Von Lücken zwischen Primzahlen zur Optimierung von Gitterpunkten

Von Christian Elsholtz

Einleitung

Von der Antike zur Moderne

Zahlentheorie gehört zu den ältesten Disziplinen der Wissenschaft. So listet z.B. eine babylonische Tafel[1] ganzzahlige Lösungen der Gleichung $x^2+y^2=z^2$ auf. Man geht davon aus, dass derartige Tafeln eine Art Vorstufe von trigonometrischen Tabellen waren. Es ist bekannt, dass auch die Ägypter das rechtwinklige Dreieck mit Seitenlängen 3, 4 und 5 zur Landvermessung verwendeten.[2] Bei Euklid[3] finden sich bereits interessante Aussagen über Primzahlen.[4] So geht der Beweis, dass es unendlich viele Primzahlen gibt, auf ihn zurück. Darüber hinaus untersuchte er Primzahlen der Form $p=2^n-1$. Die Untersuchung von Primzahlen dieser Form ist heute zu einer Art Test für neue arithmetische Algorithmen, schnelle Hardware und verteiltes Rechnen ge-worden. Die jeweils größten bekannten Primzahlen sind von dieser Form.

In den letzten Jahrhunderten wurde die Theorie der Primzahlen durch bedeutende Mathematiker wie Fermat, Euler, Gauß und Riemann weiterentwickelt.

In den letzten Jahrzehnten haben die früher gelegten Grundlagen der Primzahltheorie Anwendungen gefunden, an die man zuvor hätte gar nicht denken können. Z.B. hängt die Sicherheit elektronischer Kommunikation (wie z.B. elektronischer Bezahlsysteme) zu einem erheblichen Teil daran, dass es nach unserem derzeitigen Wissen viel leichter ist, zwei große Primzahlen p und q zu finden und ihr Produkt n=pq zu berechnen, als von der Zahl n die Faktoren p und q zu finden, wenn man sie nicht kennt. Bei dem Problem, große Primzahlen zu finden, hat es im vergangenen Jahr einen bedeutenden theoretischen Durchbruch gegeben, von dem man sich erhofft, dass Weiterentwicklungen hiervon auch Auswirkungen auf die Praxis haben könnten.[5]

Im Jahr 2000 wurden acht Preise im Wert von jeweils einer Millionen US-Dollar auf die Lösung wichtiger mathematischer Probleme ausgesetzt. Der erste Preis[6] wurde von einem Verlag auf die erste korrekte Lösung eines Problems ausgesetzt, das auf einen Briefwechsel zwischen Christian Goldbach und Leonhard Euler zurückgeht. Darin vermutete Goldbach (1742), dass jede gerade Zahl n>2 als Summe von zwei Primzahlen geschrieben werden kann, (also z.B. 4=2+2, 6=3+3, 8=3+5, 10=3+7 usw.). Diese Vermutung ist eine der bekanntesten offenen Fragen der Mathematik.

Fragen, die ohne Fachkenntnisse verständlich sind, die aber so schwer sind, dass sie niemand beantworten kann, haben seit jeher einen besonderen Reiz auf die Mathematiker ausgeübt. Ein beachtlicher Teil der heutigen Mathematik ist entwickelt worden, um sich an solche Fragen heranzuwagen. Die hierbei entwickelten Methoden sind in der Regel dann wichtiger als die ursprünglichen Fragen, weil man mit den neuen Methoden auch viele weitere Fragen beantworten kann.

Die sieben anderen Millionendollarpreise wurden vom Clay-Institute[7] ausgelobt. Darunter sind immerhin zwei weitere zahlentheoretische Probleme, wovon die Lösung eines der Probleme (die Riemann'sche Vermutung) Konsequenzen für unser Wissen über Lücken zwischen Primzahlen hätte.

Bisher wurde über einige Probleme der Zahlentheorie berichtet, bei denen entweder ein Durchbruch erzielt wurde oder bei denen man sich einen Durchbruch durch die Aussetzung der Preise erhofft.

Aktuelle Fragen über Lücken zwischen Primzahlen

In den folgenden Abschnitten werden wir uns verschiedenen Fragen nach Abständen zwischen Primzahlen zuwenden. Ich habe im Rahmen meiner Forschung der vergangenen Jahre hierzu neue Methoden entwickelt und werde über die Ergebnisse berichten. Die Methoden sind allgemein genug, um auch auf einige Gitterpunktprobleme angewendet werden zu können. Eine mögliche Anwendung eines solchen Problems diskutieren wir im letzten Abschnitt.

