Die Dichte quadratfreier Werte ganzzahliger Polynome

Diplomarbeit

von

Lukas Christopher Pottmeyer

Dem Fachbereich Mathematik der TU Dortmund vorgelegt

im Juli 2009.

Betreuer: Prof. Dr. Walter Gubler

Inhaltsverzeichnis

Einleitung

Diese Arbeit widmet sich einer weniger bekannten Folgerung aus der *abc*-Vermutung. Die *abc*-Vermutung ist eine zahlentheoretische Vermutung, die 1985 von David Masser und Joseph Oesterlé auf einer Konferenz in Bonn formuliert wurde. Sie entstand im Zusammenhang mit der Betrachtung elliptischer Kurven. Für eine genauere Erklärung der Entstehung sei hier auf [re] verwiesen, wo Briefe von Masser und Oesterlé veröffentlich sind, die die Herleitung der Vermutung genauer erläutern.
Das Radikal einer Zahl n ungleich 0 ist definiert als $\mathrm{rad}(n) := \prod_{p|n} p$. Also bezeichnet das Radikal das Produkt aller verschiedenen Primteiler eines Elementes. Daher kann diese Definition für alle faktoriellen Ringe benutzt werden. Die *abc*-Vermutung besagt nun Folgendes:

abc-Vermutung 0.1. *Seien $a, b, c \in \mathbb{N}$ paarweise teilerfremde Zahlen mit $a+b = c$. Dann existiert zu jedem $\varepsilon > 0$ eine Konstante $C(\varepsilon)$, so dass für jedes Tupel $(a, b, c) \in \mathbb{N}^3$ der obigen Form gilt*

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

Grob formuliert behauptet die *abc*-Vermutung also, dass das Produkt aller paarweise verschiedener Primteiler der Elemente einer Gleichung $a + b = c$ aus $\mathbb{Z}$ nicht „viel kleiner“ werden kann als das betragsmäßige Maximum von a, b und c. Durch eine geeignete Umstellung der Gleichung kann man ohne Einschränkung annehmen, dass $a, b, c \in \mathbb{N}$ sind.
Es existieren viele verschiedene Formulierungen der *abc*-Vermutung. Eine der bekanntesten expliziten Formulierungen ist die, in der $\varepsilon = C(\varepsilon) = 1$ gesetzt wird. Also, dass unter den Voraussetzungen von 0.1 stets die Ungleichung

$$c \leq \mathrm{rad}(abc)^2$$

erfüllt ist. Diese Formulierung wird auch als *schwache abc-Vermutung* bezeichnet und könnte durch ein Gegenbeispiel widerlegt werden. Tupel (a, b, c) wie in 0.1 können durch die Funktion $L(a, b, c) := \frac{\log c}{\log \mathrm{rad}(abc)}$ bewertet werden. Die schwache *abc*-Vermutung ist also äquivalent zu der Aussage

$$L(a, b, c) \leq 2$$

für alle teilerfremden natürlichen Zahlen a, b, c, die die Gleichung $a + b = c$ erfüllen. Um ein Gegenbeispiel für die schwache *abc*-Vermutung zu finden, muss also ein Tupel (a, b, c) gefunden werden, dessen Bewertung größer als 2 ist. Mit einer Bewertung

von $1,62991$ ist das Beispiel $a = 2$, $b = 3^{10} * 109$ und $c = 23^5$, welches von Eric Reyssat konstruiert wurde, das bisher „Beste“. Einen weniger konstruktiven als direkten Zugang liefert die Internetseite [re], die 2006 von der Universität Leiden ins Leben gerufen wurde. Hier wird von so vielen Gleichungen obiger Form wie möglich $L(a, b, c)$ ausgerechnet, in der Hoffnung neue Tupel (a, b, c) mit einer hohen Bewertung zu finden. Bis zum Erscheinen dieser Arbeit (Juli 2009) sind dort mehr als $123 * 10^{12}$ Gleichungen getestet worden, von denen 7576651 eine Bewertung größer als 1 hatten.

Ein Beweis der *abc*-Vermutung in jeglicher Formulierung hätte weitreichende zahlentheoretische Folgen. So ist zum Beispiel Fermats letzter Satz eine Konsequenz der schwachen *abc*-Vermutung.
Angenommen es existieren Zahlen $x, y, z \in \mathbb{N}$ so, dass die Gleichung $x^n + y^n = z^n$ erfüllt ist für eine Zahl $n \geq 3$. Dann folgt aus der schwachen *abc*-Vermutung

$$z^n \leq \mathrm{rad}((xyz)^n)^2 = \mathrm{rad}(xyz)^2 < z^6 \quad .$$

Hieraus folgt, dass $n \leq 5$ sein muss. Allerdings sind diese Fälle schon lange bekannt. Euler bewies im Jahr 1753 Fermats letzten Satz für $n = 3$, Fermat selbst bewies den Fall $n = 4$ (Mitte des 17. Jahrhunderts) und für $n = 5$ wurde die Aussage von Dirichlet und Legendre bewiesen (1825). Wird die *abc*-Vermutung 0.1 vorausgesetzt, führen dieselben Abschätzungen darauf, dass n beschränkt sein muss.

Neben Fermats letztem Satz lassen sich auch andere bekannte Sätze wie Roths Theorem und die Catalan-Vermutung aus der *abc*-Vermutung ableiten. Doch auch unbewiesene Vermutungen, wie die Szpiro- und die Hall-Vermutung, könnten unter Voraussetzung der *abc*-Vermutung bewiesen werden. Dies sind nur einige Beispiele von Konsequenzen, die verdeutlichen, dass die *abc*-Vermutung Anwendungen in der Theorie der elliptischen Kurven (Szpiro-Vermutung), der diophantischen Geometrie (Hall-Vermutung) und, wie in dieser Arbeit zu sehen, in der Polynomtheorie hat. An dieser Stelle sei kurz bemerkt, dass die *abc*-Vermutung für $\varepsilon = 0$ nicht erfüllt ist, da sich ein Gegenbeispiel durch die Folge von Gleichungen $1 + k = 3^{2^n}$ konstruieren lässt, wobei n über alle natürlichen Zahlen läuft (siehe [BG] Example 12.4.13). Neben schwächeren expliziten Formulierungen existieren auch diverse Verallgemeinerungen der *abc*-Vermutung. In dieser Arbeit ist eine Verallgemeinerung auf algebraische Zahlkörper (3.15) von besonderem Interesse. Aus dieser Formulierung folgt unter anderem die Mordell-Vermutung. Diese Vermutung bewies Gerd Faltings ohne

die *abc*-Vermutung zu benutzen. Für diesen Beweis wurde Faltings 1986 die Fields Medaille verliehen (ebenso wie Klaus Friedrich Roth für Roths Theorem (1958)). Analog zu 0.1 kann man auch eine *abc*-Vermutung auf Polynomringen über Körpern der Charakteristik 0 formulieren. Diese Version der *abc*-Vermutung wurde 1981 von Wilson Stothers bewiesen und gilt sogar für den Fall $\varepsilon = 0$:
Sei K ein Körper der Charakteristik 0. Dann ist der Polynomring $K[x]$ ein faktorieller Ring und man kann die Definition des Radikals auch für Polynome ungleich 0 benutzen. Sind $a(x), b(x), c(x)$ paarweise teilerfremde Polynome aus $K[x]\backslash\{0\}$, die nicht alle konstant sind und die Gleichung $a(x) + b(x) = c(x)$ erfüllen, so gilt

$$\max\{\text{grad}(a(x)), \text{grad}(b(x)), \text{grad}(c(x))\} \leq \text{grad}(\text{rad}(a(x)b(x)c(x))) - 1 \quad .$$

Ein Beweis dieses Theorems ist zum Beispiel in [BG] Theorem 12.4.1 gegeben.
Für weitere detaillierte Informationen zur *abc*-Vermutung wird auf [Bro] und [uc] verwiesen.

Eine andere Vermutung besagt, dass die Dichte der quadratfreien Werte in der Menge $f(0), f(1), ...$ positiv ist, wenn $f \in \mathbb{Z}[x]$ selbst quadratfrei ist und kein fixierter quadratischer Teiler der Werte von f existiert. Dies bedeutet also insbesondere, dass jedes dieser Polynome unendlich viele quadratfreie Werte darstellt. Dass f quadratfrei ist und die Werte von f keinen gemeinsamen quadratischen Teiler besitzen, sind die minimalen Voraussetzungen, die man an f stellen muss. Es ist nämlich klar, dass ein Polynom, das eine dieser Bedingungen erfüllt, keinen einzigen quadratfreien Wert annehmen kann. Allerdings ist sogar die Frage, ob jedes Polynom mit diesen Eigenschaften zumindest einen quadratfreien Wert annimmt, noch nicht geklärt. Sollte jedes dieser Polynome mindestens einen quadratfreien Wert annehmen, so würde bereits folgen, dass jedes dieser Polynome unendlich viele quadratfreie Werte annimmt (analog zum Beweis von Theorem 2 in [Fi1]).
Aufgrund seiner Forschungen auf diesem Gebiet wird diese Vermutung Paul Erdös zugesprochen und in dieser Arbeit als *Erdös Vermutung* bezeichnet. Trygve Nagel bewies in [Na] (1922) die Vermutung für Polynome vom Grad kleiner gleich 2. Dieses Resultat existierte also bereits vor Erdös Studien. Erdös selbst bewies 1953 in [Er], dass jedes quadratfreie Polynom vom Grad 3, dessen Werte keinen fixierten quadratischen Teiler besitzen, unendlich viele quadratfreie Werte darstellt. Jedoch konnte er in seiner Arbeit keine Aussage über die Dichte dieser Werte machen. 14 Jahre später konnte Christopher Hooley (in [Ho]) dieses Resultat verstärken und zeigen, dass die Dichte der quadratfreien Werte tatsächlich positiv ist (siehe auch Satz 2.4).

Jerzy Browkin, Michael Filaseta, George Greaves und Andrej Schinzel konnten 1997 in [BFGS] zeigen, dass man unter der Voraussetzung eines Beweises der *abc*-Vermutung auch Erdös Vermutung für alle zyklotonischen Polynome beweisen kann. Mit anderen Mitteln und unter Verwendung eines Theorems von Michael Langevin zeigte Andrew Granville 1998 in [Gr], dass Erdös Vermutung eine Folgerung aus der *abc*-Vermutung ist. Diese Aussage (aus der *abc*-Vermutung folgt Erdös Vermutung) wird im Folgenden als *Granvilles Theorem* bezeichnet. Ebenfalls in [Gr] wird gezeigt, dass man auch für Polynome aus $\mathbb{Z}[x, y]$ ein ähnliches Resultat erhalten kann.
Um nochmals die Aussagekraft der *abc*-Vermutung zu verdeutlichen sei erwähnt, dass bis heute von noch keinem irreduziblen Polynom vom Grad größer 3 gezeigt werden konnte, dass es unendlich viele quadratfreie Werte darstellt. Sogar die Existenz eines solchen Polynoms ist noch nicht geklärt (siehe [Fi2]).

Die vorliegende Arbeit ist in drei Kapitel unterteilt. Im ersten Kapitel wird zunächst Granvilles Theorem bewiesen. Hierbei folgen wir dem Beweis aus [BG] (12.2.15). Später im selben Kapitel werden die Bedingungen an das Polynom etwas gelockert und es wird Folgendes bewiesen:

Granvilles Theorem (verallgemeinerte Version) 0.2. *Sei $f(x)$ ein quadratfreies Polynom aus $\mathbb{Z}[x]$, B der größte gemeinsame Teiler aller Werte $f(n), n \in \mathbb{Z}$. Sei B' der kleinste Teiler von B für den $\frac{B}{B'}$ quadratfrei ist. Unter der Voraussetzung, dass die abc-Vermutung 0.1 allgemein gültig ist, folgt*

$$\left| \left\{ 0 \leq n \leq y \,\middle|\, \frac{f(n)}{B'} \text{ quadratfrei} \right\} \right| \sim c(f)y$$

für $c(f) > 0$ konstant.

Diese Formulierung ist deshalb interessant, weil es Polynome gibt, die zwar normiert sind, doch deren Werte trotzdem einen fixierten quadratischen Teiler besitzen. Ein Beispiel für ein solches Polynom ist $f(x) = x(x-1)(x-2)(x-3)$. Denn es ist stets genau einer der Faktoren von f durch 4 teilbar.
Das zweite Kapitel widmet sich Erdös Vermutung ohne sich auf die *abc*-Vermutung zu stützen. Es werden die Fälle bewiesen, in denen der Grad des Polynoms kleiner gleich 2 ist. Leider wird in dem Kapitel auch festgestellt, dass sich der Beweis dieser Fälle, ebenso wie Hooleys Beweis für Polynome vom Grad 3, nicht auf Polynome höheren Grades übertragen lässt.
Der Hauptteil dieser Arbeit ist das dritte Kapitel, in dem Granvilles Theorem für

beliebige Zahlkörper bewiesen wird. Dass dies möglich ist, erwähnte Granville in seiner Arbeit ohne jedoch eine Formulierung oder einen Beweis anzugeben. Es liegt auf der Hand, dass in diesem Fall die *abc*-Vermutung für beliebige Zahlkörper benutzt werden muss. Sei K ein Zahlkörper vom Grad n. Wir benutzen die Bezeichnungen s für die Anzahl von komplexen Einbettungen von K, $\|.\|_\infty$ für die Maximumsnorm auf $\mathbb{R}^n$, $\mathfrak{o}_K$ für den Ring der ganz-algebraischen Zahlen in K und Δ_K für die Diskriminante von K. Die Funktion $\varphi : K \longrightarrow \mathbb{R}^n$ beschreibt die Abbildung

$$a \mapsto (\sigma_1(a), ..., \sigma_r(a), \mathrm{Re}(\sigma_{r+1}(a)), \mathrm{Im}(\sigma_{r+1}(a)), ..., \mathrm{Re}(\sigma_{r+s}(a)), \mathrm{Im}(\sigma_{r+s}(a))) \quad ,$$

wobei $\sigma_1, ..., \sigma_r$ alle reellen Einbettungen und $\sigma_{r+1}, ..., \sigma_{r+s}$ die paarweise nicht konjugierten komplexen Einbettungen von K in einen algebraischen Abschluss von K sind. Mit diesen Bezeichnungen beweisen wir folgendes Theorem:

Granvilles Theorem für beliebige Zahlkörper 0.3. *Sei K ein Zahlkörper vom Grad n und $f(x) \in \mathfrak{o}_K[x]$ ein quadratfreies Polynom. Weiter existiere kein Primideal $P \lhd \mathfrak{o}_K$, so dass $f(a) \in P^2$ für alle $a \in \mathfrak{o}_K$. Unter Voraussetzung der abc-Vermutung für Zahlkörper gilt*

$$\left|\left\{a \in \mathfrak{o}_K \mid \|\varphi(a)\|_\infty \leq y, f(a) \notin P^2 \text{ für alle Primideale } P \lhd \mathfrak{o}_K\right\}\right| \sim c(f)\frac{2^{n+s}}{\sqrt{|\Delta_K|}}y^n$$

für eine Konstante $c(f) > 0$.

Der Beweis dieses Theorems orientiert sich am Beweis des Falles $K = \mathbb{Q}$ aus dem ersten Kapitel.

In den ersten beiden Kapiteln wird größtenteils elementare Zahlentheorie und etwas analytische Zahlentheorie benutzt. Die Methoden, die in Kapitel 3 angewendet werden, stammen hauptsächlich aus der algebraischen Zahlentheorie. Für die dabei verwendeten Grundlagen wird auf [Ne] verwiesen. Zwar benutzt die auf beliebige Zahlkörper verallgemeinerte *abc*-Vermutung Bezeichnungen aus der algebraischen Geometrie, doch ihre Folgerung wird, wie in 0.3 zu sehen, wieder in die Sprache der algebraischen Zahlentheorie zurück übersetzt.

Lukas Pottmeyer *Dortmund, im Juli 2009*

Notationen

Sind f und g zwei Funktionen nach $\mathbb{R}$, dann schreiben wir $f \ll g$, falls eine Konstante $C < \infty$ existiert, so dass gilt $|f| \leq |Cg|$. Analog bedeutet $f \gg g$, dass $g \ll f$ gilt. $\ll$ und $\gg$ heißen Vinogradov-Symbole.

Sind $f(x), g(x)$ Funktionen von $\mathbb{R}_0^+$ nach $\mathbb{R}$, deren sämtliche Nullstellen in einem beschränkten Intervall liegen, dann schreiben wir $f \in O(g)$ oder gleichbedeutend $f = O(g)$, falls

$$\limsup_{x \to \infty} \left| \frac{f(x)}{g(x)} \right| = C$$

für eine Konstante $C < \infty$ ist. Falls $C = 0$ ist, so schreiben wir $f \in o(g)$ oder $f = o(g)$. Sind f und g asymptotisch gleich, also $C = 1$, so schreiben wir $f \sim g$.

