{r=0}^{b-a-1} \prod_{j=r+1}^{b} G(j) + \tag{2.6}$$

$$+ \sum_{s=b-a}^{b} \prod_{t=s+1}^{b} G(t) - \sum_{r=0}^{a} \prod_{j=r+1}^{a} G(j)\,.$$

Jeder Summand der ersten Summe von (2.6) enthält den Faktor $G(b-a)$ und wegen (2.3) somit den Faktor $(b-a)$. In der mittleren Summe von (2.6) ersetzen wir s durch $r = s - b + a$ und t durch $j = t - b + a$; wir erhalten

$$\sum_{s=b-a}^{b} \prod_{t=s+1}^{b} G(t) - \sum_{r=0}^{a} \prod_{j=r+1}^{a} G(j)$$
$$= \sum_{r=0}^{a} \left(\prod_{j=r+1}^{a} G(j+b-a) - \prod_{j=r+1}^{a} G(j) \right)$$

und beachten

$$G(j+b-a) \equiv G(j) \bmod (b-a) \qquad (r<j\leqq a)$$

wegen (2.2). Insgesamt folgt $[H(b)]\equiv[H(a)] \bmod (b-a)$.

In Satz 4 kann man etwa jedes $G(X)=b_1X+\ldots+b_gX^g$ nehmen mit $g>0$, $b_j\geqq 0$ $(0<j<g)$, $b_g>0$. Mit

$$G(X) = X \quad \text{und} \quad E := \sum_{r\geqq 0} \frac{1}{r!}$$

kommt $([n!\,E]:n>0) \in W(\mathsf{N},1)$ (vgl. [3, Corollary] für $g=1$).

3.

Nach Lagrange hat die Kongruenz

$$X^g+b_1X^{g-1}+\ldots+b_g \equiv 0 \bmod p$$

für jede Primzahl p höchstens g Lösungen. Dagegen gilt

Satz 5. *Es sei eine beliebige unendliche Menge vom Primzahlen* $p_1<p_2<p_3<\ldots$ *gegeben mit* $p_1\geqq 3$ *und mit* $p_j>p_{j-1}+j$ $(j>1)$; *ferner sei* $k>0$; *dann gibt es dazu überabzählbarviele* $F\in W(\mathsf{N},k)$ *mit* (1.2) (*oder mit* (1.6)) *derart, dass für passendes* c_j *die Kongruenz* $F(X)\equiv c_j \bmod p_j$ *mindestens* j *Lösungen hat* $(j>0)$.

Beweis. Es sei noch $p_0:=1$. Wir verfeinern die Konstruktion aus Satz 1 mit $a_n=n$. Für jedes $n\in\mathsf{N}$ gibt es genau ein $t\in\mathsf{N}$ mit $p_{t-1}\leqq n<p_t$. Im Fall $n<p_t-t$ fordern wir nur (1.4); $F(n)$ kann dann noch beliebig in einer bestimmten Restklasse $\bmod [1^k,2^k,\ldots,(n-1)^k]$ gewählt werden. Im Fall $p_t-t\leqq n$ $(<p_t)$ fordern wir (1.4) und zusätzlich

$$F(n) \equiv F(p_t-t-1) \bmod p_t^k;$$

$F(n)$ kann dann noch beliebig in einer bestimmten Restklasse $\bmod [1^k,2^k,\ldots,(n-1)^k,p_t^k]$ gewählt werden. Für gegebenes $j>0$ folgt mit

$$X = p_j-j-1+h \quad (0\leqq h<j), \qquad c_j = F(p_j-j-1)$$

die Behauptung.

Bemerkung. Ob die Ringe $W(M,k)$ aus Satz 2, ihre Körper der Quotienten und die Quotientenringe $W(M,k)/W(M,l)$ $(0 \leqq k < l)$ algebraisch interessant sind, vermag ich nicht zu sagen.

4.

Es sei K ein algebraischer Zahlkörper; es bezeichne $\mathfrak{o}$ den Ring der ganzen Zahlen von K. Für $\alpha \in \mathfrak{o}$ bezeichne $N\alpha$ die Norm von α und $\langle\alpha\rangle$ das von α erzeugte Hauptideal in $\mathfrak{o}$. Die obigen Überlegungen übertragen sich weitgehend von $\mathbf{Z}$ auf $\mathfrak{o}$. So liefert der Beweis von Satz 1 sofort

Satz 6. *Für jedes $k>0$ gibt es überabzählbarviele $F\colon \mathfrak{o} \to \mathfrak{o}$ mit*

$$F(\alpha) \equiv F(\beta) \bmod \langle\alpha-\beta\rangle^k \qquad (\alpha \in \mathfrak{o},\ \beta \in \mathfrak{o})$$

und

$$NF(\alpha) > 2^{|N\alpha|}\,.$$

5.