Während Primzahlen über die Multiplikation (bzw. Division) definiert sind, sind Fragen, die die Addition oder Subtraktion von Primzahlen betreffen, zumeist sehr schwer. Wir listen einige typische Fragen auf:

1) Kann jede gerade Zahl n>2 als Summe von zwei Primzahlen geschrieben werden? (Goldbach'sche Vermutung, s.o.)
2) Gibt es unendlich viele Primzahlen p, so dass auch p+2 eine Primzahl ist? (Beispiele sind (5, 7), (11, 13), (17, 19)). (Primzahlzwillingsproblem)
3) a) Gibt es unendlich viele Primzahlen der Form $p=a^2+1$?
   b) Gibt es unendlich viele Primzahlen, die in der Form $p=a^2+b^2$ (a, b sind ganze Zahlen) geschrieben werden können?
4) Gibt es zwischen n^2 und $(n+1)^2$ immer mindestens eine Primzahl?

Während Frage 3b) vollständig gelöst ist, gelten die anderen Fragen als hoffnungslos schwer. Es sind dort nur Teilantworten bekannt. Im nächsten Abschnitt wird die Antwort auf Frage 3b) erläutert, und in den folgenden Abschnitten werden Verallgemeinerungen von Frage 2 betrachtet.

Summen von zwei Quadraten

Die Frage, ob es unendlich viele Primzahlen von einer vorgegebenen Form wie a^2+b^2 gibt und wie man diese Primzahlen noch beschreiben kann, ist historisch wichtig gewesen und hat zur Entwicklung neuer Methoden im Bereich der Algebra und der Analysis geführt. Darüber hinaus werden wir im letzten Abschnitt sehen, dass ▸

[1] Die Tafel namens Plimpton 322 stammt etwa von 1750 vor Christus. Informationen unter *http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Babylonian_Pythagoras.html*

[2] Es ist $3^2+4^2=5^2$ und nach der Umkehrung des Satzes von Pythagoras folgt, dass dieses Dreieck rechtwinklig ist.

[3] etwa 300 vor Chr. Euklids Bücher galten Jahrhunderte lang als Standardwerk.

[4] Eine Primzahl ist eine natürliche Zahl n>1, die außer sich selbst und der 1 keine ganzzahligen Teiler hat. Die Menge der Primzahlen beginnt also mit 2,3,5,7,11,13,17...

[5] M. Agarwal, N. Kayal, N. Saxena: Primes is in P. Für das Originalmanuskript und relevante Information siehe *http://fatphil.org/maths/AKS/*

[6] Über die Millionendollarofferte vom 15. März 2000 berichten: *http://www.apostolosdoxiadis.com/million.htm* bzw. *http://www.apostolosdoxiadis.com/rules.htm*, *http://www.times-archive.co.uk/news/pages/tim/2000/03/16/timfeafea02004.html*

[7] Clay Institute, Millennium prize problems, (24. Mai 2000), *http://www.claymath.org/*

mit der Antwort auf diese Frage Probleme der diskreten Optimierung gelöst werden können.

Die Frage nach den Primzahlen der Form wird vollständig durch den folgenden Satz von Fermat und Euler beantwortet.

Satz 1: *Eine Primzahl p ist genau dann als Summe von zwei Quadraten natürlicher Zahlen darstellbar, wenn p=2 ist oder wenn p-1 durch 4 teilbar ist. Darüber hinaus ist (bis auf die Reihenfolge) die Darstellung $p=a^2+b^2$ eindeutig.*

Die Primzahlen p>2 lassen sich in zwei Klassen einteilen, nämlich solche, die bei Division durch 4 den Rest 1 lassen (wie z.B. 5, 13, 17, 29), und solche, die den Rest 3 lassen (wie z.B. 3, 7, 11, 19, 23). Der Satz besagt also, dass die Primzahlen der einen Klasse in der Form geschrieben werden können (wie z.B. $5 = 1^2 + 2^2, 13 = 2^2 + 3^2$), die Primzahlen der anderen Klasse aber nicht. Es ist sogar so, dass Primzahlen in beiden dieser Klassen im Wesentlichen gleich häufig vorkommen.