Der Inhalt eines Polynoms ist der größte gemeinsame Teiler aller Koeffizienten des Polynoms. Also insbesondere gleich eins für jedes normierte Polynom.

0 ist nicht enthalten in $\mathbb{N}$. Die Menge $\mathbb{N} \cup \{0\}$ wird $\mathbb{N}_0$ genannt. p bezeichnet stets eine Primzahl.

Sei $n \in \mathbb{N}$, dann bezeichnet $\mathrm{rad}(n)$ den größten quadratfreien Teiler von n. Es ist also $\mathrm{rad}(n) = \prod_{p|n} p$.

Die Anzahl aller Primzahlen bis zu einer Schranke $z \in \mathbb{R}$ wird $\pi(z)$ genannt.

Die Gaußklammern $\lfloor x \rfloor$ runden $x \in \mathbb{R}$ auf die nächst kleinere ganze Zahl ab. Analog rundet $\lceil x \rceil$ die Zahl $x \in \mathbb{R}$ auf die nächst größere ganze Zahl auf.
Für ein $x \in \mathbb{C}$ beschreibt $|x|$ den Standardbetrag auf $\mathbb{C}$. Ist H eine Menge, so bezeichnet $|H|$ die Kardinalität dieser Menge.

Eine Fundamentalmasche eines (Unter-)Gitters ist ein parallelepipedischer Fundamentalbereich.

$\mathfrak{o}_K$ bezeichnet den Ring der ganzalgebraischen Zahlen in einem algebraischen Zahlkörper K . Ist S die Menge aller $\mathbb{Q}$-Einbettungen von K in $\mathbb{C}$ (genauer, in einen algebraischen Abschluss von K), so gilt $|S| = [K : \mathbb{Q}] = n < \infty$.

Den üblichen Notationen entsprechend bezeichnen wir die Norm eines Elementes $a \in \mathfrak{o}_K$ mit $N(a) := N_{\mathbb{Q}}^K(a)$ und die Norm eines Ideals $I \lhd \mathfrak{o}_K$ mit $N(I) := N_{\mathbb{Q}}^K(I)$. Es gilt

$$|\prod_{\sigma \in S} \sigma(a)| = |N(a)| = N(a\mathfrak{o}_K) = |\mathfrak{o}_K / a\mathfrak{o}_K| \quad .$$

Sei K ein Zahlkörper, $\overline{K}$ ein algebraischer Abschluss von K und $m \in \mathbb{N}$. Dann bezeichnen wir mit $\mathbb{P}_K^m$ den m-dimensionalen projektiven Raum über K. Das bedeutet, dass $\mathbb{P}_K^m$ die Menge aller eindimensionalen Unterräume von $\overline{K}^{m+1}$ ist. Punkte in $\mathbb{P}_K^m$ schreiben wir als $\boldsymbol{x} := (x_0 : ... : x_m)$, mit $x_i \in \overline{K}$ und $x_i \neq 0$ für mindestens ein i. Die Teilmenge der Punkte aus $\mathbb{P}_K^m$, deren sämtliche Koeffizienten in K liegen, bezeichnen wir mit $\mathbb{P}_K^m(K)$.

1 Granvilles Theorem

abc-Vermutung 1.1. *Seien $a, b, c \in \mathbb{N}$ paarweise teilerfremde Zahlen mit $a+b=c$. Dann existiert zu jedem $\varepsilon > 0$ eine Konstante $C(\varepsilon)$, so dass für jedes Tupel $(a,b,c) \in \mathbb{N}^3$ der obigen Form gilt*

$$c \leqslant C(\varepsilon)\,\mathrm{rad}(abc)^{1+\varepsilon} \quad .$$

Theorem 1.2. *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*

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

Dieses Theorem ist eine bekannte Folgerung der *abc*-Vermutung (siehe z.B. [Gr] Theorem 5), dessen Beweis wir in dieser Arbeit nicht ausführen werden.

Es gilt sogar, dass die Aussage in Theorem 1.2 äquivalent ist zur *abc*-Vermutung. Denn setzen wir $F(x,y) := xy(y-x)$, so erhalten wir sofort 1.1.

Korollar 1.3. *Sei $\varepsilon > 0$ und $f(x) \in \mathbb{Z}[x]$ quadratfrei und vom Grad d, dann impliziert die abc-Vermutung 1.1, dass für alle $n \in \mathbb{Z}$ mit $f(n) \neq 0$ gilt*

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

Beweis: Betrachte das Polynom $F(x,y) = y^{d+1} f(\frac{x}{y})$. Dies ist offensichtlich homogen vom Grad $d+1$. Ebenso zerfällt $F(x,y)$ über $\mathbb{C}$ in paarweise verschiedene Linearfaktoren, denn seien $x_1, ..., x_d$ die Nullstellen von f, so gilt

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

Weiter gilt $F(n,1) = f(n)$ und somit nach Theorem 1.2

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

□

Wir wollen nun Aussagen über die Anzahl bzw. die Dichte von quadratfreien Werten von Polynomen über $\mathbb{Z}$ treffen. Zunächst ist klar, dass f hierfür selbst quadratfrei sein muss, da sonst keine quadratfreien Werte angenommen werden können. Weiter

betrachten wir zunächst nur Polynome, deren Werte keinen fixierten quadratischen Teiler besitzen. Das bedeutet, dass kein p existiert, sodass p^2 ein Teiler von $f(n)$ ist für alle $n \in \mathbb{Z}$. Polynome, denen man die Existenz eines festen quadratischen Teilers seiner Werte sofort ansieht, sind diejenigen, deren Inhalt nicht quadratfrei ist. Allerdings kann man im Allgemeinen einem Polynom nur schwer ansehen, ob seine Werte einen fixierten quadratischen Teiler besitzen.
Zum Beispiel gilt für $f(x) = x^4 - 6x^3 + 11x^2 - 6x$, dass $24 \mid f(n)$ für alle $n \in \mathbb{Z}$. Dies wird klar, wenn man sich die Zerlegung von f in Linearfaktoren ansieht, denn $f(x) = x(x-1)(x-2)(x-3)$. Dieses Beispiel eines fixierten Teilers ist in gewissem Sinne „optimal“, wie der folgende Satz zeigt.

Satz 1.4. *Sei $f(x) \in \mathbb{Z}[x]$ vom Grad d und der Inhalt von $f(x)$ sei gleich 1. Weiter sei $k \neq 1$ ein fester Teiler der Werte $f(n)$ mit $n \in \mathbb{Z}$. Dann ist k ein Teiler von $d!$.*

Beweis: Wir schreiben $f(x) = a_0 + a_1 x + ... + a_d x^d$. Da k fester Teiler der Werte von f ist, gilt für alle $n \in \mathbb{Z}$ die Kongruenzen $f(n) \equiv 0 \mod k$. Betrachten wir nur die Kongruenzen mit $n \in \{0, 1, ..., d\}$, so erhalten wir

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

Nach Voraussetzung gilt $\overline{a} \not\equiv \overline{0} \mod k$. Also besitzt k einen gemeinsamen Teiler mit der Determinante von A. Diese ist, da A eine Van-der-Monde-Matrix ist, leicht zu bestimmen. Es ist

$$\det(A) = d! \cdot (d-1)! \cdots 2! \cdot 1 \quad .$$

Also folgt aus $\mathrm{ggT}(k, \det(A)) \neq 1$ auch $g := \mathrm{ggT}(k, d!) \neq 1$. Wir schreiben $k = g \cdot k'$ mit $\mathrm{ggT}(k', d!) = 1$. Da k' ein Teiler von k ist, gilt immer noch

$$A \cdot \overline{a} \equiv \overline{0} \mod k' \quad .$$

Angenommen es gilt $k' \neq 1$. Da $\mathrm{ggT}(k', d!) = 1$ ist, gilt auch $\mathrm{ggT}(k', \det(A)) = 1$. Also ist A in $\mathbb{Z}/k'\mathbb{Z}$ invertierbar, woraus sich unmittelbar ergibt, dass $\overline{a} \equiv \overline{0} \mod k'$ gilt. Dies ist ein Widerspruch zur Voraussetzung, dass der Inhalt von f gleich 1 ist.

Also muss $k' = 1$ und somit $k \mid d!$ gelten. □

Die Vermutung, mit der wir uns beschäftigen wollen, besagt Folgendes:

Erdös Vermutung 1.5. *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*

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

für eine Konstante $c(f) > 0$.

Diese Vermutung ist bis heute nur für die Fälle $\text{grad}(f) \in \{1, 2, 3\}$ bewiesen worden (siehe Kapitel 2). Allerdings können wir die Vermutung allgemein beweisen, wenn die *abc*-Vermutung als gültig angesehen wird.

Granvilles Theorem 1.6. *Sei $f(x) \in \mathbb{Z}[x]$ ein quadratfreies Polynom vom Grad d, dessen Werte keinen fixierten quadratischen Teiler besitzen. Unter der Voraussetzung, dass die abc-Vermutung 1.1 allgemein gültig ist, folgt*

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

für $c(f) > 0$ konstant.

Wir können Granvilles Theorem also auch kurz schreiben als

$$abc\text{-Vermutung} \Rightarrow \text{Erdös Vermutung} .$$

Bevor wir dies beweisen, benötigen wir noch einige Vorüberlegungen und Definitionen.

Definition 1.7. *Die Anzahl der Lösungen der Kongruenz $f(n) \equiv 0 \mod p^2$ bezeichnen wir mit $\omega(p)$. Es gilt also*

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

Definition 1.8. *Sei R ein Integritätsbereich 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*

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

wobei a_d der höchste Koeffizient von f ist.

Diese Definition der Diskriminante ist eine sehr spezielle. Später werden wir eine sehr viel allgemeinere Definition betrachten.

Satz 1.9. *Sei f gewählt wie in Definition 1.8. Dann ist $\Delta f \in R$.*

Beweis: Sei f wie oben und f' die formale Ableitung von f. D.h. also,

$$f(x) = a_0 + a_1 x + ... + a_d x^d \quad \text{und} \quad f'(x) = a_1 + 2a_2 x + ... + d a_d x^{d-1} \ .$$

Betrachte die $(2d-1) \times (2d-1)$ Matrix A entstehend durch die Koeffizienten

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

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

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

(siehe z.B. [Co] Proposition 3.3.5 unter Berücksichtigung von 3.3.3 und 3.3.4). Da alle Koeffizienten von A aus R sind, ist auch $\det(A) \in R$. Weiter sind a_d und da_d die einzigen Einträge ungleich Null in der ersten Spalte von A. Also ist a_d ein Teiler der Determinante von A. Damit ist auch $a_d^{-1} \det(A) \in R$, was unseren Beweis beendet. □

Satz 1.10. *Seien R und R' zwei Integritätsbereiche, $\varphi : R \to R'$ ein Ringhomomorphismus und $\widetilde{\varphi} : R[x] \to R'[x]$ die kanonische Erweiterung von φ. Dann gilt für jedes $f \in R[x]$*

$$\varphi(\Delta f) = \Delta \widetilde{\varphi}(f) \quad .$$

Beweis: Sei d der Grad von f. Wir betrachten wieder die Matrix A aus dem Beweis von Satz 1.9 und die Gleichung

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

Durch diese Gleichung und mit der Tatsache, dass $\varphi(\det(A)) = \det(\varphi(A))$ (also φ angewendet auf alle Koeffizienten von A), kann der Beweis leicht geschlossen werden. □

Insbesondere gilt also für ein Polynom f aus $\mathbb{Z}[x]$, die Gleichung $\Delta\overline{f} = \overline{\Delta f}$, wobei $\overline{\cdot}$ die Reduktion modulo einer Primzahl ist.

Satz 1.11. *Sei $f \in \mathbb{Z}[x]$ quadratfrei, dann gilt für jedes p, das die Diskriminante von f nicht teilt, die Ungleichung*

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

Beweis: Zunächst zeigen wir, dass unter den gegebenen Voraussetzungen $\overline{f}$ ebenfalls quadratfrei ist. Es gilt $\Delta f \not\equiv 0 \mod p$. Nach Satz 1.10 ist $\Delta\overline{f} = \overline{\Delta f} \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Also kann f modulo p keine mehrfache Nullstelle haben und ist damit quadratfrei. Wir betrachten nun die Kongruenzen

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

Sei a eine Lösung von (1), dann wollen wir zeigen, dass es in der Restklasse von a modulo p genau eine Lösung von (2) gibt. Daher betrachten wir die neue Kongruenz

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

Durch Ausmultiplizieren erhalten wir

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

(3) ist also äquivalent zu $f(a) + pzf'(a) \equiv 0 \mod p^2$, was wiederum äquivalent ist zur Kongruenz

$$\frac{f(a)}{p} + zf'(a) \equiv 0 \mod p \quad .$$

Diese Kongruenz ist wohldefiniert und eindeutig lösbar, da $p \mid f(a)$ und $p \nmid f'(a)$ (es ist $f'(a) \not\equiv 0 \mod p$, da a sonst eine doppelte Nullstelle von f modulo p wäre). Alle Nullstellen von (3) liegen also in der selben Restklasse modulo p. Hieraus folgt, dass (2) genau eine Lösung in der Restklasse von a modulo p besitzt. Weiter gilt

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

Also besitzen (1) und (2) tatsächlich gleich viele Lösungen und da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, ist diese Anzahl durch grad(f) beschränkt. □

Kommen wir nun zum Beweis von Granvilles Theorem 1.6.

Beweis von 1.6: Sei $c_p(f) := 1 - \frac{\omega(p)}{p^2}$. Angenommen es wäre $c_p(f) = 0$ für ein p, dann würde folgen, dass $\omega(p) = p^2$, also dass $f(n) \equiv 0 \mod p^2$ für alle $n \in \mathbb{Z}$ ist.

Da f aber als Polynom ohne fixierten quadratischen Teiler der Werte $f(n)$, $n \in \mathbb{Z}$, gewählt wurde, kann ein solches p nicht existieren. Daher ist $c_p(f) \neq 0$ für alle p. Die Summe über alle Brüche $\frac{d}{m^2}$, wobei m über alle natürlichen Zahlen mit $m^2 > d$ läuft, konvergiert (absolut). Damit konvergiert auch das Produkt $\prod_{m\in\mathbb{N},m^2>d}(1-\frac{d}{m^2})$ absolut (siehe [Le] 19.3 Proposition 5). Es gilt also $\prod_{m\in\mathbb{N},m^2>d}(1-\frac{d}{m^2}) > 0$. Damit folgt für ein $s > \max\{d, \Delta f\}$

$$\prod_p c_p(f) \geq \prod_{p\leq s}(1-\frac{\omega(p)}{p^2})\prod_{p>s}(1-\frac{d}{p^2}) > 0 \quad .$$

Dies gilt, da das erste Produkt endlich und das zweite offensichtlich größer als $\prod_{m\in\mathbb{N},m^2>d}(1-\frac{d}{m^2}) > 0$ ist. Das s ist gerade so gewählt, dass ein $p > s$ kein Teiler von Δf sein kann und stets $\frac{d}{p^2} < 1$ gilt. Daher können wir nach Satz 1.11 $\omega(p)$ durch d abschätzen für alle $p > s$.

Sei nun y eine beliebige große Zahl, dann definieren wir

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

Behauptung: Für jedes $t \in \mathbb{Z}$ liegen in der Menge $\{t, t+1, ..., t+M_y-1\}$ genau $\prod_{p\leq\sqrt{\log y}}(p^2-\omega(p))$ Zahlen n, so dass $f(n) \not\equiv 0 \mod p^2$ für alle $p \leq \sqrt{\log y}$.

Zunächst ist klar, dass für alle $p \leq \sqrt{\log y}$ gilt

$$f(t) \equiv 0 \mod p^2 \Leftrightarrow f(t+M_y) \equiv 0 \mod p^2 \quad .$$

Dies zeigt, dass in jeder solchen Menge gleich viele Werte n sind, die das Gewünschte erfüllen. Es genügt also die Menge $\{0, ..., M_y - 1\}$ zu betrachten. Für ein festes p ist die Anzahl der Elemente $0 \leq n \leq p^2-1$ mit $f(n) \not\equiv 0 \mod p^2$ genau $p^2-\omega(p)$. Nach dem chinesischen Restsatz sind also genau $\prod_{p\leq\sqrt{\log y}}(p^2-\omega(p))$ solcher Elemente in $\{0, ..., M_y - 1\}$ enthalten. Damit ist die Behauptung bewiesen.

