Theorem von Granville

Johannes Nüßle

4. August 2010

Inhaltsverzeichnis

1 Einleitung

Im Folgenden soll eine Aussage über die Dichte quadratfreier Werte eines Polynoms betrachtet werden. Dabei heißt ein Wert quadratfrei, wenn jeder Primteiler nur von erster Ordnung ist. Man betrachtet nun ein Polynom mit ganzzahligen Koeffizienten $f \in \mathbb{Z}[x]$ und wertet dieses an den natürlichen Zahlen aus. Es ist einsichtig, dass keiner dieser Werte quadratfrei ist, wenn f einen doppelten Linearfaktor oder einen konstanten quadratischen Teiler besitzt. Es zeigt sich, dass aus der abc-Vermutung folgt, dass die Dichte der quadratfreien Werte unter den Funktionswerten von f in natürlichen Zahlen positiv ist, wenn man die erwähnten Sonderfälle ausschließt.

2 Theorem von Granville

Es soll folgendes Theorem bewiesen werden:

Theorem 1 (Theorem von Granville)
Sei $f \in \mathbb{Z}[x]$ quadratfrei vom Grad d so, dass die Werte von f keinen fixierten

quadratischen Teiler besitzen, d.h. es gibt kein $k \in \mathbb{Z}$ *mit* $\forall n \in \mathbb{Z} : k|f(n)$. *Falls die abc-Vermutung gültig ist, gilt dann:*

$$|\{0 \leq n \leq y | f(n) quadratfrei\}| \sim c(f) \cdot y$$

für ein $c(f) > 0$ *konstant.*

3 Bereits bekannte Sätze

In diesem Abschnitt sollen noch einmal einige bereits bekannte Sätze und Definitionen aufgeführt werden, die für den Beweis benötigt werden. Die Beweise dazu finden sich in den angegebenen Quellen und werden hier nicht dargestellt.

Definition 1
Sei $f \in \mathbb{Z}$ *ein Polynom und* p *prim. Dann wird* $\omega(p)$ *definiert als*

$$\omega(p) := |\{0 \leq n < p^2 | f(n) \equiv 0 \mod p^2\}|$$

Satz 1
Sei $f \in \mathbb{Z}[x]$ *quadratfrei. Dann gilt für* p *prim mit* $p \not| \Delta(f)$, *wobei* $\Delta(f)$ *die Diskriminante von* f *sei, die Ungleichung:*

$$\omega(p) \leq grad(f)$$

Beweis. siehe [1] □

Satz 2
Sei $\epsilon > 0$ *beliebig und* $f \in \mathbb{Z}[x]$ *quadratfrei vom Grad* d. *Dann folgt aus der abc-Vermutung, dass für alle* $n \in \mathbb{Z}$ *mit* $f(n) \neq 0$ *gilt:*

$$rad(f(n)) \gg |n|^{d-1-\epsilon}$$

Beweis. siehe [2] □

4 Vorbereitungen

Als Vorbereitung sollen noch einige Lemmata bewiesen werden, die im Beweis Verwendung finden. Um die Darstellung zu vereinfachen, soll in allen folgenden Abschnitten p generell eine Primzahl sein.

Lemma 1
Sei $f \in \mathbb{Z}[x]$. Dann gilt für alle $t, k \in \mathbb{Z}$:

$$f(t + kp^2) \equiv f(t) \mod p^2$$

Beweis. Es genügt, die Aussage für die Monome zu zeigen. Dabei gilt aber:

$$\begin{aligned}(t + kp^2)^n &= \sum_{j=0}^{n} \binom{n}{j} t^{n-j} k^j p^{2j} \\ &\equiv t^n \mod p^2\end{aligned}$$

(da jeder Summand mit $j \neq 0$ ein Vierlfaches von p^2 ist) □

Lemma 2
Definiere:

$$M_y := \prod_{p \leq \sqrt{\log y}} p^2$$

Dann gilt für alle $y \in \mathbb{N}$ und $t \in \mathbb{Z}$:

$$|\{t \leq n < M_y + t | \forall p \leq \sqrt{\log y} : f(n) \not\equiv 0 \mod p^2\}| = \prod_{p \leq \sqrt{\log y}} (p^2 - \omega(p))$$