Das Primzahlzwillingsproblem und seine Verallgemeinerungen

Auch wenn die Frage, ob es unendlich viele Primzahlzwillinge (p, p+2) gibt (Frage 2 der obigen Liste), von niemandem beantwortet werden konnte, wurden bereits wesentlich weitergehende Fragen gestellt. Empirische Beobachtungen legen nahe, dass jede gerade Zahl unendlich oft als Differenz zweier Primzahlen vorkommt, (z.B. 10=17-7=47-37=107-97=...). Analog wurden auch längere „Muster“ von Lücken zwischen Primzahlen untersucht; allerdings ist hierbei etwas mehr Vorsicht geboten. Die Zahlen 3, 5 und 7 sind das einzige Tripel von drei aufeinander folgenden ungeraden Primzahlen. Im allgemeinen ist immer eine von drei aufeinander folgenden ungeraden Zahlen durch 3 teilbar. Im Gegensatz dazu wird vermutet, dass es unendlich viele Primzahlen p gibt, für die auch p+2 und p+6 prim sind, z.B. (11, 13, 17), und (41, 43, 47). Allgemeiner definiert man sogenannte zulässige Muster. Vereinfacht gesagt, ist ein Muster zulässig, wenn es keinen elementaren Grund dafür gibt, dass dieses Muster nur für endlich viele Primzahltupel vorkommen kann.[8]

Auch kompliziertere zulässige Muster von Primzahllücken kommen vermutlich unendlich oft vor. Durch empirische und heuristische Untersuchungen ist es sogar gelungen, diese Vermutungen zu quantifizieren, d.h. es gibt Prognosen, die voraussagen, wie oft diese Muster in einem endlichen Intervall [1,N] vorkommen. Um dies zu erläutern, beginnen wir mit einem der Hauptsätze der Primzahltheorie, der von Gauß vermutet und von Hadamard und de la Vallée-Poussin bewiesen wurde.

Satz 2: *Für die Anzahl $\pi(N)$ der Primzahlen im Intervall [1,N] gilt folgende Näherungsformel:*[9, 10]

$$\pi(N) \sim \frac{N}{\log N} \quad .$$

Anschaulich besagt der Satz, dass für eine zufällig gewählte große natürliche Zahl n die Wahrscheinlichkeit, dass n prim ist, etwa 1/log n beträgt. Wendet man das gleiche Zufallsexperiment auf n+2 an, so könnte man, wenn die Experimente unabhängig wären, erwarten, dass es im Intervall [1,N] etwa N/(log N)^2 viele Primzahlzwillinge gibt. Leider ist es nicht so, dass die Ereignisse „n ist prim“ und „n+2 ist prim“ unabhängig sind. Ist z.B. n+2 prim, so ist n ungerade, und damit auch n+2 ungerade, also keine echte Zufallszahl im ganzen Intervall [1,N]. Das Ergebnis wurde also um einen Faktor 2 verfälscht. Ist z.B. n durch 7 teilbar, so ist n+2 nicht durch 7 teilbar. Es lässt sich heuristisch erklären, wie diese Fehler durch einen geeigneten Korrekturfaktor berichtigt werden können; aber es ist noch niemandem gelungen, einen Beweis anzugeben. Hier ist eine genauere Formulierung dieser Vermutungen:

Vermutung 1: *Für die Anzahl $\pi_2(N)$ der Primzahlzwillinge (p, p+2) im Intervall [1,N] gilt:*

$$\pi_2(N) \sim C \frac{N}{(\log N)^2} \quad .$$

Hierbei ist

$$C = 2\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right) = 1{,}320\ldots$$

eine Konstante.

Als Verallgemeinerung hiervon vermutet man nun für längere Primzahllückenmuster:

Vermutung 2: Es sei $(a_1,\ldots,a_k)$ ein zulässiges Muster. Für die Anzahl $\pi_{(a_1,\ a_2,\ldots,a_k)}(N)$ der Primzahltupel $(n+a_1,\ n+a_2,\ \ldots,\ n+a_k)$ im Intervall [1,N] gilt

$$\pi_{(a_1,a_2,\ldots,a_k)}(N) \sim C_{(a_1,a_2,\ldots,a_k)} \frac{N}{(\log N)^k} \quad .$$

Hierbei ist $C_{(a_1,\ a_2,\ldots,a_k)}$ eine positive Konstante.