Nun benötigen wir eine asymptotische Abschätzung über das Wachstum von M_y für $y \to \infty$. Aus dem Primzahlsatz, $\pi(z) \sim \frac{z}{\log z}$, erhalten wir sofort

$$\sum_{p\leq\sqrt{\log y}} \log p \leq \pi(\sqrt{\log y}) \log\sqrt{\log y} \sim \sqrt{\log y} \quad .$$

Mit dieser Abschätzung gilt

$$M_y = \prod_{p\leq\sqrt{\log y}} p^2 = \exp\left(\sum_{p\leq\sqrt{\log y}} \log p^2\right) = \exp\left(2\sum_{p\leq\sqrt{\log y}} \log p\right) = \exp(O(\sqrt{\log y})).$$

Damit ist M_y in $o(y)$, denn:

$$\frac{M_y}{y} = \frac{\exp(O(\sqrt{\log y}))}{y} = \exp\left(O(\sqrt{\log y}) - \log(y)\right) \longrightarrow 0 \quad .$$

Folglich ist $\left|\left\{0 \leq n \leq y \,\middle|\, f(n) \not\equiv 0 \mod p^2 \quad \forall p \leq \sqrt{\log y}\right\}\right|$

$$(1) \qquad = \left\lfloor \frac{y}{M_y} \right\rfloor \prod_{p \leq \sqrt{\log y}} (p^2 - \omega(p)) + O(M_y)$$

$$(2) \qquad = \left\lfloor \frac{y}{M_y} \right\rfloor M_y \prod_{p \leq \sqrt{\log y}} (1 - \frac{\omega(p)}{p^2}) + O(M_y)$$

$$(3) \qquad = y \prod_{p \leq \sqrt{\log y}} (1 - \frac{\omega(p)}{p^2}) + O(M_y)$$

$$(4) \qquad \sim c(f)y \quad .$$

Hierbei ist $c(f) := \prod_p c_p(f) > 0$, wie bereits gezeigt.
In (1) haben wir das betrachtete Intervall $[0, ..., y]$ in so viele disjunkte Intervalle mit M_y Elementen wie möglich unterteilt, da wir in obiger Behauptung gezeigt haben, dass in jedem solchen Intervall genau $\prod_{p \leq \sqrt{\log y}}(p^2 - \omega(p))$ Elemente mit der gewünschten Eigenschaft existieren. Nach Konstruktion haben wir also maximal M_y Elemente nicht beachtet, wodurch der $O(M_y)$-Term entsteht. Um die Gleichung (2) zu erhalten haben wir alle Primzahlquadrate aus dem Produkt gezogen, was nach Definition M_y ergibt. $\lfloor \frac{y}{M_y} \rfloor M_y$ lässt sich auch schreiben als $y - tM_y$ mit $0 \leq t < 1$. Da $-tM_y \prod_{p \leq \sqrt{\log y}}(1 - \frac{\omega(p)}{p^2}) + O(M_y)$ immer noch in $O(M_y)$ liegt, erhalten wir die Gleichung (3). $O(M_y)$ ist wie M_y ein $o(y)$-Term, spielt also für die Asymptotik keine Rolle. Nach Wahl von $c(f)$ gilt also auch (4). Fazit:

$$\left|\left\{0 \leq n \leq y \mid f(n) \not\equiv 0 \mod p^2 \quad \forall p \leq \sqrt{\log y}\right\}\right| \sim c(f)y \quad .$$

Kommen wir nun zu zwei weiteren Abschätzungen. Erstens gilt

$$\sum_{p \leq y} \omega(p) \overset{1.11}{\ll} d\pi(y) \ll \frac{y}{\log y} \ll \frac{y}{\sqrt{\log y}} \quad .$$

Nach Euler ist $\sum_{m \in \mathbb{N}} \frac{1}{m^2} = \frac{\pi^2}{6}$. Sei $z \in \mathbb{R}^+$ beliebig, dann ist

$$\sum_{m > z} \frac{1}{m^2} = \frac{1}{z^2} \sum_{m > z} \frac{z^2}{m^2} \quad .$$

Der erste Summand in der rechten Summe ist $\frac{z^2}{\lceil z \rceil^2} \leq 1$. Damit sind insbesondere die ersten $\lceil z \rceil$ Summanden kleiner als 1. Allgemein gilt

$$\frac{1}{n^2} \geq \frac{z^2}{(n\lceil z \rceil)^2} \geq \frac{z^2}{(n\lceil z \rceil + 1)^2} \geq \cdots \geq \frac{z^2}{((n+1)\lceil z \rceil - 1)^2} \quad .$$

Damit erhalten wir

$$\sum_{m>z} \frac{1}{m^2} \leq \frac{\lceil z \rceil}{z^2} \sum_{m \in \mathbb{N}} \frac{1}{m^2} \sim \frac{1}{z} \frac{\pi^2}{6}$$

und somit die zweite Abschätzung

$$\sum_{p>z} \frac{1}{p^2} < \sum_{m>z} \frac{1}{m^2} = O(\frac{1}{z}) \quad .$$

Die Anzahl der Elemente $0 \leq n \leq y$ für die $f(n)$ durch ein p^2 teilbar ist mit $\sqrt{\log y} < p \leq y$ ist nach oben beschränkt durch

$$\sum_{p>\sqrt{\log y}} \omega(p) \left\lfloor \frac{y}{p^2} \right\rfloor + \sum_{\sqrt{\log y}<p\leq y} \omega(p) \leq \left(\sum_{p>\sqrt{\log y}} \frac{\omega(p)}{p^2} \right) y + \sum_{p \leq y} \omega(p)$$

$$\overset{1.11}{\ll} \left(\sum_{p>\sqrt{\log y}} \frac{1}{p^2} \right) y + \sum_{p \leq y} \omega(p) \quad .$$

Dies ist nach obigen beiden Abschätzungen gerade gleich $O(\frac{y}{\sqrt{\log y}})$, also ein $o(y)$-Term. Da wir bereits gezeigt haben, dass eine positive Konstante $c(f)$ existiert, so dass $\left|\left\{0 \leq n \leq y \,\middle|\, f(n) \not\equiv 0 \mod p^2 \quad \forall p \leq \sqrt{\log y}\right\}\right| \sim c(f)y$ gilt, spielen diese Werte in unserer Abschätzung keine Rolle mehr. Das heißt,

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

$$= |\{0 \leq n \leq y | f(n) \not\equiv 0 \mod p^2 \quad \forall p \leq \sqrt{\log y}\}| - o(y) \sim c(f)y \quad .$$

Bis jetzt sind alle Ergebnisse unabhängig von Vermutungen. Doch um nun die Behauptung aus Erdös Vermutung 1.5 zu beweisen, müssen wir zeigen, dass die Anzahl der Elemente $n \in \mathbb{N}_0$ mit $p^2 \mid f(n)$ für ein $p > y$ ein $o(y)$-Term ist. Hierzu benutzen wir Korollar 1.3, also die Annahme, dass die *abc*-Vermutung stimmt.

Sei $\epsilon > 0$ beliebig. Dann ist zu zeigen, dass gilt

$$\delta := \limsup_{y \to \infty} \frac{|\{0 \leq n \leq y \mid f(n) \equiv 0 \mod p^2 \text{ für ein } p > y\}|}{y} < \epsilon \quad .$$

Wähle $m \in \mathbb{N}$ so, dass m größer ist als der Abstand von je zwei Nullstellen von $f(x)$ und $l \in \mathbb{N}$ so, dass $\frac{1}{l} < \epsilon$. Wir betrachten nun die Polynome

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

mit $0 \leq i \leq m-1$.
Da $f(x)$ keine mehrfache Nullstelle besitzt, gilt dies auch für alle $f(x+rm+i)$ und nach Wahl von m können $f(x+rm+i)$ und $f(x+r'm+i)$ auch keine gemeinsame Nullstelle besitzen für verschiedene $r, r' \in \mathbb{Z}$. Also haben auch alle Polynome $g_i(x)$ nur einfache Nullstellen. Somit können wir Korollar 1.3 auf $g_i(x)$ anwenden und erhalten für alle $n \in \mathbb{Z}$ mit $g_i(n) \neq 0$ die Abschätzung

$$|n|^{(l+1)d-1-\varepsilon} \ll \mathrm{rad}(g_i(n)) \quad .$$

Für jedes $n \in \mathbb{Z}$, das keine Nullstelle von $g_i(x)$ ist, existieren $u, v \in \mathbb{N}$, so dass $g_i(n) = \pm uv^2$ ist. Dann folgt mit obiger Abschätzung $|n|^{(l+1)d-1-\epsilon} \ll uv$. Hieraus erhalten wir mit dem Verhältnis $|g_i(n)| = uv^2 \sim |a_d|^{(l+1)}|n|^{(l+1)d}$, dass gilt

$$v \ll |n|^{1+\varepsilon} \quad .$$

Für hinreichend großes n kann $g_i(n)$ also maximal einen Teiler p^2 mit $p > n$ besitzen. Somit wird maximal einer der Faktoren $f(n+i), ..., f(n+lm+i)$ von einem solchen p^2 geteilt. Da wir nur endlich viele Polynome betrachten (genau m Stück) gilt für hinreichend großes $n_0 \in \mathbb{N}$:
Für $n > n_0$ sind höchstens m der Werte $f(n), ..., f(n+(l+1)m-1)$ durch ein p^2 mit $p > n$ teilbar. Da diese Aussage für alle $n > n_0$ gilt, erhalten wir ebenso, dass von den Elementen $f(n+k(l+1)m), ..., f(n+(k+1)(l+1)m)$ für beliebiges $k \in \mathbb{N}_0$ maximal m durch ein p^2 mit $p > n+k(l+1)m$ teilbar sind. Daher gilt

$$\delta \leq \frac{m}{(l+1)m} < \frac{1}{l} < \epsilon \quad .$$

Genauer haben wir gezeigt, dass mit Korollar 1.3 folgt, dass die Dichte der Menge $H := \{n > n_0 \mid f(n) \equiv 0 \mod p^2 \text{ für ein } p > n\}$ in $\mathbb{N}_0$ kleiner ist als ϵ. Da aber mit steigendem y die Menge $\{0 \leq n \leq y \mid 0 \neq f(n) \equiv 0 \mod p^2 \text{ für ein } p > y\}$ irgendwann in H enthalten ist und es maximal d Nullstellen von f in $\mathbb{N}_0$ gibt, gilt auch tatsächlich $\delta < \varepsilon$. □

Was wir innerhalb des Beweises ohne *abc*-Vermutung gezeigt haben, ist Folgendes:

Korollar 1.12. *Für jedes $f(x) \in \mathbb{Z}[x]$ gilt*

$$\left|\left\{0 \leq n \leq y \,\middle|\, f(n) \not\equiv 0 \mod p^2 \quad \forall p \leq y\right\}\right| \sim c(f)y$$

für eine positive Konstante $c(f) := \prod_p (1 - \frac{\omega(p)}{p^2})$.

Die Schwierigkeit in Erdös Vermutung liegt also darin, eine Abschätzung für die „großen“ Primzahlen zu finden.

Nun wollen wir Granvilles Theorem verallgemeinern, indem wir nicht mehr verlangen, dass die Werte $f(n), n \in \mathbb{Z}$, keinen fixierten quadratischen Teiler besitzen.

Granvilles Theorem (verallgemeinerte Version) 1.13. *Sei $f(x)$ ein quadratfreies Polynom aus $\mathbb{Z}[x]$, B der größte gemeinsame Teiler aller Werte $f(n), n \in \mathbb{Z}$. Sei B' der kleinste Teiler von B, für den $\frac{B}{B'}$ quadratfrei ist. Unter der Voraussetzung, dass die abc-Vermutung 1.1 allgemein gültig ist, folgt*

$$\left|\left\{0 \leq n \leq y \,\middle|\, \frac{f(n)}{B'} \text{ quadratfrei } \right\}\right| \sim c(f)y$$

für $c(f) > 0$ konstant.

Offensichtlich ist 1.6 ein Spezialfall hiervon mit $B' = 1$.

Beweis: Sei $B' := \prod_p p^{v_p}$. Definiere

$$\begin{aligned} \omega'(p) &:= \left|\left\{n \middle| \tfrac{f(n)}{B'} \equiv 0 \mod p^2 \,,\, 0 \leq n \leq p^{2+v_p} - 1\right\}\right| \\ &= \left|\left\{n \middle| f(n) \equiv 0 \mod p^{2+v_p} \,,\, 0 \leq n \leq p^{2+v_p} - 1\right\}\right| \quad . \end{aligned}$$

Falls p kein Teiler von B' ist, gilt also $\omega'(p) = \omega(p)$.

Für ein y mit $B' < \sqrt{\log y}$ gilt damit offensichtlich

$$\left|\left\{n \middle| \frac{f(n)}{B'} \equiv 0 \mod p^2 \text{ für ein } p > \sqrt{\log y}\right\}\right|$$

$$= \left|\left\{n \middle| f(n) \equiv 0 \mod p^2 \text{ für ein } p > \sqrt{\log y}\right\}\right| \quad .$$

In den Beweis von $|\{0 \leq n \leq y \mid f(n) \equiv 0 \mod p^2 \text{ für ein } p > \sqrt{\log y}\}| = o(y)$ ging nirgends ein, dass die Werte von $f(x)$ keinen fixierten quadratischen Teiler

besitzen. Wir haben lediglich benutzt, dass f keine mehrfachen Nullstellen hat. Diese Voraussetzung gilt allerdings auch an dieser Stelle. Es folgt sofort

$$\left|\left\{0 \le n \le y \middle| \frac{f(n)}{B'} \equiv 0 \mod p^2 \text{ für ein } p > \sqrt{\log y}\right\}\right|$$

$$= \left|\left\{0 \le n \le y \middle| f(n) \equiv 0 \mod p^2 \text{ für ein } p > \sqrt{\log y}\right\}\right| = o(y) \quad .$$

Es genügt also zu zeigen, dass

$$\left|\left\{0 \le n \le y \,\middle|\, \frac{f(n)}{B'} \not\equiv 0 \mod p^2 \quad \forall p \le \sqrt{\log y}\right\}\right| \sim c(f)y$$

gilt. Die Vorgehensweise ist analog zum Fall $B' = 1$.

Sei $M'_y := \prod_{p \le \sqrt{\log y}} p^{2+v_p}$ und wie vorher $M_y := \prod_{p \le \sqrt{\log y}} p^2$.

Analog zum Beweis von 1.6 folgt aus dem chinesischen Restsatz, dass für jedes $t \in \mathbb{Z}$ in jeder Menge $\{t, t+1, ..., t+M'_y-1\}$ genau $\prod_{p \le \sqrt{\log y}} p^{2+v_p} - \omega'(p)$ viele Elemente n existieren, mit $f(n) \not\equiv 0 \mod p^{2+v_p}$ für alle $p \le \sqrt{\log y}$.

Die Anzahl der Elemente $0 \le n \le y$ mit $\frac{f(n)}{B'} \not\equiv 0 \mod p^2$ für alle $p \le \sqrt{\log y}$ ist also gleich

$$\left\lfloor \frac{y}{M'_y} \right\rfloor \prod_{p \le \sqrt{\log y}} (p^{2+v_p} - \omega'(p)) + O(M'_y) = \left\lfloor \frac{y}{M'_y} \right\rfloor M'_y \prod_{p \le \sqrt{\log y}} (1 - \frac{\omega'(p)}{p^{2+v_p}}) + O(M'_y) \quad .$$

Es ist klar, dass $M'_y = B'M_y = o(y)$ gilt, wie bereits gezeigt. Um den Beweis zu beenden, müssen wir also zeigen, dass gilt

$$c(f) := \prod_{p \le \sqrt{\log y}} (1 - \frac{\omega'(p)}{p^{2+v_p}}) > 0 \quad .$$

Angenommen es wäre $1 - \frac{\omega'(p)}{p^{2+v_p}} = 0$ für ein p . Dann wäre $\omega'(p) = p^{2+v_p}$, also würde für alle $0 \le n \le p^{2+v_p} - 1$ die Kongruenz $f(n) \equiv 0 \mod p^{2+v_p}$ gelten. Damit wäre p^{2+v_p} ein fixierter Teiler der Werte von f, also ein Teiler von B. Nach Definition von v_p gilt dann aber $p^2 \mid \frac{B}{B'}$ im Widerspruch zur Wahl von B'.
Sei $s > \max\{B', \sqrt{d}, \Delta f\}$, dann gilt

$$c(f) \ge \prod_{p \le s} (1 - \frac{\omega'(p)}{p^{2+v_p}}) \prod_{p > s} (1 - \frac{d}{p^2}) \quad ,$$

denn für ein $p > B'$ ist $\omega(p) = \omega'(p)$. Falls weiter $p > \Delta f$ ist, gilt $d \ge \omega(p) = \omega'(p)$. Der Faktor $\sqrt{d}$ stellt sicher, dass für ein $p > s$ auch tatsächlich $\frac{d}{p^2} < 1$ gilt. Das

erste Produkt ist endlich und das zweite größer als $\prod_{m\in\mathbb{N},m^2>d}(1-\frac{d}{m^2})>0$. Damit erhalten wir

$$c(f) \geq \prod_{p\leq s}(1-\frac{\omega'(p)}{p^{2+v_p}})\prod_{p>s}(1-\frac{d}{p^2})>0 \quad .$$

Also ist auch die verallgemeinerte Version von 1.6 bewiesen. □

2 Erdös Vermutung für grad(f) ≤ 2

In diesem Kapitel sei f stets ein quadratfreies Polynom aus $\mathbb{Z}[x]$, dessen Werte keinen fixierten quadratischen Teiler besitzen und d der Grad von f. Wir wollen Erdös Vermutung in Spezialfällen betrachten, ohne uns auf die *abc*-Vermutung zu stützen. Wir werden Folgendes beweisen:

Satz 2.1. *Falls* $d := \text{grad}(f) \in \{1, 2\}$, *dann gilt*

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

für eine positive Konstante $c(f) := \prod_p (1 - \frac{\omega(p)}{p^2})$.

