Seminar der AlZAGK
SS 2010

Dichte quadratfreier Polynomwerte I

Dilara Badem
dilara@uni-bremen.de

8. Dezember 2010

Inhaltsverzeichnis

Einleitung **III**

Notationen **IV**

1 abc-Vermutung **1**

2 Satz von Granville **3**

Literaturverzeichnis **6**

Einleitung

Diese Arbeit ist die schriftliche Ausarbeitung des Vortrags über die "Dichte quadratfreier Polynomwerte I" im Seminar der AlZAGK im Sommersemester 2010. Grundlage dieser Ausarbeitung ist die Diplomarbeit über "Die Dichte quadratfreier Werte ganzzahliger Polynome"von Lukas C. Pottmeyer.
Dieser Vortrag ist einer aus einer Reihe von Vorträgen zur *abc*-Vermutung. Daher wird im ersten Kapitel diese Vermutung vorgestellt.
Das zweite Kapitel ist der Hauptteil der Arbeit und beschäftigt sich mit mit dem Satz von Granville, welcher besagt, dass die Vermutung von Erdős aus der *abc*-Vermutung folgt. Der Beweis des Satzes wird hier nur vorbereitet, denn die Durchführung des Beweises erfolgt im Vortrag "Dichte quadratfreier Polynomwerte II".

Notationen

Seien f und g Funktionen nach $\mathbb{R}$. Existiert ein $c < \infty$, sodass $|f| \leq |cg|$ gilt für $x \to \infty$, wird $f \ll g$ geschrieben, wobei $\ll$ das **Vinogradov-Symbol** ist.

Das **Radikal** $\mathrm{rad}(n)$ einer natürlichen Zahl n bezeichnet den größten quadratfreien Teiler dieser Zahl, d.h es gilt $\mathrm{rad}(n) = \prod_{p|n} p$.

1 abc-Vermutung

1.1 abc-Vermutung

Seien $a, b, c \in \mathbb{N}$ paarweise teilerfremde Zahlen mit $a + b = c$. Dann existiert zu jedem $\varepsilon > 0$ eine Konstante $C(\varepsilon)$, sodass gilt

$$c \leq C(\varepsilon) rad(abc)^{1+\varepsilon}$$

1.2 Satz

Sei $\varepsilon > 0$ und $F(x, y) \in \mathbb{Z}[x, y]$ ein homogenes Polynom vom Grad d, welches über $\mathbb{C}$ in paarweise verschiedene Linearfaktoren zerfällt. Dann impliziert die *abc*-Vermutung 1.1, dass für alle $m, n \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = 1$ und $F(m, n) \neq 0$ gilt

$$\max\{|m|, |n|\}^{d-2-\varepsilon} \ll \mathrm{rad}(F(m, n))$$

Dies ist eine Folgerung aus der *abc*-Vermutung und wird $F(x, y) := xy(y - x)$ gewählt, F homogen vom Grad $d = 3$, ist dieses Satz sogar äquivalent zur *abc*-Vermutung. Es gilt nämlich:

$$\begin{aligned} \max\{|m|, |n|\}^{1-\varepsilon} &\ll \mathrm{rad}(mn(n-m)) \\ \max\{|m|, |n|\} &\ll \mathrm{rad}(mn(n-m))^{1+\varepsilon} \end{aligned}$$

Beweis: Der Beweis wird in dieser Ausarbeitung nicht ausgeführt.
Siehe dazu: "*ABC allows us to count squarefrees*" von Granville, Theorem 5

Das folgende Korollar ist eine Folgerung des obigen Satzs und wird im Beweis des Satzes von Granville gebraucht.