Eine allgemeinere Frage, die derartige k-Tupel-Probleme umfasst, kann wie folgt formuliert werden. Man definiert die Summe zweier Mengen A+B={a+b:a∈A, b∈B} (z.B. {1, 2, 7}+{2, 10}={3, 4, 9, 11, 12, 17}). Die Frage lautet dann, für welche Mengen A und B die Summenmenge A+B eine Teilmenge der Menge der Primzahlen ist. Das Primzahltripelproblem für (n, n+2, n+6) ist dann als Spezialfall enthalten: A={0, 2, 6} und B ist eine Teilmenge der Primzahlen, die z.B. die Zahlen 5, 11, 17, 41 enthalten darf. Die neue Formulierung enthält die obigen k-Tupelprobleme, ist aber allgemeiner, weil A und B auch Mengen mit unendlich vielen Elementen sein können.

Eine wichtige Frage in diesem Zusammenhang geht auf Ostmann zurück. Zunächst kann man prüfen, ob die Menge P aller Primzahlen auf diese Weise additiv zerlegt werden kann, so dass A+B=P gilt, wobei die Mengen A und B mindestens zwei Elemente enthalten. Eine nähere Untersuchung zeigt, dass dies (z.B. wegen der Primzahlen 2 und 3) nicht sein kann; aber Ostmann fragte, ob es Mengen A und B mit jeweils mindestens zwei Elementen gibt, so dass die Summenmenge A+B=P' für genügend große Elemente mit der Menge der Primzahlen übereinstimmt. Dies ist ein etwa 50 Jahre altes offenes Problem, das auch *inverses Goldbachproblem* genannt wird. Eine Reihe Mathematiker zeigte: Wenn es eine derartige Zerlegung A+B=P' geben sollte, dann müssen beide Mengen A und B unendlich viele Elemente enthalten. Aus einer Arbeit von Hornfeck aus dem Jahre 1954 ergibt sich ein quantitatives Resultat: Die Anzahl A(N) der Elemente der Menge A, die im Intervall [1,N] liegen, beträgt mindestens $(\log N)^k$, aber höchstens

$$N/(\log N)^k.$$

(Hierbei ist k eine beliebig große Konstante). Mit den damals vorhandenen Methoden konnte man kein besseres Resultat erwarten.

Erst im Jahre 1996 ergab eine Arbeit von Hofmann und Wolke den ersten Fortschritt. Sie verbesserten dies durch Anwendung einer neueren Methode zu mindestens[11] $\exp(c \log N/\log\log N)$, aber höchstens $N/\exp(c \log N/\log\log N)$. Auch hierbei sind die obere und untere Schranke noch weit auseinander. Durch die Entwicklung eines neuen Siebverfahrens, das die Vorteile zweier vorher bekannter Siebverfahren kombiniert, konnten nun diese Resultate um einen Faktor von fast $\sqrt{N}$ verbessert werden: A(N) muss mindestens

$$\frac{\sqrt{N}}{(\log N)^3} \quad ,$$

▸

[8] Ein Muster $(a_1, \ldots, a_k)$ ist dann zulässig, wenn die Zahlen $a_1, \ldots, a_k$ bei Division durch jede der Primzahlen $p \le k$ jeweils höchstens p-1 verschiedene Reste annehmen. Das Muster (0, 2, 4) erzeugt bei Division durch 3 alle drei möglichen Reste, ist also nicht zulässig, aber das Muster (0, 2, 6) ergibt bei Division durch 2 nur den Rest 0, und bei Division durch 3 nur die Reste 0 und 2, ist also zulässig.

[9] Hierbei bedeutet $f(N) \sim g(N)$, dass der Quotient $f(N)/g(N)$ gegen 1 geht, wenn N groß wird.

[10] Hier und im folgenden ist log der natürliche Logarithmus, der auch oft mit ln abgekürzt wird.

[11] Hierbei ist $\exp(x) = e^x$.

kann aber höchstens $\sqrt{N}(\log N)^2$ groß sein. Diese Schranken liegen also sehr nahe beieinander.