Für die Bedeutung von $\omega(p)$ siehe Definition 1.7.

In Korollar 1.12 haben wir gezeigt, dass sich die Menge der Zahlen $n \in \mathbb{N}_0$ mit $n \leq y$, für die $f(n) \not\equiv 0 \mod p^2$ für alle $p \leq y$, verhält wie $c(f)y$. Um nun Satz 2.1 zu beweisen wollen wir also zeigen, dass die Menge der Zahlen $0 \leq n \leq y$, für die $f(n)$ durch ein p^2 teilbar ist, mit $p > y$ „klein“ ist. Genauer müssen wir zeigen, dass gilt

$$\left|\left\{0 \leq n \leq y \,\middle|\, f(n) \equiv 0 \mod p^2 \text{ für ein } p > y\right\}\right| = o(y) \quad .$$

Lemma 2.2. *Unter den gegebenen Voraussetzungen an* f *gilt*

$$\left|\left\{0 \leq n \leq y \,\middle|\, f(n) \equiv 0 \mod p^2 \textit{ für ein } p > y\right\}\right| \ll d \sum_{y < p \leq \sqrt{|f(y)|}} 1 \quad .$$

Beweis: Da $f(x)$ ein Polynom ist, existiert ein $x_0 \in \mathbb{R}$, sodass $|f(x)|$ streng monoton steigt für $x \geq x_0$. Sei $p > y$ und $n > x_0$ mit $f(n) \equiv 0 \mod p^2$. Dann ist p kleiner als $\sqrt{|f(y)|}$. Denn:
Da n echt größer ist als x_0, ist $f(n) \neq 0$ und somit folgt aus $f(n) \equiv 0 \mod p^2$, dass $p^2 \leq |f(n)|$. Nun ist $n \leq y$. Da $n > x_0$, ist auch $p^2 \leq |f(n)| \leq |f(y)|$, woraus unmittelbar $p \leq \sqrt{|f(y)|}$ folgt. Weiter ist jedes n mit $0 \neq f(n) \equiv 0 \mod p^2$ für ein $p > y$ für hinreichend großes y stets größer als x_0.
Wir können also zusammenfassen, dass für hinreichend großes y jedes $p > y$ mit $0 \neq f(n) \equiv 0 \mod p^2$ für ein $n \leq y$ beschränkt ist durch $\sqrt{|f(y)|}$.
Nach Definition existieren für $p > y$ in jeder Menge $\{0, 1, ..., \lfloor y \rfloor\}$ maximal $\omega(p)$ Elemente n, sodass p^2 ein Teiler von $f(n)$ ist. Nach Satz 1.11 ist $\omega(p) \leq d$ für

$p > y > \Delta f$. Da es weiter maximal d Nullstellen von f aus $\mathbb{N}_0$ gibt, erhalten wir folgende Abschätzung:

$$\begin{aligned}
&\left|\left\{0 \le n \le y \,\middle|\, f(n) \equiv 0 \mod p^2 \text{ für ein } p > y\right\}\right| \\
&\ll \left|\left\{0 \le n \le y \,\middle|\, 0 \neq f(n) \equiv 0 \mod p^2 \text{ für ein } p > y\right\}\right| \\
&\le \sum_{y<p\le\sqrt{|f(y)|}} \omega(p) \overset{1.11}{\ll} d \sum_{y<p\le\sqrt{|f(y)|}} 1 \quad .
\end{aligned}$$

Diese Abschätzung ergibt sich dadurch, dass wir annehmen, dass alle Lösungen der Kongruenzen $f(n) \equiv 0 \mod p^2$ kleiner sind als y und alle paarweise verschieden. Hierbei betrachten wir alle „möglichen“ Kongruenzen, d.h. diejenigen mit $p > y$ nach Voraussetzung und $p \le \sqrt{|f(y)|}$ nach unseren Vorüberlegungen. □

Diese Abschätzung ist sehr ungenau und wir werden zeigen, dass sie für $d \ge 3$ nicht mehr anwendbar ist, um Erdös Vermutung zu beweisen.

Satz 2.3. *Es gilt genau dann* $d \sum_{y<p\le\sqrt{|f(y)|}} 1 = o(y)$, *wenn* $d \in \{1, 2\}$.

Beweis: Da d nur ein konstanter Faktor ist, ändert es nichts an einer o-Abschätzung der Summe. Zu zeigen ist also

$$\sum_{y<p\le\sqrt{|f(y)|}} 1 = \pi\left(\sqrt{|f(y)|}\right) - \pi(y) = o(y) \Leftrightarrow d \le 2 \quad .$$

Mit dem Primzahlsatz ist $\pi(y) \sim \frac{y}{\log y} = o(y)$. Es bleibt also nur noch

$$\pi\left(\sqrt{|f(y)|}\right) = o(y) \Leftrightarrow d \le 2$$

zu zeigen. Wie immer schreiben wir $f(x) = a_d x^d + ... + a_0$. Es ist klar, dass gilt $\sqrt{|f(x)|} \sim \sqrt{|a_d|} x^{d/2}$. Was wir nun zeigen möchten ist, dass damit auch gilt $\log(\sqrt{|f(x)|}) \sim \log(\sqrt{|a_d|} x^{d/2})$. Hierzu überlegen wir uns zunächst, dass gilt

$$\frac{|f'(x)|}{|f(x)|} \sim dx^{-1} \quad .$$

Weiter rechnet man nach, dass die Ableitung von $\log(\sqrt{|f(x)|})$ gleich $\frac{|f'(x)|}{2|f(x)|} \sim \frac{d}{2} x^{-1}$ nach obiger Überlegung ist. Die Ableitung von $\log(\sqrt{|a_d|} x^{d/2})$ ist genau gleich $\frac{d}{2} x^{-1}$. Nach diesen Überlegungen erhalten wir durch Anwendung des Satzes von l'Hospital

$$\lim_{x\to\infty} \frac{\log(\sqrt{|f(x)|})}{\log(\sqrt{|a_d|} x^{d/2})} = 1 \quad .$$

Also haben wir gezeigt, dass gilt

$$\log\left(|f(x)|\right) \sim \log\left(\sqrt{|a_d|}x^{d/2}\right) \quad .$$

Damit erhalten wir sofort

$$\pi\left(\sqrt{|f(x)|}\right) \sim \frac{\sqrt{|f(x)|}}{\log(\sqrt{|f(x)|})} \sim \frac{\sqrt{|a_d|}x^{d/2}}{\log(\sqrt{|a_d|}x^{d/2})} \sim \pi\left(\sqrt{|a_d|}x^{d/2}\right) \quad .$$

$\pi\left(\sqrt{|a_d|}y^{d/2}\right) \sim \frac{\sqrt{|a_d|}y^{d/2}}{\log(\sqrt{|a_d|}y^{d/2})}$ ist aber genau dann ein $o(y)$-Term, wenn $\frac{d}{2} \leq 1$ ist, also genau dann, wenn $d \in \{1, 2\}$. □

Der Beweis von Satz 2.1 ist nun eine einfache Zusammenführung der letzten Resultate.

Beweis von 2.1: Sei $d \in \{1, 2\}$. Nach Korollar 1.12 existiert eine positive Konstante $c(f)$, mit der gilt

$$\left|\left\{0 \leq n \leq y \,\middle|\, f(n) \not\equiv 0 \mod p^2 \quad \forall p \leq y\right\}\right| \sim c(f)y \quad .$$

Also genügt es zu zeigen, dass $|\{0 \leq n \leq y \mid f(n) \equiv 0 \mod p^2 \text{ für ein } p > y\}| = o(y)$ gilt. Dies erhalten wir gerade durch Lemma 2.2 und Satz 2.3. Denn

$$|\{0 \leq n \leq y \mid f(n) \equiv 0 \mod p^2 \text{ für ein } p > y\}| \overset{2.2}{\ll} d \sum_{y < p \leq \sqrt{|f(y)|}} 1 \overset{2.3}{=} o(y) \quad .$$

□

Wir haben jetzt zwar Satz 2.1 bewiesen, allerdings haben wir in Satz 2.3 auch gezeigt, dass sich unser Beweis nicht auf Polynome höheren Grades übertragen lässt.
Sei $m \in \mathbb{N}$. Wir bezeichnen für den Moment eine Zahl n als m-frei, wenn in der Primfaktorzerlegung von n jeder Exponent echt kleiner als m ist. Hooley bewies in [Ho] folgenden Satz:

Satz 2.4. *Sei $f(x) \in \mathbb{Z}[x]$ und $d = \text{grad}(f)$. Weiter existiere kein fixierter Teiler der Werte von f mit Exponent $d-1$. Falls $d \geq 3$, so gilt*

$$|\{0 \leq n \leq y \,|\, f(n) \text{ ist } (d-1)\text{-frei}\}| = Ay + O\left(\frac{y}{\log^{2/3} y}\right)$$

für ein $A > 0$.

Der Fall $d = 3$ in Satz 2.4 beweist also Erdös Vermutung für $d = 3$. Allerdings kann man bereits an der Aussage des Satzes erkennen, dass sich auch dieser Beweis nicht auf Polynome höheren Grades erweitern lässt.

Wenn man Erdös Vermutung nur für irreduzible Polynome betrachtet, sind die bewiesenen Fälle ($d = \text{grad}(f) \leq 3$) genau diejenigen, in denen man nicht voraussetzen muss, dass f keinen fixierten quadratischen Teiler besitzt. Denn nach Satz 1.4 kann ein solcher Teiler für $d \leq 3$ nicht existieren.

Beispiel 2.5. Wir wollen nun die Konstante $c(f)$ aus Erdös Vermutung explizit berechnen für alle Polynome $f(x) = a_1x + a_0$ aus $\mathbb{Z}[x]$ mit $\text{ggT}(a_1, a_0) = 1$, also für lineare Polynome leeren Inhaltes. Der wichtigste Schritt hierbei ist die Bestimmung von $\omega(p)$. Für ein p mit $p \nmid a_1$ ist die Kongruenz $a_1n + a_0 \equiv 0 \mod p^2$ eindeutig lösbar. Falls p ein Teiler von a_1 ist, kann die Kongruenz $a_1n + a_0 \equiv 0 \mod p^2$ nur dann erfüllt sein, wenn p auch a_0 teilt. Dies wurde aber nach Wahl von f ausgeschlossen. Also ist $\omega(p)$ bestimmt durch

$$\omega(p) = \begin{cases} 1 & \text{für} \quad p \nmid a_1 \\ 0 & \text{für} \quad p \mid a_1 \end{cases} .$$

Damit folgt aus Satz 2.1 und der Konstruktion von $c(f)$

$$|\{0 \leq n \leq y \,|\, f(n) \text{ quadratfrei } \}| \sim \prod_{p \nmid a_1} (1 - \frac{1}{p^2})y = \prod_{p} (1 - \frac{1}{p^2}) \prod_{p \mid a_1} (1 - \frac{1}{p^2})^{-1} y$$

$$= \left(\sum_{m \in \mathbb{N}} \frac{1}{m^2} \right)^{-1} \prod_{p \mid a_1} \frac{p^2}{p^2 - 1} y = \frac{6}{\pi^2} \prod_{p \mid a_1} \frac{p^2}{p^2 - 1} y \quad .$$

Für die hierbei verwendete bekannte Gleichung $\prod_p (1 - \frac{1}{p^2}) = \left(\sum_{m \in \mathbb{N}} \frac{1}{m^2} \right)^{-1}$ verweisen wir auf [Bru] Gleichung (1.3).

3 Granvilles Theorem für beliebige Zahlkörper

In Theorem 1.6 haben wir unter Voraussetzung der *abc*-Vermutung bewiesen, dass die Dichte quadratfreier Werte von gewissen Polynomen aus $\mathbb{Z}[x]$ positiv ist. Dieses Resultat wollen wir auf beliebige Zahlkörper verallgemeinern. Sei K ein beliebiger Zahlkörper vom Grad n und $\mathfrak{o}_K$ der Ring der ganz-algebraischen Zahlen in K. Da $\mathfrak{o}_{\mathbb{Q}} = \mathbb{Z}$ ist, werden wir also Polynome aus $\mathfrak{o}_K[x]$ betrachten. In $\mathfrak{o}_K$ können wir keine eindeutige Primfaktorzerlegung mehr voraussetzen. Daher benötigen wir einen anderen Begriff von quadratfrei als bisher. Allerdings ist $\mathfrak{o}_K$ ein Dedekind-Ring (siehe z.B. [Ne], I.3.1) und somit ist bis auf $\{0\}$ und $\mathfrak{o}_K$ jedes Ideal eindeutig (bis auf Reihenfolge) als Produkt von endlich vielen Primidealen zerlegbar (siehe [Ne], I.3.3). Damit können wir auch von Teilbarkeit bei Idealen sprechen. Für zwei Ideale I und J in $\mathfrak{o}_K$ schreiben wir $I \mid J$ genau dann wenn ein Ideal I' existiert mit $II' = J$. Zur Vereinfachung benutzen wir folgenden Satz:

Satz 3.1. *Seien I, J Ideale aus $\mathfrak{o}_K$, dann gilt*

$$I \mid J \Leftrightarrow J \subseteq I \quad .$$

Beweis: Siehe [JS] X §2 Korollar 3.6 a) □

Dies führt uns auf den allgemeineren Begriff von quadratfrei.

Definition 3.2. *Ein Element $a \in \mathfrak{o}_K$ heißt quadratfrei, wenn es kein Primideal $P \lhd \mathfrak{o}_K$ gibt, so dass $a \in P^2$.*

Nach Satz 3.1 ist dies äquivalent dazu, dass alle Exponenten in der Primidealzerlegung vom Hauptideal $a\mathfrak{o}_K$ gleich 1 sind ($a \in P^2 \Leftrightarrow a\mathfrak{o}_K \subseteq P^2$).
Da im Spezialfall $K = \mathbb{Q}$ jedes von $\{0\}$ verschiedene Primideal in $\mathfrak{o}_K = \mathbb{Z}$ eindeutig durch sein erzeugendes Primelement bestimmt ist, stimmt die Definition von quadratfrei über $\mathbb{Z}$ mit Definition 3.2 überein.

$\mathfrak{o}_K$ besitzt eine n-elementige $\mathbb{Z}$-Basis $W := \{w_1, ..., w_n\}$. Weiter existieren genau n verschiedene $\mathbb{Q}$-Einbettungen von K in einen algebraischen Abschluss von K.

Definition und Satz 3.3. *Seien $\sigma_1, ..., \sigma_n$ die verschiedenen Einbettungen von K. Als Diskriminante von K definieren wir*

$$\Delta_K := \det(\sigma_i(w_j))^2 \in K \backslash \{0\} \quad .$$

Diese Definition ist unabhängig von der Wahl der Basis.

Beweis: Wir werden an dieser Stelle lediglich zeigen, dass diese Definition tatsächlich unabhängig von der Wahl der Basis ist. Für den Beweis, dass die Diskriminante stets aus $K\backslash\{0\}$ ist, siehe [La], III §3 Proposition 9.
Sei also $V := \{v_1, ..., v_n\}$ eine weitere $\mathbb{Z}$-Basis von $\mathfrak{o}_K$ und A die Basiswechselmatrix von W nach V. Dann gilt $A \in GL_n(\mathbb{Z})$, also $\det(A) = \pm 1$. Wie in der Definition setzen wir $\Delta_K := \det(\sigma_i(w_j))^2$. Es ist

$$\det(\sigma_i(v_j))^2 = \det\left(\sigma_i\left(\sum_{k=1}^{n} a_{jk}w_k\right)\right)^2 = \det\left(\sum_{k=1}^{n} a_{jk}\sigma_i(w_k)\right)^2 = \det(A(\sigma_i(w_k)))^2 \quad .$$

Also gilt

$$\det(\sigma_i(v_j))^2 = \det(A)^2\Delta_K = \Delta_K \quad .$$

Damit ist die Wahl der Basis nicht entscheidend für den Wert der Diskriminante. □

Eine Einbettung σ von K heißt *reell*, falls $\sigma(K) \subset \mathbb{R}$ gilt und *komplex*, falls nicht. Für jede komplexe Einbettung σ ist auch $\overline{\sigma}$ eine Einbettung. Wir werden die Einbettungen ab jetzt wie folgt nummerieren:

$$\sigma_1, ..., \sigma_r, \sigma_{r+1}, ..., \sigma_{r+s} \quad .$$

Hierbei sind $\sigma_1, ..., \sigma_r$ alle reellen Einbettungen und $\sigma_{r+1}, ..., \sigma_{r+s}$ seien die verschiedenen paarweise nicht zueinander konjugierten komplexen Einbettungen (sie sind nicht eindeutig bestimmt). Es gilt also $n = r + 2s$. Sei $\varphi : \mathfrak{o}_K \to \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$ die geometrische Abbildung definiert durch

$$\varphi(a) := (\sigma_1(a), ..., \sigma_r(a), \sigma_{r+1}(a), ..., \sigma_{r+s}(a)) \quad .$$

φ ist ein injektiver $\mathbb{Z}$-Modulhomomorphismus, da dies auch für alle Einbettungen gilt. Wir können also $\mathfrak{o}_K$ durch $\varphi(\mathfrak{o}_K)$ als Untergruppe von $\mathbb{R}^n$ auffassen.