1.3 Korollar

Sei $\varepsilon > 0$ und $f(x) \in \mathbb{Z}[x]$ quadratfrei und vom Grad d, dann impliziert die *abc*-Vermutung, dass für alle $n \in \mathbb{Z}$ mit $f(n) \neq 0$ gilt

$$|n|^{d-1-\varepsilon} \ll \mathrm{rad}(f(n))$$

Beweis: Es wird das Polynom $F(x, y) = y^{d+1} f(\frac{x}{y})$ betrachtet, welches offensichtlich ein homogenes Polynom vom Grad $d + 1$ ist. Seien $x_1, ..., x_d$ die Nullstellen von f. Dann erhält man

$$F(x, y) = y^{d+1} f\left(\frac{x}{y}\right) = y^{d+1}\left(\frac{x}{y} - x_1\right) \cdot ... \cdot \left(\frac{x}{y} - x_d\right) = y(x - yx_1) \cdot ... \cdot (x - yx_d)$$

Da f nach Voraussetzung quadratfrei ist, sind dies paarweise verschiedene Linearfaktoren. Es sind also alle Voraussetzungen für das Satz 1.2 erfüllt. Es gilt: $F(n,1) = f(n)$. Dann folgt mit 1.2

$$|n|^{d-1-\varepsilon} \ll \mathrm{rad}(F(n,1)) = \mathrm{rad}(f(n))$$

□

2 Satz von Granville

Unser Ziel ist es, Aussagen über die Anzahl bzw. die Dichte von quadratfreien Werten von Polynomen über $\mathbb{Z}$ zu treffen. Dazu sollte f quadratfrei sein und die Werte von f dürfen keine fixierten quadratischen Teiler besitzen, d.h es existiert kein p, sodass p^2 für alle $n \in \mathbb{Z}$ ein Teiler von $f(n)$ ist. Aber man kann meist nur schwer erkennen, ob ein Polynom die zweite Bedingung erfüllt, was auch das folgende kleine Beispiel zeigt.
Sei $f(x) = x^4 - 6x^3 + 11x^2 - 6x = x(x-1)(x-2)(x-3)$. Es gilt: $24 \mid f(n)$ für alle $n \in \mathbb{Z}$.
Der folgende Satz gibt eine Hilfestellung bei der Suche nach fixierten quadratischen Teilern.

2.1 Satz

Sei $f(x) \in \mathbb{Z}[x]$ vom Grad d und sei der größte gemeinsame Teiler aller Koeffizienten von $f(x)$ gleich 1. Sei $k \neq 1$ ein fester Teiler der Werte $f(n)$ mit $n \in \mathbb{Z}$. Dann ist k ein Teiler von $d!$.

Beweis: Sei $f(x) = a_0 + a_1 x + ... + a_d x^d$. Da nach Voraussetzung k ein fester Teiler der Werte $f(n)$ ist, gilt $f(n) \equiv 0 \bmod k$ für aale n. Es werden nun die Kongruenzen mit $n \in \{0, 1, ..., d\}$ betrachtet und wir erhalten

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & ... & 0 \\ 1 & 1 & 1 & ... & 1 \\ 1 & 2 & 4 & ... & 2^d \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & d & d^2 & ... & d^d \end{pmatrix}}_{=:A} \cdot \underbrace{\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_d \end{pmatrix}}_{=:\overline{a}} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod k,$$

wobei $\overline{a} \not\equiv \overline{0} \bmod k$ gilt, da der größte gemeinsame Teiler aller Koeffizienten von $f(x)$ gleich 1 ist. Dann muss die Determinante von A einen gemeinsamen Teiler mit k besitzen. A ist eine Van-der-Monde-Matrix und daher ist die Determinante einfach zu bestimmen

$$\det(A) = \prod_{d+1 \geq k > j \geq 1} ((k-1) - (j-1)) = d! \cdot (d-1)! \cdot ... \cdot 2! \cdot 1!$$

Da der $\mathrm{ggT}(k, \det(A)) \neq 1$ ist, ist $\mathrm{ggT}(k, d!) \neq 1$. Sei $g := \mathrm{ggT}(k, d!)$ und sei $k := g \cdot \overline{k}$ mit $\mathrm{ggT}(\overline{k}, d!) = 1$.
Da $\overline{k}$ ein Teiler von k ist, gilt auch

$$A \cdot \overline{a} \equiv \overline{0} \bmod \overline{k}.$$

Nun wollen wir zeigen, dass $\overline{k} = 1$ ist. Dazu nehmen wir an: $\overline{k} \neq 1$.
Da $\mathrm{ggT}(\overline{k}, d!) = 1$ ist, ist auch $\mathrm{ggT}(\overline{k}, \det(A)) = 1$. Daher ist A in $\mathbb{Z}/\overline{k}\mathbb{Z}$ invertierbar.