Beweis. Es gilt für alle $p \leq \sqrt{\log y}$:

$$f(n) \equiv 0 \mod p^2 \iff f(n + M_y) \equiv 0 \mod p^2$$

Also ist die Mächtigkeit der gegebenen Menge für alle t gleich und es genügt, die Aussage des Lemmas für $t = 0$ zu zeigen.
Für festes p gibt es genau $p^2 - \omega(p)$ Werte $0 \leq n < p^2$ mit $f(n) \not\equiv 0 \mod p^2$. Seien diese Werte $c_1^{(p)}; \ldots; c_{p^2-\omega(p)}^{(p)}$. Dann gilt für $0 \leq n < M_y$:

$$f(n) \not\equiv 0 \mod p^2 \iff \exists j : n \equiv c_j^{(p)} \mod p^2$$

Wählt man nun für jedes $p \leq \sqrt{\log y}$ einen Index j_p mit $1 \leq j_p \leq p^2 - \omega(p)$ aus, so ergibt die Forderung $\forall p \leq \sqrt{\log y} : f(n) \not\equiv 0 \mod p^2$ ein System:

$$\forall p \leq \sqrt{\log y} : \qquad n \equiv c_{j_p}^{(p)} \mod p^2$$

Für jede mögliche Wahl der Indizies j_p entsteht ein solches System, dessen Lösungen der Forderung $\forall p \leq \sqrt{\log y} : f(n) \not\equiv 0 \mod p^2$ genügen. Umgekehrt ist jede mögliche Lösung dieser Forderung durch genau ein solches System gegeben. Nach dem chinesischen Restesatz gibt es für ein solches System eine eindeutige Lösung n mit $0 \leq n < M_y$. Da es insgesamt genau

$$\prod_{p \leq \sqrt{\log y}} p^2 - \omega(p)$$

Möglichkeiten gibt, ein solches System aufzustellen, gibt es ebensoviele Möglichkeiten, ein n mit $0 \leq n < M_y$ zu finden, das

$$\forall p \leq \sqrt{\log y} : f(n) \not\equiv 0 \mod p^2$$

erfüllt.

$\square$

Lemma 3
Sei $f \in \mathbb{Z}[x]$ ohne fixierten quadratischen Teiler und vom Grad d. Definiere dann

$$c_p(f) := 1 - \frac{\omega(p)}{p^2}$$

und

$$c(f) := \prod_p c_p(f)$$

Dann gilt c(f) > 0.

Beweis. Zuerst gilt $c_p(f) \neq 0$, denn wäre $c_p(f) = 0$, so wäre nach Definition $\omega(p) = p^2$. Nach Definition von $\omega(p)$ wäre dann

$$\forall 0 \leq t < p^2 : f(t) \equiv 0 \mod p^2$$

und damit wegen Lemma 1 auch

$$\forall t \in \mathbb{Z} : f(t) \equiv 0 \mod p^2$$

Damit hätte aber f einen fixierten quadratischen Teiler.
Wähle $s \in \mathbb{N}$ so, dass $s > \max\{\Delta f; d\}$ gilt. Sei $p \geq s$ prim. Dann gilt in jedem Fall $p > \Delta f$, also $p \not| \Delta f$. Also gilt nach Satz 1 $\omega(p) \leq d$. Es gilt, dass:

$$\sum_{m > s} \frac{d}{m^2} < \infty$$

absolut konvergent ist (durch Vergleich mit der Zeta-Funktion $\zeta(2)$). Damit ist aber

$$\prod_{m > s} (1 - \frac{d}{m^2}) > 0$$

konvergent, somit gilt auch:

$$\prod_{p>s}(1-\frac{d}{p^2}) > \prod_{m>s}(1-\frac{d}{m^2})$$
$$> 0$$

Damit kann man abschätzen:

$$\begin{aligned} c(f) &= \prod_p c_p(f) \\ &= \left(\prod_{p\leq s} c_p(f)\right)\left(\prod_{p>s} c_p(f)\right) \\ &> \left(\prod_{p\leq s} c_p(f)\right)\left(\prod_{p>s}(1-\frac{d}{p^2})\right) \\ &> 0 \end{aligned}$$

da der erste Faktor als endliches Produkt echt positiver Faktoren und der zweite, wie oben gezeigt, echt positiv ist. □