Satz 3.4. *$\varphi(\mathfrak{o}_K)$ ist ein Gitter im $\mathbb{R}^n$.*

Beweis: Sei wieder $W := \{w_1, ..., w_n\}$ eine $\mathbb{Z}$-Basis von $\mathfrak{o}_K$. Dann gilt

$$\varphi(\mathfrak{o}_K) = \varphi(\mathbb{Z}w_1 + ... + \mathbb{Z}w_n) = \mathbb{Z}\varphi(w_1) + ... + \mathbb{Z}\varphi(w_n) \quad .$$

Es bleibt also zu zeigen, dass $\varphi(w_1), ..., \varphi(w_n)$ $\mathbb{R}$-linear unabhängig sind. In $\mathbb{R}^n$ fassen wir $\varphi(w_k)$ auf als

$$(\sigma_1(w_k), ..., \sigma_r(w_k), \mathrm{Re}(\sigma_{r+1}(w_k)), \mathrm{Im}(\sigma_{r+1}(w_k)), ..., \mathrm{Re}(\sigma_{r+s}(w_k)), \mathrm{Im}(\sigma_{r+s}(w_k))) \quad .$$

Durch elementare Spaltenumformungen erhalten wir

$$\Delta_K = \det \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_r(w_1) & \sigma_{r+1}(w_1) & \overline{\sigma_{r+1}(w_1)} & \cdots & \sigma_{r+s}(w_1) & \overline{\sigma_{r+s}(w_1)} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_r(w_n) & \sigma_{r+1}(w_n) & \overline{\sigma_{r+1}(w_n)} & \cdots & \sigma_{r+s}(w_n) & \overline{\sigma_{r+s}(w_n)} \end{pmatrix}$$

$$= (-2i)^s \det \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_r(w_1) & \mathrm{Re}(\sigma_{r+1}(w_1)) & \mathrm{Im}(\sigma_{r+1}(w_1)) & \cdots & \mathrm{Re}(\sigma_{r+s}(w_1)) & \mathrm{Im}(\sigma_{r+s}(w_1)) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_r(w_n) & \mathrm{Re}(\sigma_{r+1}(w_n)) & \mathrm{Im}(\sigma_{r+1}(w_n)) & \cdots & \mathrm{Re}(\sigma_{r+s}(w_n)) & \mathrm{Im}(\sigma_{r+s}(w_n)) \end{pmatrix}$$

Also ist der Betrag der Determinante der Matrix $(\varphi(w_1), ..., \varphi(w_n))$ gleich $2^{-s}\sqrt{|\Delta_K|}$. Da die Diskriminante eines Zahlkörpers nach 3.3 stets ungleich Null ist, folgt, dass auch die berechnete Determinante ungleich Null ist. Somit sind $\varphi(w_1), ..., \varphi(w_n)$ linear unabhängig über $\mathbb{R}$, also ist $\varphi(\mathfrak{o}_K)$ ein Gitter im $\mathbb{R}^n$. □

Mit diesen Vorüberlegungen können wir bereits eine erste Verallgemeinerung von Korollar 1.12 formulieren.

Satz 3.5. *Sei $f(x) \in \mathfrak{o}_K[x]$ ein quadratfreies Polynom vom Grad d. Weiter existiere kein Primideal $P \lhd \mathfrak{o}_K$ so, dass $f(a) \in P^2$ für alle $a \in \mathfrak{o}_K$. Dann folgt*

$$|\{a \in \mathfrak{o}_K \mid \|\varphi(a)\|_\infty \leq y, f(a) \notin P^2 \quad \forall P \lhd \mathfrak{o}_K \text{ mit } N(P) \leq y\}| \sim c(f,K)y^n$$

für $c(f,K) > 0$ konstant.

$\|.\|_\infty$ bezeichnet die Maximumsnorm auf $\mathbb{R}^n$. Es ist also

$$\|\varphi(a)\|_\infty = \max\{|\sigma_1(a)|, ..., |\sigma_r(a)|, |\,\mathrm{Re}(\sigma_{r+1}(a))|, |\,\mathrm{Im}(\sigma_{r+1}(a))|, ..., |\,\mathrm{Im}(\sigma_{r+s}(a))|\}$$

für alle $a \in \mathfrak{o}_K$. Die Wahl dieser Norm auf $\mathbb{R}^n$ hat rein praktische Zwecke, wie am Schluss dieser Arbeit noch genauer erklärt wird.

Da $\mathfrak{o}_K$ ein Dedekind-Ring ist, ist jedes von $\{0\}$ verschiedene Primideal P auch ein Maximalideal. Damit ist also $N(P) = |\mathfrak{o}_K/P| = p^k$ für ein $k \in \mathbb{N}$. Um in 3.3 die Diskriminante eines Zahlkörpers zu definieren haben wir bemerkt, dass $\mathfrak{o}_K$ ein $\mathbb{Z}$-Modul vom Rang n ist. Damit gilt

$$N(p\mathfrak{o}_K) = |\mathfrak{o}_K/p\mathfrak{o}_K| = |\mathbb{Z}^n/p\mathbb{Z}^n| = |\mathbb{Z}/p\mathbb{Z}|^n = p^n \quad .$$

Sei P ein Primideal mit $\mathrm{char}(\mathfrak{o}_K/P) = p$, dann ist $[p] = [0]$ in $\mathfrak{o}_K/P$ und somit $p \in P$. Damit ist auch $p\mathfrak{o}_K \subseteq P$ und nach Satz 3.1 kommt P in der Primidealzerlegung von $p\mathfrak{o}_K$ vor. Aufgrund der Multiplikativität der Norm gilt für jedes P aus

der Primidealzerlegung von $p\mathfrak{o}_K$ allerdings auch $N(P) \mid N(p\mathfrak{o}_K) = p^n$. Damit haben wir gezeigt:
Ein Primideal P kommt genau dann in der Primidealzerlegung von $p\mathfrak{o}_K$ vor, wenn $N(P) = p^k$ für ein $k \in \mathbb{N}$ gilt.

Seien nun $P_1, ..., P_r$ alle Primideale in $\mathfrak{o}_K$ mit $N(P_i) = p^{f_i}$ für ein $f_i \in \mathbb{N}$. Dann hat P die Primidealzerlegung $P = \prod_{i=1}^{r} P_i^{e_i}$ für gewisse $e_i \in \mathbb{N}$. Damit gilt

$$p^n = N(p\mathfrak{o}_K) = N(P_1)^{e_1} \cdots N(P_r)^{e_r}$$

und wir erhalten sofort $n = \sum_{i=1}^{r} e_i f_i$.
Da sowohl e_i als auch f_i stets größer oder gleich 1 sind, kann es für festes p maximal n Primideale P geben mit $p = \text{char}(\mathfrak{o}_K/P)$. Für eine beliebige Schranke $z \in \mathbb{R}$ erhalten wir somit, dass die Anzahl von Primidealen $P \lhd \mathfrak{o}_K$ mit $\text{char}(\mathfrak{o}_K/P) \leq z$ nach oben beschränkt ist durch $n\pi(z)$.

Wir fassen die wichtigsten Resultate im folgenden Satz zusammen:

Satz 3.6. *Mit den Bezeichnungen von oben gilt:*
a) $n = \sum_{i=1}^{r} e_i f_i$.
b) *Für beliebiges* $z \in \mathbb{R}$ *ist* $|\{P \lhd \mathfrak{o}_K \,|\text{char}(\mathfrak{o}_K/P) \leq z\}| \leq n\pi(z)$.

Wir können $f \in \mathfrak{o}_K[x]$ kanonisch auffassen als Polynom über einem beliebigen Faktorring von $\mathfrak{o}_K$. Dies ermöglicht uns auch Restklassen in f einzusetzen. Unter den Voraussetzungen von Satz 3.5 beweisen wir die folgenden beiden Resultate ähnlich wie in Kapitel 1:

Lemma 3.7. *Sei* $\omega(P) := |\{a \in \mathfrak{o}_K/P^2 \mid f(a) \equiv 0 \mod P^2\}|$ *eine Verallgemeinerung von Definition 1.7. Dann gilt für jedes Primideal* $P \lhd \mathfrak{o}_K$ *mit* $\Delta f \notin P$

$$\omega(P) \leq d \quad .$$

Lemma 3.8.

$$0 < \prod_{P \lhd \mathfrak{o}_K} (1 - \frac{\omega(P)}{N(P)^2}) =: c(f)$$

Beweis von 3.7: Zunächst folgt mit Satz 1.10 aus $\Delta f \notin P$, dass $\Delta\overline{f} \neq 0$ in $\mathfrak{o}_K/P$ ist, wobei $\overline{\cdot}$ wieder die Reduktion modulo P beschreibt. Also besitzt f keine mehrfachen Nullstellen in $\mathfrak{o}_K/P$ für $\Delta f \notin P$. Sei $\mathfrak{o}_K/P = \{\alpha_1, ..., \alpha_{N(P)}\}$.

Behauptung: Es existieren Elemente $x_1, ..., x_{N(P)} \in P$ so, dass gilt

$$\mathfrak{o}_K/P^2 = \{\alpha_1 + x_1, ..., \alpha_1 + x_{N(P)}, \alpha_2 + x_1, ..., \alpha_{N(P)} + x_{N(P)}\} \quad .$$

Da beide Seiten gleiche Kardinalität besitzen, genügt es zu zeigen, dass alle Restklassen der rechten Seite verschieden sind. Sei $\alpha_i + x_j \equiv \alpha_k + x_l \mod P^2$. Dann ist erst recht $\alpha_i - \alpha_k \equiv x_l - x_j \equiv 0 \mod P$. Also muss $i = k$ gelten. Wir erhalten also die Kongruenz $x_l \equiv x_j \mod P^2$.
Wir wählen nun $x_1, ..., x_{N(P)}$ so, dass stets gilt $x_j \not\equiv x_l \mod P^2$ für $l \neq j$. Dies ist möglich, da $|P/P^2| = |\mathfrak{o}_K/P| = N(P)$ (siehe z.B. [Ko], Lemma 3.5.2). Mit der Voraussetzung $x_j \not\equiv x_l \mod P^2$ für $j \neq l$ sind also alle Restklassen verschieden und es gilt

$$\mathfrak{o}_K/P^2 = \{\alpha_1 + x_1, ..., \alpha_1 + x_{N(P)}, \alpha_2 + x_1, ..., \alpha_{N(P)} + x_{N(P)}\} \quad .$$

Es ist klar, dass für $f(\alpha_i + x_j) \equiv 0 \mod P^2$ auch gilt $f(\alpha_i) \equiv 0 \mod P$.
Betrachte die Kongruenz $f(x) \equiv 0 \mod P$. Sei α_i eine Lösung dieser Kongruenz. Wir wollen zeigen, dass für maximal ein k die Kongruenz $f(\alpha_i + x_k) \equiv 0 \mod P^2$ erfüllt ist. Wie im Beweis von Satz 1.11 erhalten wir durch Ausmultiplizieren

$$f(\alpha_i + x_k) \equiv f(\alpha_i) + x_k f'(\alpha_i) \mod P^2 \quad .$$

Damit gelten die Äquivalenzen

$$\begin{aligned} & f(\alpha_i + x_k) \equiv f(\alpha_i + x_j) \mod P^2 \\ \Leftrightarrow \quad & f(\alpha_i) + x_k f'(\alpha_i) \equiv f(\alpha_i) + x_j f'(\alpha_i) \mod P^2 \\ \Leftrightarrow \quad & (x_k - x_j) f'(\alpha_i) \equiv 0 \mod P^2 \quad . \end{aligned}$$

Da f keine doppelte Nullstelle modulo P besitzt, ist $f'(\alpha_i)$ nicht in P enthalten und somit ist $x_k \equiv x_j \mod P^2$, also nach Voraussetzung $k = j$.
Wir haben nun gezeigt, dass ein $\alpha_i + x_j$ nur dann Nullstelle von f modulo P^2 sein kann, wenn α_i Nullstelle von f modulo P ist, und dass es in der Menge $\{\alpha_i + x_1, ..., \alpha_i + x_{N(P)}\}$ maximal eine Nullstelle von f modulo P^2 geben kann. Dies ist gleichbedeutend damit, dass f maximal so viele Nullstellen in $\mathfrak{o}_K/P^2$ besitzt wie Nullstellen in $\mathfrak{o}_K/P$. Allerdings ist $\mathfrak{o}_K/P$ ein Körper, weshalb die Anzahl

der Nullstellen von f in $\mathfrak{o}_K/P$ durch d beschränkt ist. □

Beweis von 3.8: Wir beweisen dieses Lemma in zwei Schritten.

Schritt 1: Sei $p \geq \sqrt{d}+1$ und $P_1, ..., P_r$ alle Primideale mit $\text{char}(\mathfrak{o}_K/P_i) = p$. Dann gilt

$$\prod_{i=1}^{r}(1-\frac{d}{N(P_i)^2}) \geq \left(1-\frac{d}{p^2}\right)^n \quad .$$

Wir zeigen zunächst, dass $\left(1-\frac{d}{(p^k)^2}\right) \geq \left(1-\frac{d}{p^2}\right)^k$ gilt. Es ist

$$\left(1-\frac{d}{(p^k)^2}\right) \geq \left(1-\frac{d}{p^2}\right)^k \Leftrightarrow \frac{p^{2k}-d}{p^{2k}} \geq \frac{(p^2-d)^k}{p^{2k}} \Leftrightarrow p^{2k} \geq \left(p^2-d\right)^k + d \; .$$

Betrachten wir beide Seiten der letzten Ungleichung als Polynome in p, so ist klar, dass für beliebiges $k \in \mathbb{N}$ die linke Seite schneller wächst als die rechte. Da die Ungleichungen für $p = \sqrt{d+1} < \sqrt{d}+1$ erfüllt sind, gelten sie somit für jedes $p \geq \sqrt{d}+1$. Damit können wir Schritt 2 schnell beenden, denn

$$\prod_{i=1}^{r}(1-\frac{d}{N(P_i)^2}) = \prod_{i=1}^{r}(1-\frac{d}{(p^{f_i})^2}) \geq \prod_{i=1}^{r}(1-\frac{d}{p^2})^{f_i} \quad .$$

Da $\sum_{i=1}^{r} f_i \leq n$ ist (folgt aus Satz 3.6 a)), haben wir Schritt 1 gezeigt.

Schritt 2: Beweisende

Für jedes $P \lhd \mathfrak{o}_K$ gilt $1-\frac{\omega(P)}{N(P)^2} \neq 0$. Sonst wäre nämlich $\omega(P) = N(P^2)$, was bedeuten würde, dass für jedes $a \in \mathfrak{o}_K/P$ die Kongruenz $f(a) \equiv 0 \mod P^2$ gelten würde. Das heißt, $f(a) \in P^2$ für jedes $a \in \mathfrak{o}_K$, was nach Voraussetzung ausgeschlossen wurde. Sei $s > \max\{N\left((\Delta f)\mathfrak{o}_K\right), \sqrt{d}+1\}$. Wir teilen das Produkt wieder in zwei Produkte auf und erhalten

$$c(f) := \prod_{P \lhd \mathfrak{o}_K}(1-\frac{\omega(P)}{N(P)^2}) = \prod_{\substack{P \\ \text{char}(\mathfrak{o}_K/P)<s}}(1-\frac{\omega(P)}{N(P)^2}) \prod_{\substack{P \\ \text{char}(\mathfrak{o}_K/P)\geq s}}(1-\frac{\omega(P)}{N(P)^2}) \quad .$$

Nach Satz 3.6 b) ist das erste Produkt endlich. Weiter gilt $\Delta f \notin P$ für jedes Primideal P mit $\text{char}(\mathfrak{o}_K/P) > N\left((\Delta f)\mathfrak{o}_K\right)$. Denn sonst wäre $(\Delta f)\mathfrak{o}_K \subset P$ und aus der Multiplikativität der Norm und Satz 3.1 würde folgen, dass $\text{char}(\mathfrak{o}_K/P)$ ein Teiler

von $N((\Delta f)\mathfrak{o}_K)$ ist, was durch die Wahl von P ausgeschlossen wurde.