Also gilt

$$\begin{aligned} A \cdot \overline{a} &\equiv \overline{0} \bmod \overline{k} \\ \Rightarrow A^{-1} \cdot A \cdot \overline{a} &\equiv A^{-1} \cdot \overline{0} \bmod \overline{k} \\ \Rightarrow \overline{a} &\equiv \overline{0} \bmod \overline{k} \end{aligned}$$

Dies ist ein Widerspruch dazu, dass der größte gemeinsame Teiler aller Koeffizienten von $f(x)$ gleich 1 ist. Also ist $\overline{k} = 1$ und $k = g = \text{ggT}(k, d!)$.
Daraus folgt die Behauptung. □

Nun folgen die Erdős Vermutung und das Satz von Granville, welche die Kernaussagen dieser Arbeit liefern.

2.2 Erdős Vermutung

Sei $f(x) \in \mathbb{Z}[x]$ quadratfrei und es existiere kein fixierter quadratischer Teiler der Werte von f. Dann besitzt die Folge $(f(n))_{n \in \mathbb{N}_0}$ unendlich viele quadratfreie Werte. Genauer gilt

$$\limsup_{y \to \infty} \left| \frac{|\{0 \leq n \leq y | f(n) \; quadratfrei\}|}{c(f)y} \right| = 1$$

für eine Konstante $c(f) > 0$.

Die Aussage der Vermutung ist überraschend, da man eigentlich erwarten würde, dass die Dichte der quadratfreien Polynomwerte um Größenordnungen kleiner ist als das y, aber stattdessen ist die Dichte asymptotisch gleich y multipliziert mit einer Konstanten. Diese Vermutung wurde bisher nur für $\deg(f) \in \{1, 2, 3\}$ bewiesen. Allgemein konnte der Beweis dieser Vermutung nur unter Annahme der *abc*-Vermutung erbracht werden.

2.3 Satz von Granville

abc-Vermutung $\Rightarrow$ Erdős Vermutung

Der Beweis dieses Satzes ist Teil des Vortrags "Dichte quadratfreier Polynomwerte II" und wird daher in dieser Ausarbeitung nicht durchgeführt.
Im folgenden sind Definition und Vorüberlegungen zu finden, die für den Beweis des Satzes benötigt werden.

2.4 Definition

Sei p eine Primzahl. Die Anzahl der Lösungen der Kongruenz $f(n) \equiv 0 \bmod p^2$ wird mit $\omega(p)$ bezeichnet. Also gilt

$$\omega(p) := |\{n | f(n) \equiv 0 \bmod p^2, 0 \leq n \leq p^2 - 1\}|.$$

2.5 Definition

Sei R ein Integritätsring und $Q(R)$ sein Quotientenkörper. Weiter sei $f \in R[x]$ mit $\text{grad}(f) = d$. Sind $y_1, ..., y_d$ alle Nullstellen von f in einem algebraischen Abschluss von $Q(R)$, so ist die Diskriminante von f definiert als

$$\Delta f := a_d^{2d-2} \prod_{i<j} (y_i - y_j)^2,$$

wobei a_d der höchste Koeffizient von f ist.

2.6 Satz

Sei f wie in Definition 2.5. Dann ist $\Delta f \in R$.

Beweis: Sei $f(x) = a_0 + a_1 x + ... + a_d x^d$ und sei $f'(x) = a_1 + 2a_2 x + ... + d a_d x^{d-1}$ die Ableitung von f. Sei A eine $(2d-1) \times (2d-1)$-Matrix mit den Einträgen

$$a_{i,j} := \begin{cases} a_{d-(j-i)} & \text{für } 1 \leq i \leq d-1 \\ (1+i-j)a_{1+i-j} & \text{für } d \leq i \leq 2d-1 \end{cases},$$

wobei alle $a_k = 0$ für $k \notin \{0, 1, ..., d\}$ gilt. Es gilt

$$\Delta f = (-1)^{d(d-1)/2} a_d^{-1} \det(A)$$

und folgt aus der Resultanten-Theorie (siehe dazu z.B Cohen, Henri: A corse in computational algegraic number theory, Proposition 3.3.5). Da alle Einträge von A aus R sind, ist auch $\det(A) \in R$. Weiter sind a_d und $d a_d$ die einzigen Einträge ungleich Null in der ersten Spalte von A. Also ist $\det(A)$ teilbar durch a_d und damit gilt auch $a_d^{-1} \det(A) \in R$. □