Lemma 4
Es gilt:

1.
$$M_y = o(y)$$

2. *Sei $f \in \mathbb{Z}[x]$ quadratfrei und ohne fixierten quadratischen Teiler mit $deg(f) = d$. Dann gilt:*
$$\sum_{p\leq y}\omega(p) = \mathcal{O}(\frac{y}{\sqrt{\log y}})$$

3.
$$\sum_{p>y}\frac{1}{p^2} = \mathcal{O}(\frac{1}{y})$$

Beweis. 1. Sei $\pi(x)$ die Anzahl der Primzahlen, die kleiner oder gleich x sind. Dann erhält man mit dem Primzahlsatz:

$$\pi(x) \sim \frac{x}{\log x}$$

Damit erhält man dann:

$$\begin{aligned}\sum_{p\leq\sqrt{\log y}} \log p &\leq \pi(\sqrt{\log y})\log(\sqrt{\log y})\\ &\sim \frac{\sqrt{\log y}}{\log(\sqrt{\log y})}\log(\sqrt{\log y})\\ &= \sqrt{\log y}\end{aligned}$$

Damit folgt:

$$\begin{aligned}M_y &= \prod_{p\leq\sqrt{\log y}} p^2\\ &= \exp(\sum_{p\leq\sqrt{\log y}} \log p^2)\\ &= \exp(2\sum_{p\leq\sqrt{\log y}} \log p)\\ &= \exp(\mathcal{O}(\sqrt{\log y})) \qquad \text{(wie oben gezeigt)}\end{aligned}$$

und somit:

$$\begin{aligned}\frac{M_y}{y} &= \frac{\exp(\mathcal{O}(\sqrt{\log y}))}{y}\\ &= \exp(\mathcal{O}(\sqrt{\log y}) - \log y)\\ &\longrightarrow 0\end{aligned}$$

für $y \to \infty$, da $\log y$ schneller wächst als jeder $\mathcal{O}(\sqrt{\log y})$-Term. Also ist:

$$M_y = o(y)$$

2. Es gilt:

$$\begin{aligned}\sum_{p\leq y}\omega(p) &\ll \sum_{p\leq y} d \qquad \text{(Nach Satz 1)}\\ &= d\pi(y)\\ &\ll d\cdot\frac{y}{\log y} \qquad \text{(Primzahlsatz)}\\ &\leq d\cdot\frac{y}{\sqrt{\log y}}\end{aligned}$$

und folglich

$$\sum_{p\leq y}\omega(p) = \mathcal{O}(\frac{y}{\sqrt{\log y}})$$

3. Weiter ist:

$$\begin{aligned}\sum_{p>y} \frac{1}{p^2} &< \sum_{m>y} \frac{1}{m^2} \\ &\leq \int_{y-1}^{\infty} \frac{1}{x^2} dx \\ &= -\frac{1}{x}\Big|_{x=y-1}^{\infty} \\ &= \frac{1}{y-1}\end{aligned}$$

Also:

$$\sum_{p>y} \frac{1}{p^2} = \mathcal{O}(\frac{1}{y})$$

$\square$

Damit kann nun der Beweis für das Theorem von Granville geführt werden.

5 Beweis des Theorems von Granville

Beweis. Wird die Konstante $c(f)$ genauso definiert wie in Lemma 3, dann ist dort bereits gezeigt worden, dass $c(f) > 0$ gilt. Es bleibt also Folgendes zu zeigen:

$$|\{0 \leq n \leq y | f(n) \text{ teilerfrei}\} \sim c(f)y$$

Der Ansatz des Beweises ist es nun, Funktionswerte von f zu betrachten, die zumindest keinen quadratischen Primteiler haben, der kleiner als eine bestimmte Grenze ist, und dann diese Grenze in mehreren Schritten bis unendlich auszudehnen. Zu diesem Zweck wird zunächst folgende Menge betrachtet:

$$\{0 \leq n \leq y | \forall p \leq \sqrt{\log y} : f(n) \not\equiv 0 \mod p^2\}$$