Also können wir durch Lemma 3.6 und Schritt 1 das zweite Produkt wie folgt abschätzen:

$$\prod_{\substack{P \\ \mathrm{char}(\mathfrak{o}_K/P)\geq s}} (1-\frac{\omega(P)}{N(P)^2}) \geq \prod_{\substack{P \\ \mathrm{char}(\mathfrak{o}_K/P)\geq s}} (1-\frac{d}{N(P)^2}) \geq \prod_{p\geq s}(1-\frac{d}{p^2})^n = \left(\prod_{p\geq s}(1-\frac{d}{p^2})\right)^n \quad .$$

Wie schon im Beweis von Theorem 1.6 gezeigt, ist $\prod_{p\geq s}(1-\frac{d}{p^2}) > 0$ und somit auch $\left(\prod_{p\geq s}(1-\frac{d}{p^2})\right)^n > 0$. Also gilt

$$0 < \prod_{P\lhd\mathfrak{o}_K} (1-\frac{\omega(P)}{N(P)^2}) =: c(f) \quad .$$

□

Wir haben in Kapitel 1 gezeigt, dass die Dichte quadratfreier Werte eines Polynoms größer als 0 ist. Daher müssen wir, um diese Aussage zu verallgemeinern, eine genaue Abschätzung für das Wachstum der Menge $\{a \in \mathfrak{o}_K \,|\, \|\varphi(a)\|_\infty \leq y\}$ finden.

Sei I ein Ideal in $\mathfrak{o}_K$, dann können wir I mit Hilfe der geometrischen Abbildung φ auf kanonische Weise als Untergitter von $\mathfrak{o}_K$ auffassen. Mit F_I bezeichnen wir eine Fundamentalmasche von I.

3.9. Sei $I \lhd \mathfrak{o}_K$ und $y \in \mathbb{R}^+$ wie bisher. Wir werden ab jetzt folgende Notationen benutzen:

1. $R_y := \{r \in \mathbb{R}^n \mid \|r\|_\infty \leq y\}$
2. $L_y(F_I) :=$ Anzahl von Translaten von F_I, die ganz in R_y enthalten sind
3. $L_y^+(F_I) :=$ Anzahl von Translaten von F_I, die R_y schneiden
4. $\widehat{L}_y(F_I) :=$ Anzahl von Translaten von F_I, die R_y schneiden, aber nicht ganz in R_y enthalten sind

Lemma 3.10. *Das Volumen einer Fundamentalmasche von $\mathfrak{o}_K$ ist gegeben durch* $\mathrm{Vol}(F_{\mathfrak{o}_K}) = 2^{-s}\sqrt{|\Delta_K|}$.

Beweis: Im Beweis von Satz 3.4 haben wir gezeigt, dass $|\det(\varphi(w_1),...,\varphi(w_n))|$ gleich $2^{-s}\sqrt{|\Delta_K|}$ ist für eine beliebige $\mathbb{Z}$-Basis $\{w_1,...,w_n\}$ von $\mathfrak{o}_K$. Allerdings ist $|\det(\varphi(w_1),...,\varphi(w_n))| = \mathrm{Spat}(\varphi(w_1),...,\varphi(w_n)) = \mathrm{Vol}(F_{\mathfrak{o}_K})$. □

Satz 3.11. *Mit den Bezeichnungen aus* 3.9 *gilt:*
a) $L_y(F_I) = \frac{2^{n+s}}{N(I)\sqrt{|\Delta_K|}} y^n + O(y^{n-1}) = L_y^+(F_I)$
b) $\widehat{L}_y(F_I) = O(y^{n-1})$.

Beweis: Aus der Definition in 3.9 folg direkt

$$\widehat{L}_y(F_I) = L_y^+(F_I) - L_y(F_I) \quad .$$

Damit folgt b) sofort aus a). Es genügt also a) zu beweisen.
Sei $B := \{b_1, ..., b_n\}$ eine Basis von $\varphi(I)$. Schreibe $b_i = (b_{i1}, ..., b_{in})^t \in \mathbb{R}^n$. Die Länge von F_I in die i-te Koordinatenrichtung bezeichnen wir mit $L_i := \sum_{j=1}^n |b_{ji}|$. Diese Werte sind gerade so gewählt, dass jedes Translat von F_I, das R_y schneidet, ganz im n-dimensionalen Quader mit den Eckpunkten $(\pm(y+L_1), ..., \pm(y+L_n))$ liegt. Dieser Quader hat das Volumen $2^n \prod_{i=1}^n (y + L_i)$. Damit erhalten wir die Abschätzung

$$L_y(F_I) \leq L_y^+(F_I) \leq \mathrm{Vol}(F_I)^{-1} 2^n \prod_{i=1}^n (y + L_i) = \mathrm{Vol}(F_I)^{-1} 2^n y^n + O(y^{n-1}) \quad .$$

Mit demselben Argument erhalten wir, dass die Translate von F_I, die ganz in R_y liegen, den Quader mit den Eckpunkten $(\pm(y-L_1), ..., \pm(y-L_n))$ komplett überdecken. Da dieser das Volumen $2^n \prod_{i=1}^n (y - L_i)$ hat, gilt auch

$$\mathrm{Vol}(F_I)^{-1} 2^n \prod_{i=1}^n (y - L_i) = \mathrm{Vol}(F_I)^{-1} 2^n y^n + O(y^{n-1}) \leq L_y(F_I) \leq L_y^+(F_I) \quad .$$

Damit haben wir nun gezeigt:

$$L_y(F_I) = \mathrm{Vol}(F_I)^{-1} 2^n y^n + O(y^{n-1}) = L_y^+(F_I) \quad .$$

Mit dem Verhältnis $\mathrm{Vol}(F_I) = N(I)\,\mathrm{Vol}(F_{\mathfrak{o}_K})$ (eine einfache Anwendung des Elementarteilersatzes auf I und $\mathfrak{o}_K$) und Lemma 3.10 folgt direkt die Aussage a) und damit der Satz. □

Satz 3.11 angewendet auf $I = \mathfrak{o}_K$ liefert, da in jeder Fundamentalmasche von $F_{\mathfrak{o}_K}$ genau ein Element aus $\mathfrak{o}_K$ liegt, dass $\frac{2^{n+s}}{\sqrt{|\Delta_K|}} y^n + O(y^{n-1})$ Elemente aus $\mathfrak{o}_K$ in R_y liegen.

Nun können wir Satz 3.5 weiter konkretisieren. Zu zeigen ist jetzt

$$\left|\left\{a \in \mathfrak{o}_K \,\middle|\, \|\varphi(a)\|_\infty \leq y, f(a) \notin P^2 \quad \forall P \lhd \mathfrak{o}_K \text{ mit } N(P) \leq y\right\}\right| \sim c(f) \frac{2^{n+s}}{\sqrt{|\Delta_K|}} y^n \quad .$$

Diese Formulierung von Satz 3.5 wollen wir nun beweisen.

Beweis von 3.5: Wir definieren das Ideal $M_y := \prod_{\substack{P \\ N(P)\leq\sqrt{\log y}}} P^2$. Es gilt

$$N(M_y) = \prod_{\substack{P \\ N(P)\leq\sqrt{\log y}}} N(P)^2 \leq \prod_{\substack{P \\ \mathrm{char}(\mathfrak{o}_K/P)\leq\sqrt{\log y}}} N(P)^2 \overset{3.6}{\leq} \prod_{p\leq\sqrt{\log y}} p^{2n}$$

$$= \exp\left(\sum_{p\leq\sqrt{\log y}} \log p^{2n}\right) \leq \exp\left(2n \sum_{p\leq\sqrt{\log y}} \log p\right) = \exp\left(O(\sqrt{\log y})\right) = o(y) \quad .$$

Die letzten beiden Gleichungen entnehmen wir dem Beweis von Theorem 1.6 .
Wir werden wieder zeigen, dass in $\mathfrak{o}_K/M_y$ genau $\prod_{P,N(P)\leq\sqrt{\log y}}(N(P^2)-\omega(P))$ Elemente a existieren, sodass $f(a) \not\equiv 0 \mod P^2 \quad \forall P \lhd \mathfrak{o}_K$ mit $N(P) \leq \sqrt{\log y}$. Nach dem chinesischen Restsatz gilt $\mathfrak{o}_K/M_y \cong \mathfrak{o}_K/P_1^2 \times \cdots \times \mathfrak{o}_K/P_r^2$, wobei $P_1, ..., P_r$ genau die Primideale sind, deren Norm kleiner oder gleich $\sqrt{\log y}$ ist. In jedem $\mathfrak{o}_K/P_i^2$ existieren nach Definition von $\omega(P)$ genau $N(P_i^2) - \omega(P_i)$ Elemente a, sodass $f(a) \not\equiv 0 \mod P_i^2$ gilt. Daraus folgt die Behauptung.
Also sind in jeder Fundamentalmasche von $\varphi(M_y)$ genau $\prod_P(N(P^2)-\omega(P))$ Elemente aus $\mathfrak{o}_K$ mit gewünschter Eigenschaft, wobei P in dem Produkt über alle Primideale $P \lhd \mathfrak{o}_K$ mit $N(P) \leq \sqrt{\log y}$ läuft. Mit den Notationen aus 3.9 erhalten wir ähnlich wie in Kapitel 1:

$$\left|\left\{a \in \mathfrak{o}_K \,\middle|\, \|\varphi(a)\|_\infty \leq y, f(a) \not\equiv 0 \mod P^2 \quad \forall P \lhd \mathfrak{o}_K \text{ mit } N(P) \leq \sqrt{\log y}\right\}\right|$$

$$= L_y(F_{M_y}) \prod_{\substack{P \\ N(P)\leq\sqrt{\log y}}} (N(P^2)-\omega(P)) + O(N(M_y))\widehat{L}_y(F_{M_y})$$

$$\overset{3.11}{=} \frac{2^{n+s}}{N(M_y)\sqrt{|\Delta_K|}} y^n N(M_y) \prod_{\substack{P \\ N(P)\leq\sqrt{\log y}}} (1 - \frac{\omega(P)}{N(P)^2}) + o(y)O(y^{n-1})$$

$$\sim \frac{2^{n+s}}{\sqrt{|\Delta_K|}} c(f) y^n \quad .$$

Dies gilt, da $o(y)O(y^{n-1}) = o(y^n)$ ist und $c(f) > 0$ nach Lemma 3.8.

Um zu zeigen, dass die Anzahl von Elementen $a \in \mathfrak{o}_K$ mit $\|\varphi(a)\|_\infty \leq y$ und $f(a) \in P^2$ für ein $P \lhd \mathfrak{o}_K$ mit $\sqrt{\log y} < N(P) \leq y$ in $o(y^n)$ liegt, benötigen wir noch weitere Abschätzungen.

Es gilt

$$\sum_{\substack{P \\ N(P)\leq y}} \omega(P) \overset{3.7}{\ll} \sum_{\substack{P \\ N(P)\leq y}} d \ll \sum_{\substack{P \\ \mathrm{char}(\mathfrak{o}_K/P)\leq y}} d \overset{3.6b)}{\ll} nd\pi(y) \ll \frac{y}{\log y} \ll \frac{y}{\sqrt{\log y}}$$

und

$$\sum_{\substack{P \\ N(P)>z}} \frac{\omega(P)}{N(P)^2} \overset{3.7}{\ll} \sum_{\substack{P \\ N(P)>z}} \frac{d}{\mathrm{char}(\mathfrak{o}_K/P)^2} \leq d\sum_{p>z} n\frac{1}{p^2} \ll \frac{1}{z} \quad ,$$

wobei wir die letzte Abschätzung bereits in Kapitel 1 bewiesen haben.

Die Anzahl von Elementen $a \in \mathfrak{o}_K$ mit $\|\varphi(a)\|_\infty \leq y$ mit $f(a) \in P^2$ für ein $P \lhd \mathfrak{o}_K$ mit $\sqrt{\log y} < N(P) \leq y$ ist nach oben beschränkt durch

$$\sum_{\substack{P \\ y\geq N(P)>\sqrt{\log y}}} \omega(P)L_y^+(F_{P^2})$$

$$\overset{3.11}{\leq} \sum_{\substack{P \\ N(P)>\sqrt{\log y}}} \omega(P)\frac{2^{n+s}}{N(P^2)\sqrt{|\Delta_K|}}y^n + \sum_{\substack{P \\ N(P)\leq y}} \omega(P)O(y^{n-1})$$

$$\ll \frac{2^{n+s}}{\sqrt{|\Delta_K|}}y^n \sum_{\substack{P \\ N(P)>\sqrt{\log y}}} \frac{\omega(P)}{N(P)^2} + O(y^{n-1}) \sum_{\substack{P \\ N(P)\leq y}} \omega(P)$$

$$\ll \frac{y^n}{\sqrt{\log y}} = o(y^n)$$

wie in den beiden obigen Abschätzungen gezeigt.

Damit haben wir schließlich

$$\left|\left\{a \in \mathfrak{o}_K \middle| \|\varphi(a)\|_\infty \leq y, f(a) \notin P^2 \quad \forall P \lhd \mathfrak{o}_K \text{ mit } N(P) \leq y\right\}\right|$$

$$= \left|\left\{a \in \mathfrak{o}_K \middle| \|\varphi(a)\|_\infty \leq y, f(a) \notin P^2 \quad \forall P \lhd \mathfrak{o}_K \text{ mit } N(P) \leq \sqrt{\log y}\right\}\right| - o(y^n)$$

$$\sim c(f)\frac{2^{n+s}}{\sqrt{|\Delta_K|}}y^n \quad .$$

□

Um nun Granvilles Theorem für Zahlkörper zu beweisen, wollen wir uns wiederum auf die *abc*-Vermutung stützen. Hierzu benötigen wir zunächst eine Erweiterung der *abc*-Vermutung auf Zahlkörper.

Definition 3.12. *Ein Absolutbetrag auf einem Körper ist eine multiplikative Betragsfunktion $|.|$. Er wird nicht archimedisch genannt, falls die stärkere Dreiecksungleichung $|x+y| \leq \min\{|x|,|y|\}$ gilt und archimedisch, falls diese nicht gilt.*
Wir nennen zwei Absolutbeträge $|.|_1$ und $|.|_2$ äquivalent, falls ein positives reelles s existiert mit $|.|_1 = |.|_2^s$.

Wir können jedes $a \in K\backslash\{0\}$ eindeutig als Produkt von gebrochenen Primidealen darstellen in der Form

$$a\mathfrak{o}_K = \prod_P P^{v_P(a)} \quad ,$$

wobei P über alle Primideale läuft und $v_P(a) \in \mathbb{Z}$ nur für endlich viele Primideale P ungleich 0 ist (siehe [Ne] I Korollar 3.9). Für alle Primideale P setzen wir $v_P(0) = \infty$.

Satz 3.13. *Auf einem Zahlkörper K existieren bis auf Äquivalenz genau $r+s$ archimedische Absolutbeträge, nämlich die Beträge $|\sigma_i(.)|_\infty$, wobei $1 \leq i \leq r+s$ und $|.|_\infty$ den Standardbetrag auf $\mathbb{C}$ bezeichnet.*
Die paarweise nicht äquivalenten, nicht archimedischen Absolutbeträge auf K sind mit obigen Bezeichnungen gegeben durch

$$|.|_P = N(P)^{-v_P(.)} \quad ,$$

wobei P über alle Primideale in $\mathfrak{o}_K$ läuft.

Beweis: Siehe [Le] 20.4 Satz 6 und Satz 7. □

Ist der Grad des Zahlkörpers von K gleich n, normieren wir die Absolutbeträge aus Satz 3.13 wie folgt:

- $|\sigma(.)|^{1/n}$, falls σ eine reelle Einbettung von K ist.
- $|\sigma(.)\overline{\sigma(.)}|^{1/n}$, falls σ eine komplexe Einbettung von K ist.
- $|.|_P = N(P)^{-v_P(.)/n}$ für alle Primideale P aus $\mathfrak{o}_K$.

Die Menge aller auf diese Weise normierten Absolutbeträge bezeichnen wir mit M_K, die Teilmenge der nicht archimedischen Absolutbeträge mit M_K^{fin}. Wir können also jedem $v \in M_K^{\text{fin}}$ eindeutig ein Primideal aus $\mathfrak{o}_K$ zuordnen. Dieses wird im Folgenden mit P_v bezeichnet. $M_\mathbb{Q}$ ist also die Menge bestehend aus dem Standardbetrag $|.|_\infty$ und den p-adischen Beträgen $|.|_p$, wobei p über alle Primzahlen läuft.