2.7 Satz

Seien R und R' zwei Integritätsringe, $\varphi : R \to R'$ ein Ringhomomorphismus und $\tilde{\varphi} : R[x] \to R'[x]$ die kanonische Erweiterung von φ. Dann gilt für jedes $f \in R[x]$

$$\varphi(\Delta f) = \Delta \tilde{\varphi}(f).$$

Beweis: Sei d der Grad von f. Sei A wie im letzten Beweis und

$$\Delta f = (-1)^{d(d-1)/2} a_d^{-1} \det(A).$$

Zusammen mit $\varphi(\det(A)) = \det(\varphi(A))$ folgt dann die Behauptung. □

Insbesondere gilt für $f \in \mathbb{Z}[x]$: $\Delta \overline{f} = \overline{\Delta f}$, wobei $\overline{\cdot}$ die Reduktion modulo einer Primzahl ist.

2.8 Satz

Sei $f \in \mathbb{Z}[x]$ quadratfrei. Dann gilt für jede Primzahl p, welches die Diskriminante von f nicht teilt, die Ungleichung

$$\omega(p) \leq \text{grad}(f)$$

Beweis: Nach Voraussetzung ist $\Delta f \not\equiv 0 \bmod p$ und mit dem Satz 2.7 gilt $\Delta \overline{f} = \overline{\Delta f} \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Daher hat f modulo p keine mehrfachen Nullstellen und ist also quadratfrei. Nun werden

$$f(x) \equiv 0 \bmod p \tag{1}$$
$$f(x) \equiv 0 \bmod p^2 \tag{2}$$

betrachtet. Sei a eine Lösung der Kongruenz (1). Nun zeigen wir, dass es in der Restklasse von a modulo p genau eine Lösung der Kongruenz (2) gibt. Dazu betrachtet man die neue Kongruenz

$$f(a+pz) \equiv 0 \bmod p^2. \tag{3}$$

Durch die Taylor-Entwicklung von $f(a+pz)$ erhält man

$$f(a+pz) \equiv f(a) + pzf'(a) \bmod p^2.$$

Also ist die Kongruenz (3) äquivalent zu

$$f(a) + pzf'(a) \equiv 0 \bmod p^2$$

und dies ist äquivalent zu

$$\frac{f(a)}{p} + zf'(a) \equiv 0 \bmod p. \tag{4}$$

Diese Kongruenz ist wohldefiniert und eindeutig nach z lösbar, denn es gilt $f(a) \equiv 0 \bmod p$ und $f'(a) \not\equiv 0 \bmod p$. Letzteres gilt, da a sonst eine doppelte Nullstelle von f modulo p wäre. Alle Nullstellen der Kongruenz (3) liegen also in derselben Restklasse modulo p. Seien $a + pz_1, ..., a + pz_n$ die Lösungen der Kongruenz (3). Dann existiert wegen (4) eine natürliche Zahl b so, dass für alle $i \in \{1, ..., n\}$ gilt

$$\begin{aligned} z_i &\equiv b \bmod p \\ \Rightarrow f(a+pb) &\equiv 0 \bmod p^2. \end{aligned}$$

Also ist $a + pb$ aus der Restklasse a modulo p die einzige Lösung der Kongruenz (2). Außerdem gilt

$$f(a) \not\equiv 0 \bmod p \Rightarrow f(a+pz) \not\equiv 0 \bmod p^2.$$

Also besitzen (1) und (2) gleich viele Lösungen und, da $\mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper ist, ist die Anzahl der Lösungen durch den Grad von f beschränkt. □

Literaturverzeichnis

- Pottmeyer,L.(2009): Die Dichte quadratfreier Werte ganzzahliger Polynome, Diplomarbeit - TU Dortmund.
- Granville, A.(1998): ABC allows us to count squarefrees, International Mathematical Research Notices No.19 S.991-1009.
- Cohen, H. (2000): A corse in computational algebraic number theory, New York, Springer.