Der Beweisgedanke von [4, Satz 1 und Satz 2] liefert leicht

Satz 7. *Es sei $1 \in S \subseteqq \mathbf{N}$, $n \in S$ $(m \in S,\ n\,|\,m,\ n>0)$, $H\colon S \to \mathbf{N}$, $m \nmid H(m)$ $(1<m \in S)$. $H(n)\,|\,H(m)$ $(m \in S,\ n\,|\,m,\ n>0)$, $A\colon \mathbf{N} \to \mathbf{Z}$, $B\colon \mathbf{N} \to \mathbf{Z}$, $(m, A(x)) = 1$ $(m \in S,\ 0<x \leqq H(m))$; ferner sei $A(x) \equiv A(y) \bmod m$, $B(x) \equiv B(y) \bmod m$ $(x>0,\ y>0,\ m \in S,\ x \equiv y \bmod H(m))$; durchläuft dann x genau $[m, H(m)]$ aufeinanderfolgende natürliche Zahlen $(m \in S)$, so nimmt $xA(x)+B(x)$ jeden Wert $\bmod m$ gleichoft (also genau $[m,H(m)]/m$-mal) an.*

Die Funktion $x \mapsto xA(x)+B(x) \bmod m$ $(x>0)$ hat die Periode $[m,H(m)]$.

Es bezeichne φ die Funktion von Euler. Es sei $a \neq 0$, $s \geqq 0$, $t \geqq 0$, $s+t \geqq 1$, $b_j \neq 0$ $(1 \leqq j \leqq s+t)$, $q_k \geqq 0$ $(1 \leqq k \leqq t)$ und $F_j \in W(\mathbf{N},1)$ mit $F_j(\mathbf{N}) \subseteqq \mathbf{N}$ $(1 \leqq j \leqq s+t)$; ferner sei L eine Funktion von $\mathbf{Z}^{s+t}$ in $\mathbf{Z}$, welche bezüglich jeder Variablen die Bedingung (1.1) mit $k=1$ erfüllt; (für jedes j mit $1 \leqq j \leqq s+t$ und jede Wahl von $x_1, \ldots, x_{s+t}$ und y_j sei also

$$L(x_1,\ldots,x_{j-1},x_j,x_{j+1},\ldots,x_{s+t}) \equiv L(x_1,\ldots,x_{j-1},y_j,x_{j+1},\ldots,x_{s+t}) \bmod (x_j-y_j);$$

insbesondere kann man jedes $L \in \mathbf{Z}[X_1,\ldots,X_{s+t}]$ nehmen;) in Satz 7 kann man dann wählen $A(x)=a$,

$$S = \{m>0 : (m, a\, b_1 \ldots b_{s+t}) = 1 \wedge (\varphi(m), q_1 \ldots q_t) = 1\}\,,$$

$$H(m) = \begin{cases} \varphi(m) & \text{im Fall } t=0 \\ \varphi(\varphi(m)) & \text{im Fall } s=0 \\ [\varphi(m), \varphi(\varphi(m))] & \text{sonst}\,, \end{cases}$$

$$B(x) \;=\; L\big(b_1^{F_1(x)},\dots,b_s^{F_s(x)},b_{s+1}^{(q_1^{F_{s+1}(x)})},\dots\, b_{s+t}^{(q_t^{F_{s+t}(x)})}\big)\,. \tag{5.1}$$

Für $n>0$, $(c,n)=1$ bezeichne $G(c;\,n)$ die kleinste natürliche Zahl mit $c^{G(c;\,n)}\equiv 1$ $\bmod n$; es ist $G(c;\,n)\,|\,\varphi(n)$. Im Fall $t=0$ hätte man oben statt $H(m)=\varphi(m)$ auch $H(m)=[G(b_1;\,m),\dots,G(b_s;\,m)]$ wählen können.