Definition 3.14. *Sei $\boldsymbol{x} = (x_0 : ... : x_m) \in \mathbb{P}^m_K(K)$, für $m \in \mathbb{N}$. Die Höhe von $\boldsymbol{x}$ wird definiert als*

$$h(\boldsymbol{x}) := \sum_{v \in M_K} \max_j \log |x_j|_v$$

und die multiplikative Höhe von $\boldsymbol{x}$ als

$$H(\boldsymbol{x}) := e^{h(\boldsymbol{x})} \quad .$$

Die Höhe eines Elementes $a \in K$ definieren wir als $h(a) := h(a : 1)$.

$h(\boldsymbol{x})$ und somit auch $H(\boldsymbol{x})$ sind unabhängig von der Wahl der Koordinaten von $\boldsymbol{x}$ (siehe [BG] Lemma 1.5.3). Damit ist die Definition wohldefiniert.

Ein Primideal P_v in $\mathfrak{o}_K$ ist im Allgemeinen kein Hauptideal, deshalb können wir nicht wie im Fall $\mathfrak{o}_K = \mathbb{Z}$ ein Primideal auf kanonische Weise mit einem Element darstellen. Für festes P_v betrachten wir den Bewertungsring

$$R_{P_v} := \{x \in K \mid |x|_v \leq 1\} = \{x \in K \mid v_{P_v}(x) \geq 0\} \quad .$$

Dieser ist ein Hauptidealbereich (siehe z.B. [Kn] Kapitel 15). Somit können wir schreiben $P_v R_{P_v} = (\pi_v)$ und auf diese Art ein Primideal P_v durch ein bis auf Multiplikation mit Einheiten in R_{P_v} eindeutiges Element $\pi_v \in K$ darstellen.

Für $K = \mathbb{Q}$ und ein beliebiges $P_v \lhd \mathbb{Q}$ überlegt man sich leicht, dass $p = \pi_v$ gilt, wobei $p\mathbb{Z} = P_v$ ist.

abc-Vermutung für Zahlkörper 3.15. *Für einen fest gewählten Zahlkörper K und ein $\varepsilon > 0$ gilt*

$$(1-\varepsilon)h(x) \leq \sum_{v_P(x)>0} \log |\frac{1}{\pi_v}|_v + \sum_{v_P(1-x)>0} \log |\frac{1}{\pi_v}|_v + \sum_{v_P(\frac{1}{x})>0} \log |\frac{1}{\pi_v}|_v + O(1)$$

für alle $x \in K \backslash \{0, 1\}$. Die drei Summen laufen über alle Primideale $P \lhd \mathfrak{o}_K$ und der $O(1)$-Term ist, da K fest gewählt wurde, nur von ε abhängig.

Für genauere Erläuterungen zu dieser Vermutung verweisen wir auf [BG], Kapitel 14. Allerdings wollen wir kurz den Zusammenhang zwischen dieser Formulierung und der Formulierung aus 1.1 herstellen. Hierzu zeigen wir, dass aus dem Fall $K = \mathbb{Q}$ in der *abc*-Vermutung für Zahlkörper 3.15 tatsächlich die *abc*-Vermutung 1.1 folgt. Sei

also $K = \mathbb{Q}$ und $(a, b, c) \in \mathbb{N}^3$ wie in 1.1 . Wir setzen nun $x = \frac{c}{b}$. Dies eingesetzt in 3.15 liefert

$$(1-\varepsilon) \sum_{v \in M_{\mathbb{Q}}} \max\left\{\log|\frac{c}{b}|_v, 0\right\} \leq \sum_{v_p(\frac{c}{b})>0} \log|\frac{1}{\pi_v}|_v + \sum_{v_p(1-\frac{c}{b})>0} \log|\frac{1}{\pi_v}|_v + \sum_{v_p(\frac{b}{c})>0} \log|\frac{1}{\pi_v}|_v + O(1) \quad .$$

Wie bereits bemerkt gilt $|\frac{1}{\pi_v}|_v = |\frac{1}{p}|_p = p$. Da a, b, c paarweise teilerfremd sind, folgt weiter
$v_p(\frac{c}{b}) > 0 \Leftrightarrow p \mid c$,
$v_p(1 - \frac{c}{b}) > 0 \Leftrightarrow v_p(\frac{-a}{b}) > 0 \Leftrightarrow p \mid a$ und
$v_p(\frac{b}{c}) > 0 \Leftrightarrow p \mid b$.
Setzen wir diese Äquivalenzen in obige Ungleichung ein erhalten wir

$$(1-\varepsilon)\left(\sum_p \max\left\{\log|\frac{c}{b}|_p, 0\right\} + \log\frac{c}{b}\right) \leq \sum_{p|c} \log p + \sum_{p|a} \log p + \sum_{p|b} \log p + O(1)$$

$$\Leftrightarrow (1-\varepsilon)\left(\log b + \log\frac{c}{b}\right) \leq \sum_{p|abc} \log p + O(1)$$

$$\Leftrightarrow c^{1-\varepsilon} \leq C(\varepsilon) \prod_{p|abc} p = C(\varepsilon)\,\mathrm{rad}(abc) \quad .$$

Die letzte Umformung erhalten wir dadurch, dass der $O(1)$-Term nach Voraussetzung nur von ε abhängig ist. Da $\varepsilon > 0$ sowohl in 3.15 als auch in 1.1 beliebig zu wählen ist, ist die letzte Ungleichung tatsächlich äquivalent zur Formulierung in 1.1.

In 3.15 ist die Verallgemeinerung des Radikals gegeben durch die Summe $\mathrm{cond}^K_{[0]}(x) + \mathrm{cond}^K_{[1]}(x) + \mathrm{cond}^K_{[\infty]}(x)$ für ein $x \in K$. Für Elemente aus $\mathbb{P}^m_K$ definieren wir allgemeiner:

Definition 3.16. *Sei $\boldsymbol{x} \in \mathbb{P}^m_K \setminus \mathrm{supp}(D)$, wobei D ein reduzierter Divisor auf $\mathbb{P}^m_K$ ist. Dann ist der Conductor von $\boldsymbol{x}$ gegeben durch*

$$\mathrm{cond}^K_\lambda(\boldsymbol{x}) := \sum_{v \in M^{\mathrm{fin}}_{K(\boldsymbol{x})}} \chi(\lambda(\boldsymbol{x}, v)) \log|\frac{1}{\pi_v}|_v \quad .$$

Hierbei gilt

$$\chi(t) = \begin{cases} 0 & \text{für } t \leq 0 \\ 1 & \text{für } t > 0 \end{cases} \quad .$$

λ bezeichnet eine lokale Höhe zu D und $K(\boldsymbol{x})$ ist definiert als $K(x_0, ..., x_m)$, wobei $\boldsymbol{x} = (x_0 : ... : x_m)$ ist.

Für die hier und im folgenden Theorem benutzten Begriffe verweisen wir auf [BG].

Theorem 3.17. *Sei D ein reduzierter Divisor auf $\mathbb{P}^m_K$. Für jedes $\varepsilon > 0$ folgt aus der abc-Vermutung für Zahlkörper* 3.15

$$h_D(\boldsymbol{x}) + h_{K_{\mathbb{P}^m_K}}(\boldsymbol{x}) \leq \mathrm{cond}^K_\lambda(\boldsymbol{x}) + \varepsilon h(\boldsymbol{x}) + O(1)$$

für alle $\boldsymbol{x} \in \mathbb{P}^m_K(K) \backslash \mathrm{supp}(D)$.

Beweis: Siehe [BG] Remark 14.4.17. □

Um eine Verallgemeinerung von Theorem 1.2 zu erhalten betrachten wir nun einen Spezialfall des obigen Theorems 3.17.
Sei $F \in \mathfrak{o}_K[x, y]$ ein homogenes quadratfreies Polynom vom Grad $d+1$, dann setzen wir $D = \mathrm{div}(F)$. D ist reduziert, da F quadratfrei ist. Mit den von uns benutzten Bezeichnungen aus [BG] ist somit $\mathrm{supp}(D)$ die Punktmenge der Nullstellen von F. Weiter setzen wir $m = 1$. Wir betrachten also Elemente $\boldsymbol{x} := (x_0 : x_1) \in \mathbb{P}^1_K(K) \backslash \mathrm{supp}(D)$, also die Tupel (x_0, x_1), für die $F(x_0, x_1) \neq 0$ ist. Zu D wählen wir die lokale Höhe

$$\lambda(P, v) := \log \frac{\max\{|x_0|_v^{d+1}, |x_1|_v^{d+1}\}}{|F(x_0, x_1)|_v}$$

(vergleiche z.B. auch [HS] Example B.8.4). Da alle Koeffizienten eines Punktes $\boldsymbol{x} \in \mathbb{P}^1_K(K)$ schon in K liegen, ist für ein solches $\boldsymbol{x}$ gerade $M_{K(\boldsymbol{x})} = M_K$. Weiter gelten die Gleichungen

$$h_D(\boldsymbol{x}) = (d+1)h(\boldsymbol{x}) + O(1) \quad \text{und} \quad h_{K_{\mathbb{P}^1_K}}(\boldsymbol{x}) = -2h(\boldsymbol{x}) + O(1)$$

(analog zu [BG], 14.4.11 und Remark 14.4.17). Mit diesen Überlegungen folgt aus Theorem 3.17, also aus der *abc*-Vermutung für Zahlkörper 3.15

$$(d - 1 - \varepsilon)h(x_0 : x_1) \leq \mathrm{cond}^K_\lambda(x_0 : x_1) + O(1) \quad .$$

Wir wählen nun $x_0, x_1 \in \mathfrak{o}_K$ teilerfremd. Dann gilt

$$\lambda((x_0 : x_1), v) = \log \frac{1}{|F(x_0, x_1)|_v} > 0 \Leftrightarrow F(x_0, x_1) \in P_v \quad .$$

Damit haben wir also

$$\mathrm{cond}^K_\lambda(x_0 : x_1) = \sum_{P_v \ni F(x_0, x_1)} \log |\frac{1}{\pi_v}|_v \quad .$$

Wir wollen nun $|\pi_v|_v$ berechnen. Da $v_{P_v}(x) \geq 0$ für jedes Element $x \in R_{P_v}$ ist, gilt $v_{P_v}(x) \geq 1$ für jedes Element $x \in P_v R_{P_v}$. Weiter existieren in P_v Elemente, die nicht in P_v^2 liegen. Dies haben wir z.B. im Beweis von Lemma 3.7 gesehen. Somit existiert ein Element $a \in P_v \subset P_v R_{P_v}$ mit $v_{P_v}(a) = 1$. Also muss auch für jedes erzeugende Element von $P_v R_{P_v}$ gelten $v_{P_v}(\pi_v) = 1$. Damit ist also nach Definition

$$|\pi_v|_v = N(P_v)^{-1/n} \quad .$$

Fassen wir alle obigen Ergebnisse zusammen, so erhalten wir folgendes Resultat als Spezialfall von Theorem 3.17:

3.18. *Sei $F \in \mathfrak{o}_K[x,y]$ ein quadratfreies homogenes Polynom vom Grad $d+1$. Unter Voraussetzung der abc-Vermutung für Zahlkörper 3.15 gilt für alle teilerfremden $x_0, x_1 \in \mathfrak{o}_K$, für die $F(x_0,x_1) \neq 0$ ist, und jedes $\varepsilon > 0$*

$$(d-1-\varepsilon)h(x_0:x_1) \leq \sum_{P_v \ni F(x_0,x_1)} \log |\frac{1}{\pi_v}|_v + O(1) \quad .$$

Dies ist offensichtlich äquivalent zu

$$H(x_0:x_1)^{(d-1-\varepsilon)} \leq c \prod_{P_v \ni F(x_0,x_1)} |\frac{1}{\pi_v}|_v = c \prod_{P_v \ni F(x_0,x_1)} N(P_v)^{1/n} \quad .$$

Satz 3.19. *Sei $f \in \mathfrak{o}_K[x]$ quadratfrei vom Grad d und $a \in \mathfrak{o}_K$ mit $f(a) \neq 0$. Unter Voraussetzung der Gültigkeit der abc-Vermutung für Zahlkörper* 3.15 *gilt für jedes $\varepsilon > 0$*

$$H(a)^{(d-1-\varepsilon)} \ll \prod_{P \ni f(a)} N(P)^{1/n} \quad .$$

Beweis: Analog zum Beweis von Korollar 1.3 zeigt man, dass $F(x,y) := y^{d+1} f(\frac{x}{y})$ ein homogenes quadratfreies Polynom vom Grad $d+1$ ist. Weiter gilt $F(a,1) = f(a)$. Wir wenden nun das Resultat 3.18 auf F an und erhalten die gewünschte Ungleichung. □

Satz 3.19 ist offensichtlich eine Verallgemeinerung von Satz 1.3. Allerdings müssen wir noch die Norm von Idealen in Bezug setzen zu dem bis hierhin verwendeten Betrag $\|\varphi(.)\|_\infty$. Dazu betrachten wir die multiplikative Höhe H.
Für ein $a \in \mathfrak{o}_K$ ist jeder Exponent in der Zerlegung in gebrochene Primideale von $a\mathfrak{o}_K$

nicht negativ. Also ist $|a|_v \leq 1$ für alle $v \in M_K^{\text{fin}}$. Diese normierten Absolutbeträge spielen daher keine Rolle für den Wert der Höhe eines Elements aus $\mathfrak{o}_K$. Es ist

$$H(a) := \prod_{v \in M_K} \max\{|a|_v, 1\} = \prod_{i=1}^{r} \max\left\{|\sigma_i(a)|^{1/n}, 1\right\} \prod_{j=r+1}^{r+s} \max\left\{|\sigma_j(a)\overline{\sigma_j(a)}|^{1/n}, 1\right\} \quad .$$

Da $|\sigma(a)| = |\overline{\sigma(a)}|$ ist, können wir also auch schreiben

$$H(a) = \prod_{\sigma} \max\left\{|\sigma(a)|^{1/n}, 1\right\} \quad .$$

Satz 3.20. *Sei $f \in \mathfrak{o}_K[x]$ ein quadratfreies Polynom vom Grad d. Unter Voraussetzung der Gültigkeit der abc-Vermutung für Zahlkörper* 3.15 *gilt für jedes $a \in \mathfrak{o}_K$ mit $\{0\} \neq f(a)\mathfrak{o}_K = I^2 J$ für $I, J \lhd \mathfrak{o}_K$ und jedes $\varepsilon > 0$*

$$\|\varphi(a)\|_\infty^{n+n\varepsilon} \gg N(I) \quad .$$

Beweis: Durch eine einfache Abschätzung erhält man $H(f(a)) \ll H(a)^d$. Weiter ist klar, dass gilt

$$H(f(a)) \geq N(f(a)\mathfrak{o}_K)^{1/n} = |N(f(a))|^{1/n} = \prod_{\sigma} |\sigma(f(a))|^{1/n} \quad .$$

Mit diesen Abschätzungen gilt

$$H(a)^d \gg H(f(a)) \geq |N(f(a))|^{1/n} = N(I)^{2/n} N(J)^{1/n} \quad .$$

Weiter erhalten wir aus Satz 3.19

$$H(a)^{(d-1-\varepsilon)} \ll N(I)^{1/n} N(J)^{1/n} \quad .$$

Fassen wir diese beiden Ungleichungen zusammen, erhalten wir

$$H(a)^{1+\varepsilon} \gg N(I)^{1/n} \quad .$$

Was uns nun noch fehlt, ist eine Abschätzung zwischen der Höhe $H(.)$ und der Maximumsnorm $\|\varphi(.)\|_\infty$. Es gilt $\max\{|\operatorname{Im}(\sigma_{r+i}(.))|, |\operatorname{Re}(\sigma_{r+i}(.))|\} \geq \frac{1}{\sqrt{2}}|\sigma_{r+i}(.)|$ und es existieren nur endlich viele Elemente $a \in \mathfrak{o}_K$ mit $\|\varphi(a)\|_\infty < 1$. Damit schließen wir

$$\|\varphi(a)\|_\infty \gg \max\{|\sigma_1(a)|, ..., |\sigma_r(a)|, |\sigma_{r+1}(a)|, ..., |\sigma_{r+s}(a)|\} \gg H(a) \quad ,$$

wodurch wir die Abschätzung

$$\|\varphi(a)\|_\infty^{1+\varepsilon} \gg N(I)^{1/n} \Leftrightarrow \|\varphi(a)\|_\infty^{n+n\varepsilon} \gg N(I)$$

erhalten. □

Für ein festes, quadratfreies f sei

$$H_y := \{a \in \mathfrak{o}_K \mid \|\varphi(a)\|_\infty \leq y, f(a) \in P^2 \text{ für ein } P \lhd \mathfrak{o}_K \text{ mit } N(P) > y\} \quad .$$