Um die Mächtigkeit der Menge abzuschätzen, wende man Lemma 2 an. Dieses Lemma gibt Auskunft darüber, wie viele von M_y aufeinanderfolgenden natürlichen Zahlen n die Bedingung

$$\forall p \leq \sqrt{\log y} : f(n) \not\equiv 0 \mod p^2$$

erfüllen. Also unterteilt man die Zahlen von 0 bis y in Abschnitte der Länge M_y. Dabei erhält man genau $\lfloor \frac{y}{M_y} \rfloor$ ganze Abschnitte, die nach Lemma 2 jeweils $\prod\limits_{p \leq \sqrt{\log y}} (p^2 - \omega(p))$ Lösungen für die Bedingung

$$\forall p \leq \sqrt{\log y} : f(n) \not\equiv 0 \mod p^2$$

enthalten. Der verbleibende Rest an Zahlen, der keinen ganzen Abschnitt der Länge M_y mehr bilden konnte, ist auf jeden Fall ein $\mathcal{O}(M_y)$-Term. Also kann man folgendermaßen rechnen:

$$\begin{aligned}
&|\{0 \le n \le y | \forall p \le \sqrt{\log y} : f(n) \not\equiv 0 \mod p^2\}| \\
=&\lfloor \frac{y}{M_y} \rfloor \prod_{p \le \sqrt{\log y}} (p^2 - \omega(p)) + \mathcal{O}(M_y) \\
=&\lfloor \frac{y}{M_y} \rfloor M_y \prod_{p \le \sqrt{\log y}} (1 - \frac{\omega(p)}{p^2}) + \mathcal{O}(M_y) && \text{(nach Definition von } M_y\text{)} \\
=&(y - tM_y) \prod_{p \le \sqrt{\log y}} (1 - \frac{\omega(p)}{p^2}) + \mathcal{O}(M_y) && \text{(mit } t \in [0;1]\text{)} \\
& && \text{(es gilt } tM_y \prod_{p \le \sqrt{\log y}} (1 - \frac{\omega(p)}{p^2}) = \mathcal{O}(M_y)\text{)} \\
=&y \prod_{p \le \sqrt{\log y}} (1 - \frac{\omega(p)}{p^2}) + \mathcal{O}(M_y) \\
=&y \prod_{p \le \sqrt{\log y}} (1 - \frac{\omega(p)}{p^2}) + o(y) && \text{(nach Lemma 4, Aussage 1)} \\
\sim& c(f) y
\end{aligned}$$

Damit wurde gezeigt, dass diese Menge bereits die vom Theorem von Granville postulierte Dichte besitzt. Es genügt also, nun noch zu zeigen, dass die „Störmenge“ $\{0 \le n \le y | f(n) \equiv 0 \mod p^2$ für ein $p > \sqrt{\log y}\}$ die asymptotische Dichte Null besitzt. Dafür wird diese Menge noch einmal in zwei Teilmengen zerschnitten. Zuerst betrachtet man die Menge:

$$\{0 \le n \le y | \exists p : \sqrt{\log y} < p \le y; f(n) \equiv 0 \mod p^2\}$$

Diese Menge soll nun nach oben abgeschätzt werden, um zu zeigen, dass sie asymptotisch Dichte Null besitzt. Für jede einzelne Primzahl p kann man dafür die natürlichen Zahlen in Abschnitte der Länge p^2 einteilen. Dann enthält jeder Abschnitt nach Definition genau $\omega(p)$ Elemente die kongruent zu Null modulo p^2 sind. Das ergibt, wenn man die Anzahl der Abschnitte nach oben abschätzt:

$$
\begin{aligned}
&|\{0 \leq n \leq y | \exists p : \sqrt{\log y} < p \leq y; f(n) \equiv 0 \mod p^2\}| \\
\leq &\sum_{\sqrt{\log y} < p \leq y} \omega(p) \lceil \frac{y}{p^2} \rceil \\
\leq &\sum_{\sqrt{\log y} < p \leq y} \omega(p) \lfloor \frac{y}{p^2} \rfloor + \sum_{\sqrt{\log y} < p \leq y} \omega(p) \\
\leq &\sum_{\sqrt{\log y} < p} \omega(p) \lfloor \frac{y}{p^2} \rfloor + \sum_{p \leq y} \omega(p) \\
\leq &y \sum_{\sqrt{\log y} < p} \frac{\omega(p)}{p^2} + \sum_{p \leq y} \omega(p) \\
\ll &y \sum_{\sqrt{\log y} < p} \frac{1}{p^2} + \sum_{p \leq y} \omega(p) && \text{(nach Satz 1)} \\
= &\mathcal{O}(\frac{y}{\sqrt{\log y}}) + \mathcal{O}(\frac{y}{\sqrt{\log y}}) && \text{(nach Lemma 4, Aussage 2 und 3)} \\
= &\mathcal{O}(\frac{y}{\sqrt{\log y}}) \\
= &o(y)
\end{aligned}
$$

Damit hat die Menge asymptotische Dichte Null und man hat insgesamt:

$$\{0 \leq n \leq y | f(n) \not\equiv 0 \mod p^2 \qquad \forall p \leq y\} \sim c(f)y$$

Bisher wurde die abc-Vermutung noch nicht verwendet, die obige Gleichung gilt somit ganz allgemein. Um diese jedoch nun noch zum Theorem von Granville zu verallgemeinern, benötigt man Satz 2, der wiederum die abc-Vermutung voraussetzt. Sei dafür d der Grad des betrachteten Polynoms f und seien $x_1, x_2, \ldots, x_d$ die Nullstellen von f. Wähle dann $m \in \mathbb{N}$ so, dass $m > diam\{x_1, x_2 \ldots, x_d\}$ ist. Sei $\epsilon > 0$ beliebig mit $\epsilon < 1$. Wähle dann $l \in \mathbb{N}$ so, dass $\frac{1}{l+1} < \epsilon$ ist. Definiere dann für $0 \leq i < m$:

$$g_i(x) := f(x+i)f(x+m+i)f(x+2m+i) \cdot \ldots \cdot f(x+lm+i)$$

Dabei taucht jeder Funktionswert $f(x), f(x+1), f(x+2), \ldots, f(x+(l+1)m-1)$ genau ein Mal als Faktor in einem der g_i auf. Ziel soll es nun sein, den Satz 2 auf die Polynome g_i anzuwenden. Dafür müssen die Voraussetzungen des Satzes überprüft werden. Das Polynom f hat keine mehrfache Nullstelle, also haben auch alle einzelnen Faktoren von g_i keine mehrfachen Nullstellen. Die einzige verbleibende Möglichkeit wäre, dass zwei Faktoren eine gemeinsame

Nullstelle hätten. Angenommen, dies wäre der Fall und es gäbe ein x^* mit $f(x^* + rm + i) = f(x^* + r'm + i) = 0$ und $r \neq r'$, also o.E. $r > r'$. Dann sind aber $x^* + rm + i$ und $x^* + r'm + i$ Nullstellen von f. Wegen

$$\begin{aligned} x^* + rm + i - (x^* + r'm + i) &= (r - r')m \\ &\geq m \\ &> diam\{x_1, x_2, \ldots, x_d\} \end{aligned}$$

ist dies ein Widerspruch, da $x_1, x_2, \ldots, x_d$ bereits alle Nullstellen von f sind. Also haben je zwei Faktoren von g_i keine gemeinsame Nullstelle und g_i hat nur einfache Nullstellen. Damit ist Satz 2 anwendbar und es gilt für alle $n \in \mathbb{Z}$ mit $g_i(n) \neq 0$:

$$|n|^{(l+1)d-1-\epsilon} \ll rad(g_i(n))$$

Sei $n \in \mathbb{Z}$ mit $g_i(n) \neq 0$. Dann gibt es Zahlen $u(n), v(n) \in \mathbb{N}$ so dass $u(n)$ quadratfrei ist und $g_i(n) = \pm u(n)(v(n))^2$. Dann ist $rad(g_i(n)) \leq u(n)v(n)$, also:

$$|n|^{(l+1)d-1-\epsilon} \ll u(n)v(n)$$

Weiter ist mit dem führenden Koeffizienten a_d von f das asymptotische Wachstum $|g_i(n)| = u(n)(v(n))^2 \sim |a_d|^{(l+1)}|n|^{(l+1)d}$. Damit folgt:

$$\begin{aligned} v(n) &= \frac{u(n)(v(n))^2}{u(n)v(n)} \\ &\ll \frac{u(n)(v(n))^2}{|n|^{(l+1)d-1-\epsilon}} \\ &\ll \frac{|n|^{(l+1)d}}{|n|^{(l+1)d-1-\epsilon}} \\ &= |n|^{1+\epsilon} \end{aligned}$$