Beispiel 1 zu Satz 7. Es sei $a=1$, $B(x)=2^x$, $m=21$; für $x=1, 2, 3, 4, 5, 6$ ist $2^x \equiv 2, 4, 8, 16, 11, 1 \bmod 21$; ferner ist $G(2;\,21)=6$; in Satz 7 können wir daher $H(21)=6$ wählen; für $0<x\leqq 42=[21,6]$ entsteht $x+2^x\equiv 3, 6, 11, 20, 16, 7, 9, 12, 17, 5, 1, 13, 15, 18, 2, 11, 7, 19, 0, 3, 8, 17, 13, 4, 6, 9, 14, 2, 19, 10, 12, 15, 20, 8, 4, 16, 18, 0, 5, 14, 10, 1 \bmod 21$; also kommt jeder Wert mod 21 genau 2-mal vor, wie es sein soll. Jetzt sei $B(x)=2^{x^2}$; für $x=1, 2, 3, 4, 5, 6$ *ist* $2^{x^2}\equiv 2, 16, 8, 16, 2, 1 \bmod 21$; für $0<x\leqq 42$ entsteht $x+2^{x^2}\equiv 3, 18, 11, 20, 7, 7, 9, 3, 17, 5, 13, 13, 15, 9, 2, 11, 19, 19, 0, 15, 8, 17, 4, 4, 6, 0, 14, 2, 10, 10, 12, 6, 20, 8, 16, 16, 18, 12, 5, 14, 1, 1 \bmod 21$; wieder kommt jeder Wert mod 21 genau 2-mal vor. Wegen $x^3 \equiv x \bmod 6$ und $x^4\equiv x^2 \bmod 6$ bringt $x+2^{x^3}$ gegenüber $x+2^x$ und $x+2^{x^4}$ gegenüber $x+2^{x^2}$ nichts Neues.

Beispiel 2 zu Satz 7. Es sei $m=57$; durch Probieren findet man $G(2;\,57)=18$; wir wählen also $H(m)=18$; nach Satz 7 hat die Kongruenz $x+2^x\equiv 0 \bmod 57$ für $0<x\leqq[57,18]=342$ genau 6 Lösungen; durch Probieren findet man $x=32, 43, 55, 110, 301, 314$. Diese 6 Zahlen bilden allerdings kein vollständiges Restsystem mod 6; das hängt damit zusammen, dass es eine Primzahl gibt, welche in m und in $H(m)$ aufgeht, aber in $H(m)$ mit höherer Potenz; wir verfolgen diesen Gedanken nicht weiter. Die Kongruenz $x+2^x\equiv 2 \bmod 57$ hat für $0<x\leqq 342$ die Lösungen 16, 117, 118, 123, 165, 328; diese sind $\equiv 4, 3, 4, 3, 3, 4 \bmod 6$; folglich gibt es keine Primzahl p mit $p+2^p\equiv 2 \bmod 57$.

Aufgrund von Satz 7 sollte man, zahlentheoretisch gesehen, ax als Hauptterm und $B(x)$ als Störterm der Funkton $x \mapsto ax+B(x)$ auffassen; für die Analysis dagegen sind diese Rollen vertauscht. Wir merken noch an, dass Ausdrücke wie $x+4^x$ in den wichtigen Arbeiten von Matijasevič (vgl. etwa [1] und die dort angegebene Literatur) zu Hilberts zehntem Problem vorkommen, wo diophantische Gleichungen der Gestalt

$$A(y_1,\dots,y_n) \;=\; x+4^x$$

untersucht werden.

6.

Es bezeichne $\boldsymbol{P}$ die Menge aller Primzahlen. Die Anwendungen von Satz 7 im Zusammenhang mit oberen Siebabschätzungen entsprechen nahezu wörtlich denen von [4]. So erhält man beispielsweise in direkter Verallgemeinerung von [4, Corollar 1] den folgenden

SATZ 8. *Es sei* $a>0$; *in der Funktion* B *aus* (5.1) *sei* (*der Bequemlichkeit halber*) $t=0$. *Die Anzahl der* x *mit* $0<x<T$ *und* $ax+B(x)\in \boldsymbol{P}$ *ist dann* $O_{a,B}(T(\log T)^{-1})$ $(2<T\in \mathsf{R})$. *Mit der zusätzlichen Bedingung* $ax+B(x)+2\in \boldsymbol{P}$ *kommt* $O_{a,B}(T(\log T)^{-2})$. *Mit der weiteren Bedingung* $x\in \boldsymbol{P}$ *kommen die Exponenten* -2 *und* -3 *statt* -1 *und* -2 *bei* $\log T$.