Nun wollen wir zeigen, dass $|H_y| = o(y^n)$ gilt. Hierzu definieren wir die Hilfsfunktion

$$\widehat{\varphi}(\gamma) := \begin{cases} \varphi(\gamma) & \text{für} \quad \gamma \in K \\ 0 & \text{für} \quad \gamma \notin K \end{cases}$$

für alle $\gamma \in \mathbb{C}$. Sind $y_1, ..., y_n \in \mathbb{C}$ die Nullstellen von f, so definieren wir

$$m_f := \max\{\|\widehat{\varphi}(y_i - y_j)\|_\infty \mid 1 \leq i, j \leq n\} \quad .$$

Sei $\mathfrak{I} \lhd \mathfrak{o}_K$ so gewählt, dass für jedes Element $\beta \in \mathfrak{I}$ gilt $\|\varphi(\beta)\|_\infty > m_f$. Ist $v \in \varphi(\mathfrak{o}_K)\backslash\{0\}$ ein Punkt mit kleinster Maximumsnorm und $k \in \mathbb{N}$ so gewählt, dass $\|kv\| > m_f$ ist, so können wir beispielsweise das Hauptideal $k\mathfrak{o}_K$ als $\mathfrak{I}$ wählen. Wir schreiben $\mathfrak{o}_K/\mathfrak{I} := \{[\beta_1], ..., [\beta_{N(\mathfrak{I})}]\}$ und betrachten die Polynome

$$g_i(x) := \prod_{\beta \in [\beta_i]} f(x+\beta)^{\chi(\beta)}, \text{ wobei } \chi(\beta) := \begin{cases} 1 & \text{falls} \quad \beta \in \{\sum_{i=1}^n t_i z v_i \,|0 \leq t_i < 1\} \\ 0 & \text{sonst} \end{cases} .$$

Hierbei ist $z \in \mathbb{N}$ beliebig und $\{v_1, ..., v_n\}$ eine Basis von $\mathfrak{o}_K$. Die Bedingung, dass $\beta \in \{\sum_{i=1}^n t_i z v_i \,|0 \leq t_i < 1\}$ ist, ist gleichbedeutend damit, dass $\beta \in F_{z\mathfrak{o}_K}$ ist. $F_{z\mathfrak{o}_K}$ bezeichnet hierbei die Fundamentalmasche von $z\mathfrak{o}_K$, die durch die Elemente $zv_1, ..., zv_n$ aufgespannt wird. Somit liegen in $F_{z\mathfrak{o}_K}$ genau z^n Elemente aus $\mathfrak{o}_K$. Da $f(x)$ quadratfrei ist, gilt dies auch für $f(x+\beta)$. Hätten $f(x+\beta)$ und $f(x+\beta')$ eine gemeinsame Nullstelle für $\beta \neq \beta'$ aus der selben Nebenklasse von $\mathfrak{I}$, so würde gelten

$$x + \beta - y_i = x + \beta' - y_j \Leftrightarrow y_j - y_i = \beta' - \beta \quad .$$

Daraus folgt aber, dass auch $\|\widehat{\varphi}(y_j - y_i)\|_\infty = \|\widehat{\varphi}(\beta' - \beta)\|_\infty$ gilt. Da nun aber $\beta' - \beta \in \mathfrak{I}$ ist, kann dies nach Wahl von $\mathfrak{I}$ nicht erfüllt sein. Somit ist $g_i(x)$ quadratfrei.

Sei $g_i(a) \in I^2 J$ für zwei Ideale $I, J \lhd \mathfrak{o}_K$. Aus Satz 3.20 folgt $\|\varphi(a)\|_\infty^{n+n\varepsilon} \gg N(I)$. Für hinreichend großes y_0 gilt also:
Für jedes $a \in \mathfrak{o}_K$ mit $\|\varphi(a)\|_\infty > y_0$ und für alle $i \in \{1, ..., N(\mathfrak{I})\}$ liegen maximal n Faktoren $f(a+\beta)$ von $g_i(a)$ in einem Primidealquadrat P^2 mit $N(P) > \|\varphi(a)\|_\infty$.

Betrachten wir die Faktoren aller Werte $\{g_1(a), ..., g_{N(\mathfrak{J})}(a)\}$, so sehen wir, dass von den Werten $f(a+b)$ mit $b \in F_{z\mathfrak{o}_K}$ maximal $nN(\mathfrak{I})$ in einem Primidealquadrat P^2 mit $N(P) > \|\varphi(a)\|_\infty$ liegen.

Sei $F_{z\mathfrak{o}_K}(a)$ das um den Vektor $\varphi(a)$ verschobene Translat von $F_{z\mathfrak{o}_K}$. Falls $\|\varphi(a)\|_\infty$ größer y_0 ist, haben wir oben gezeigt, dass in $F_{z\mathfrak{o}_K}(a) \cap \mathfrak{o}_K$ maximal $nN(\mathfrak{I})$ Elemente liegen, deren Bilder unter f in einem Primidealquadrat P^2 mit $N(P) > \|\varphi(a)\|_\infty$ enthalten sind. Gilt zusätzlich noch $\|\varphi(a)\|_\infty < y$, so ist klar, dass in $F_{z\mathfrak{o}_K}(a) \cap \mathfrak{o}_K$ maximal $nN(\mathfrak{I})$ Elemente existieren, deren Bilder unter f in einem Primidealquadrat P^2 mit $N(P) > y$ liegen. Diese Abschätzung gilt also für alle Translate von $F_{z\mathfrak{o}_K}$, die ganz in $R_y \backslash R_{y_0}$ enthalten sind. Die Elemente aus $R_y \cap \mathfrak{o}_K$, die wir auf diese Weise noch nicht betrachtet haben, sind diejenigen, die in einem Translat von $F_{z\mathfrak{o}_K}$ liegen, das entweder nicht ganz in R_y enthalten ist oder R_{y_0} schneidet. Die Anzahl dieser Elemente ist nach oben beschränkt durch $\widehat{L_y}(F_{z\mathfrak{o}_K})z^n + L^+_{y_0}(F_{z\mathfrak{o}_K})z^n$. Da $L^+_{y_0}(F_{z\mathfrak{o}_K})z^n = O(1)$ ist, spielt dieser Wert in der folgenden Abschätzung keine Rolle. Mit diesen Überlegungen gilt

$$\begin{aligned} |H_y| &:= |\{a \in \mathfrak{o}_K \mid \|\varphi(a)\|_\infty \leq y, f(a) \in P^2 \text{ für ein } P \text{ mit } N(P) > y\}| \\ &\ll L_y(F_{z\mathfrak{o}_K})nN(\mathfrak{I}) + \widehat{L_y}(F_{z\mathfrak{o}_K})z^n \overset{3.11}{\sim} \frac{2^{n+s}}{z^n\sqrt{|\Delta_K|}} y^n nN(\mathfrak{I}) + O(y^{n-1}) \quad . \end{aligned}$$

Angenommen es existiert ein Limessuperior $\epsilon > 0$ von $\frac{|H_y|}{y^n}$, dann wählen wir z so, dass gilt

$$\limsup_{y\to\infty} \frac{|H_y|}{y^n} \leq \frac{2^{n+s}nN(\mathfrak{I})}{z^n\sqrt{|\Delta_K|}} < \epsilon \quad .$$

Also kann ein solches $\epsilon > 0$ nicht existieren und folglich gilt $|H_y| = o(y^n)$. Damit gilt abschließend:

Granvilles Theorem für beliebige Zahlkörper 3.21. *Sei K ein Zahlkörper vom Grad n und $f(x) \in \mathfrak{o}_K[x]$ ein quadratfreies Polynom vom Grad d. Weiter existiere kein Primideal $P \lhd \mathfrak{o}_K$, so dass $f(a) \in P^2$ für alle $a \in \mathfrak{o}_K$. Dann gilt unter Voraussetzung der abc-Vermutung für Zahlkörper 3.15*

$$|\{a \in \mathfrak{o}_K \,|\, \|\varphi(a)\|_\infty \leq y, f(a) \text{ quadratfrei } \}| \sim c(f)\frac{2^{n+s}}{\sqrt{|\Delta_K|}} y^n$$

für eine Konstante $c(f) > 0$.

Beweis: Mit unseren Vorüberlegungen und obigen Bezeichnungen gilt

$$|\{a \in \mathfrak{o}_K \mid \|\varphi(a)\|_\infty \leq y, f(a) \text{ quadratfrei } \}|$$

$$= |\{a \in \mathfrak{o}_K \mid \|\varphi(a)\|_\infty \leq y, f(a) \notin P^2 \quad \forall P \lhd \mathfrak{o}_K \text{ mit } N(P) \leq y\}| - O(|H_y|)$$

$$\sim c(f)\frac{2^{n+s}}{\sqrt{|\Delta_K|}}y^n$$

mit $c(f) > 0$, wie in Lemma 3.7 gezeigt. □

Wir haben nun das Ziel dieses Kapitels erreicht und eine Verallgemeinerung von Granvilles Theorem auf beliebige Zahlkörper hergeleitet, formuliert und bewiesen. Unsere Formulierung in Theorem 3.21 ist nur eine Möglichkeit Granvilles Theorem zu verallgemeinern. Im Folgenden werden wir kurz einige mögliche Abänderungen in unserer Formulierung vorstellen, ohne detaillierte Beweise vorzuführen.

In 3.9 hatten wir $R_y := \{r \in \mathbb{R}^n \mid \|r\|_\infty \leq y\}$ definiert. Genauer können wir diesen Bereich auch mit $R_y(\|.\|_\infty)$ bezeichnen. Mit Satz 3.11 folgt also, dass unter den Voraussetzungen von Theorem 3.21 gilt

$$|\{a \in \mathfrak{o}_K \,|\|\varphi(a)\|_\infty \leq y, f(a) \text{ quadratfrei } \}| \sim c(f)\frac{2^s}{\sqrt{|\Delta_K|}} \operatorname{Vol}\left(R_1(\|.\|_\infty)\right) y^n \quad .$$

In dieser Formulierung von Theorem 3.21 können wir die Maximumsnorm auch durch eine beliebige andere Norm des $\mathbb{R}^n$ ersetzen. Wählen wir zum Beispiel die L_2-Norm, so folgt, wiederum unter den Voraussetzungen von Theorem 3.21, für gerades n

$$|\{a \in \mathfrak{o}_K \,|\|\varphi(a)\|_2 \leq y, f(a) \text{ quadratfrei } \}| \sim c(f)\frac{\pi^{n/2}2^s}{\sqrt{\Delta_K}(\frac{n}{2})!}y^n \quad .$$

Denn $\operatorname{Vol}(R_1(\|.\|_2))$ ist das Volumen der n-dimensionalen Einheitskugel, also gleich $\frac{\pi^{n/2}}{(\frac{n}{2})!}$ für gerades n.

Sind wir nur interessiert an Elementen aus $\varphi(\mathfrak{o}_K)$, die in einem kegelförmigen Teilbereich des $\mathbb{R}^n$ liegen, so müssen wir bei der Konstantenberechnung erst den Bereich $R_y(\|.\|)$ mit diesem Kegel schneiden.

Setzen wir in Theorem 3.21 $K = \mathbb{Q}$, so erhalten wir unter den gegebenen Voraussetzungen die Aussage

$$|\{a \in \mathbb{Z} \,||a| \leq y, f(a) \text{ quadratfrei } \}| \sim 2c(f)y \quad .$$

Wir wollen nun eine „eins-zu-eins“ Verallgemeinerung von Granvilles Theorem 1.6 formulieren. Dazu benötigen wir eine Erweiterung der natürlichen Zahlen $\mathbb{N}$ auf beliebige Zahlkörper. Wir definieren

$$\mathfrak{o}_K^+ := \{a \in \mathfrak{o}_K \,|\mathrm{Re}(\sigma(a)) > 0 \text{ für alle Einbettungen } \sigma \text{ von } K \text{ nach } \mathbb{C}\} \quad .$$

Da die einzige $\mathbb{Q}$-Einbettung von $\mathbb{Q}$ nach $\mathbb{C}$ die Identität ist, gilt $\mathfrak{o}_{\mathbb{Q}}^+ = \mathbb{N}$. Wir betrachten den Bereich

$$\mathbb{R}^n \supset R' := \left\{(x_1, ..., x_{r+2s}) \,\middle|\, x_i \in \mathbb{R}^+ \quad \forall i \in \{1, ..., r\} \cup \{r+1, r+3, ..., r+2s-1\}\right\}.$$

R' ist gerade so gewählt, dass die Gleichung $\varphi(\mathfrak{o}_K^+) = \varphi(\mathfrak{o}_K) \cap R'$ gilt. Das Volumen von $R_1(\|.\|_\infty) \cap R'$ ist gleich $\mathrm{Vol}(R_1(\|.\|_\infty))2^{-r-s}$. Damit erhalten wir durch unsere Vorüberlegungen die folgende Verallgemeinerung von Granvilles Theorem 1.6:

3.22. *Für jedes quadratfreie $f \in \mathfrak{o}_K[x]$, dessen Werte nicht in einem festen Primidealquadrat P^2 liegen, gilt unter Voraussetzung der abc-Vermutung für Zahlkörper 3.15*

$$\left|\left\{a \in \mathfrak{o}_K^+ \,|\|\varphi(a)\|_\infty \leq y, f(a) \text{ quadratfrei } \right\}\right| \sim c(f)\frac{2^{2s}}{\sqrt{|\Delta_K|}}y^n \quad ,$$

für eine Konstante $c(f) > 0$.

Setzen wir in 3.22 $K = \mathbb{Q}$, so erhalten wir Granvilles Theorem 1.6.

Literatur

[BFGS] Browkin, J.; Filaseta, M.; Greaves, G.; Schinzel, A.: *Squarefree values of polynomials and the abc-conjecture* , Greaves, G. R. H. (ed.) et al., Sieve Methods, Exponential Sums, and their Applications in Number Theory; London Mathematical Society Lecture Note Series 237 S.65-86; Cambridge University Press (1997)

[BG] Bombieri, E.; Gubler, W.: *Heights in Diophantine geometry*, New Mathematical Monographs: 4; Cambridge University Press (2006)

[Bro] Browkin, J.: *The abc-conjecture*, Bambah, R. P. (ed.) et al., Number Theory, Trends in Mathematics S.75-105; Birkhäuser (2000)

[Bru] Brüdern, J.: *Einführung in die analytische Zahlentheorie*; Springer (1995)

[Co] Cohen, H.: *A corse in computational algebraic number theory*, Graduate Texts in Mathematics Vol. 184; Springer (2000)

[Er] Erdös, P.: *Arithmetical Properties of Polynomials*, Journal of the London Mathematical Society Vol. 28 S.416-425; (1953)

[Fi1] Filaseta, M.: *Prime values of irreducible polynomials*, Acta Arithmetica 50, No.2 S.133-145; (1988)

[Fi2] Filaseta, M.: *Squarefree values of polynomials*, Acta Arithmetica 60, No.3 S.213-231; (1992)

[Gr] Granville, A.: *ABC allows us to count squarefrees*, International Mathematical Research Notices No.19 S.991-1009; (1998)

[Ho] Hooley, C.: *On the power free values of polynomials*, Mathematika Vol.14 S.21-26; (1967)

[HS] Hindry, M.; Silverman, J. H.: *Diophantine Geometry*, Graduate Texts in Mathematics Vol.201; Springer (2000)

[JS] Jantzen, J.C.; Schwermer, J.: *Algebra* ; Springer (2006)

[Kn] Kneser, M.: *Quadratische Formen*; Springer (2002)

[Ko] Koch, H.: *Zahlentheorie*, Algebraische Zahlen und Funktionen; Vieweg Studium (1997)

[La] Lang, S.: *Algebraic Number Theory*, Graduate Texts in Mathematics Vol. 110; Springer (2000)

[Le] Leutbecher, A.: *Zahlentheorie*, Eine Einführung in die Algebra; Springer (1996)

[Na] Nagel, T.: *Zur Arithmetik der Polynome*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg Vol.1 S.178-193; Springer (1922)

[Ne] Neukirch, J.: *Algebraische Zahlentheorie* ; Springer (1967)

[re] www.rekenmeemetabc.nl [Stand: 13. Juli 2009]

[uc] www.math.unicaen.fr/∼nitaj/abc.html [Stand: 13. Juli 2009]

Erklärung

- Ich erkläre mich damit einverstanden, dass meine Diplomarbeit nach § 6 Abs.1 des URG der Öffentlichkeit durch die Übernahme in die Bereichsbibliothek zugänglich gemacht wird. Damit können Leser der Bibliotheken die Arbeit einsehen und zu persönlichen wissenschaftlichen Zwecken Kopien aus dieser Arbeit anfertigen. Weitere Urheberrechte werden nicht berührt.
- Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel verfasst, sowie Zitate kenntlich gemacht habe.

Lukas Christopher Pottmeyer Dortmund, im Juli 2009