Angenommen, es gäbe Primzahlen $p, q > y \geq n$ mit $p^2 | g_i(n)$ und $q^2 | g_i(n)$.

$$\begin{aligned} &\Rightarrow p|v(n) \wedge q|v(n) \text{ (da } u(n) \text{ quadratfrei)} \\ &\Rightarrow pq|v(n) \\ &\Rightarrow pq \leq v(n) \ll |n|^{1+\epsilon} \\ &\Rightarrow |n|^2 \leq pq \leq C|n|^{1+\epsilon} \\ &\Rightarrow |n| \leq C|n|^{\epsilon} \end{aligned}$$

für ein $C > 0$. Da $\epsilon < 1$ gewählt wurde, ist dies für große n ($n > n_i$) ein Widerspruch. Für $n > n_i$ gilt also, dass es höchstens ein $p > y$ gibt, so dass $p^2 | g_i(n)$. Damit wird auch höchstens einer der Faktoren $f(n + i), f(n + m + i), \ldots, f(n + lm + i)$

von einem p^2 mit $p > y$ geteilt. Da dies für alle $g_i(n)$ gilt, können von den Faktoren $f(n), f(n+1), f(n+2), \ldots, f(n+(l+1)m-1)$ höchstens m von einem p^2 mit $p > y$ geteilt werden. Dies ermöglicht erneut eine Unterteilung der natürlichen Zahlen in Abschnitte der Länge $(l+1)m$, in denen nur jeweils m Zahlen einen quadratischen Primteiler größer als y besitzen. Dafür muss jedoch darauf geachtet werden, dass sowohl für alle i die Bedingung $n > n_i$ als auch die Bedingung $g_i(n) \neq 0$ eingehalten wird. Das ist jedoch sicher der Fall, wenn man $n > N$ mit $N := max\{n_0, n_1, \ldots, n_{m-1}, |x_1|, |x_2|, \ldots, |x_d|\}$ wählt. Es sollen also alle natürlichen Zahlen größer als N in Abschnitte der Länge $(l+1)m$ unterteilt werden. Dies ergibt die Abschätzung:

$$\begin{aligned}
&\limsup_{y\to\infty} \frac{1}{y} |\{0 \leq n \leq y | \exists p > y : f(n) \equiv 0 \mod p^2\}| \\
\leq &\limsup_{y\to\infty} \frac{1}{y} \left(\left\lceil \frac{y}{(l+1)m} \right\rceil m + N \right) \\
\leq &\limsup_{y\to\infty} \frac{1}{y} \left(\left(\frac{y}{(l+1)m} + 1 \right) m + N \right) \\
= &\limsup_{y\to\infty} \frac{1}{y} \left(\frac{y}{l+1} + m + N \right) \\
= &\limsup_{y\to\infty} \left(\frac{1}{l+1} + \frac{m+N}{y} \right) \\
= &\frac{1}{l+1} \\
< &\epsilon
\end{aligned}$$

Damit ist:

$$|\{0 \leq n \leq y | \exists p > y : f(n) \equiv 0 \mod p^2\}| = o(y)$$

und

$$\begin{aligned}
&|\{0 \leq n \leq y | f(n) \text{ ist quadratfrei}\}| \\
= &|\{0 \leq n \leq y | \forall p \leq y : f(n) \not\equiv 0 \mod p^2\}| - o(y) \\
\sim &c(f)y
\end{aligned}$$

$\square$

Damit ist die Aussage des Theorems von Granville bewiesen.

Literatur

[1] Lukas Pottmeyer, *Die Dichte quadratfreier Werte ganzzahliger Polynome*; Diplomarbeit, TU Dortmund (2009).

[2] Andrew Granville, *ABC Allows Us to Count Squarefrees*; International Mathematics Research Notices, No. 19, S. 991 - 1009 (1998)