Alle diese Abschätzungen stehen im Einklang mit der häufigen Erfahrung, wonach jeder Bedingung »$\in \boldsymbol{P}$« ein Faktor $(\log T)^{-1}$ entspricht.

Aus Satz 8 folgt in Analogie zum Zwillingssatz von Brun sofort $\sum 1/x<\infty$, wobei die Summation über alle $x>0$ mit $ax+B(x)\in \boldsymbol{P}$ und $ax+B(x)+2\in \boldsymbol{P}$ zu erstrecken ist.

Die Bedingungen $ax+B(x)\in \boldsymbol{P}$, $ax+B(x)+2\in \boldsymbol{P}$, $ax+B(x)+6\in \boldsymbol{P}$ führen in Satz 8 auf $O_{a,B}(T(\log T)^{-3})$. Mit »$+4$« statt »$+6$« ist diese Aussage trivial, da von den Zahlen $y, y+2$, $y+4$ genau eine durch 3 teilbar und daher keine Primzahl ist $(y>3)$.

7.

Satz 7 gestattet es auch, untere Siebabschätzungen heranzuziehen. Wir verzichten auf die Formulierung der allgemeinen Sätze und beschränken uns der Bequemlichkeit halber auf die wohl interessantesten Spezialfälle $x\mapsto x+2^x$ und $x\mapsto x2^x+1$. Wegen Satz 7 ist [2, Satz 7.4] mit $\omega(d)=1$, $\varkappa=1$, $\alpha=\frac{1}{2}$, $|R_d|\leqq d$ (in den dortigen Bezeichnungen) direkt anwendbar, und wie in [2, S. 220] folgt

SATZ 9. *Es gibt ein reelles* $C_1>0$ *derart, dass es mehr als* $C_1T(\log T)^{-1}$ *natürliche Zahlen* $x<T$ *gibt, für die* $x+2^x$ *nur Primfaktoren* $>T^{1/4,2}$ *hat* $(2<T\in \mathsf{R})$; *das gilt auch mit* $x2^x+1$ *statt* $x+2^x$.

Verwendet man [2, Satz 7.4] mit $\omega(p)=2$ $(2<p\in \boldsymbol{P})$, $\varkappa=2$, $\alpha=\frac{1}{2}$ (in den dortigen Bezeichnungen), so folgt unter Zuhilfenahme von [4, § 5] wie in [2, S. 220] sofort

SATZ 10. *Es gibt ein reelles* $C_2>0$ *derart, dass es mehr als* $C_2T(\log T)^{-2}$ *natürliche Zahlen* $x<T$ *gibt, für die sowohl* $x+2^x$ *als auch* $x+2^x+2$ *nur Primfaktoren* $>T^{1/8,9}$ *hat* $(2<T\in \mathsf{R})$; *das gilt auch mit* $x2^x+1$ *und* $x2^x+3$ *statt* $x+2^x$ *und* $x+2^x+2$.

Ganz ähnlich findet man

SATZ 11. *Es gibt ein reelles* $C_3 > 0$ *derart, dass es mehr als* $C_3 T(\log T)^{-2}$ *natürliche Zahlen* $x < T$ *gibt, für die sowohl* x *als auch* $x + 2^x$ *nur Primfaktoren* $> T^{1/8,9}$ *hat* ($2 < T \in \mathsf{R}$); *das gilt auch mit* $x2^x + 1$ *statt* $x + 2^x$.

Ein x aus Satz 11 hat dann höchstens 8 Primfaktoren, wobei mehrfache Primfaktoren auch mehrfach gezählt werden.

LITERATUR

1. Martin Davis, Yuri Matijasevič, and Julia Robinson, *Hilbert's tenth problem: positive aspects of a negative solution. Mathematical developments arising from Hilbert problems*, Proc. Symp. Pure Math. 28, part 2, S. 323–378, Amer. Math. Soc., Providence, R.I., 1976.
2. H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London - New York - San Francisco, 1974.
3. R. R. Hall, *On pseudo-polynomials*, Mathematika 18 (1971), 71–77.
4. G. J. Rieger, *Sur les nombres de Cullen*, Sém. Théorie des Nombres. Année 1976–1977—exposé no. 16; Université de Bordeaux I.

INSTITUT FÜR MATHEMATIK
TECHNISCHE UNIVERSITÄT HANNOVER
WELFENGARTEN 1
3 HANNOVER
BUNDESREPUBLIK DEUTSCHLAND