Satz 3: *Falls es eine Zerlegung A+B=P' gibt, wobei sich P' von der Menge der Primzahlen P nur an endlich vielen Stellen unterscheidet und wobei A und B mindestens je zwei Elemente enthalten, so gilt:*

$$c_1 \frac{\sqrt{N}}{(\log N)^3} \le A(N) \le c_2 \sqrt{N}(\log N)^2$$

mit positiven Konstanten c_1, c_2. Die gleichen Schranken gelten für $B(N)$.

Diese Methode erlaubt es auch, eine Reihe weiterer Resultate zu erzielen:

Satz 4: *Es gibt keine Menge P', die sich von den Primzahlen nur an endlich vielen Stellen unterscheidet, die als P'=A+B+C geschrieben werden kann, wobei die Mengen A, B und C jeweils mindestens zwei Elemente enthalten.*

Das multiplikative Analogon von Ostmanns Problem kann gelöst werden:

Satz 5: *Es gibt keine Menge P', die sich von den Primzahlen nur an endlich vielen Stellen unterscheidet, die als P'=AB+1 geschrieben werden kann, wobei die Mengen A und B mindestens je zwei Elemente enthalten.*

Satz 6: *Es gibt keine Menge P', die sich von den Primzahlen nur an endlich vielen Stellen unterscheidet, die als P'=A+B geschrieben werden kann, wobei A und B jeweils mindestens je zwei Elemente enthalten und wobei fast jede[12] Primzahl p genau eine Darstellung als p=a+b hat.*

Der letzte Satz ist z.B. von Interesse, weil man ja die Primzahlen der Form p≡1 mod 4 (bis auf die Reihenfolge) auf genau eine Weise als Summe von zwei Quadratzahlen schreiben kann. Eine Variante des Zweiquadratesatzes mit noch schöneren Eigenschaften kann man also nicht erwarten.

Lange Primzahlmuster

Wie beschrieben, wird vermutet, dass ein „zulässiges" Primzahlmuster $(n+a_1, n+a_2,\ldots,n+a_k)$ im Intervall [1,N] etwa

$$C_{(a_1,a_2,\ldots,a_k)} \frac{N}{(\log N)^k}$$

oft vorkommt. Auch wenn hierfür kein Beweis bekannt ist, so kann doch bewiesen werden, dass das Muster nicht sehr viel häufiger vorkommen kann:

Es gilt folgende obere Schranke

$$2^k k! C_{(a_1,a_2,\ldots,a_k)} \frac{N}{(\log N)^k}$$

für die Häufigkeit. Natürlich wären entsprechende untere Schranken für die Häufigkeit von größerem Interesse, weil sie ja die ungelösten Fragen beantworten würden. Es sind auch obere Schranken von Interesse, wenn die Länge k des Musters nicht konstant ist, sondern von der Intervalllänge N abhängen darf. Durch die Anwendung der neuen Siebmethode kann gezeigt werden, dass die obere Schranke der Form

$$N/(\log N)^k$$

in etwa richtig bleibt, so lange k< c log N/log log N gilt. Falls k noch größer ist, so geht die obere Schranke relativ schnell gegen $\sqrt{N}$. Auf der anderen Seite kann gezeigt werden, dass man diese Schranken auch nicht wesentlich verbessern kann. Es gibt nämlich Muster (die aber leider von der Intervalllänge N abhängen), für die die Länge und Häufigkeit des Musters nahe am erlaubten Maximum liegt. Insbesondere gibt es Mengen A und B mit mindestens log N/log log N vielen Elementen im Intervall [1,N], für die alle Summen aus A+B prim sind. Zum Beweis werden analytische Siebmethoden und kombinatorische Zählmethoden verwendet.

Primzahlen in dünnen Folgen

Wie beschrieben, ist die Menge der Primzahlzwillinge mit vermuteter Häufigkeit

$$\pi_2(N) \sim C \frac{N}{(\log N)^2}$$

bereits zu dünn, um sie mit heutigen Methoden zählen zu können. Vor wenigen Jahren erzielten Friedlander und Iwaniec ein spektakuläres Resultat bei einer noch viel dünneren Menge. Im Intervall [1,N] gibt es etwa $N^{3/4}$ viele Zahlen der Form $n=a^2+b^4$. Von dieser dünnen Menge bewiesen sie, dass sie Primzahlen mit der richtigen Häufigkeit enthält, d.h., dass etwa

$$\frac{N^{3/4}}{\log N}$$

dieser Zahlen prim sind. Dies war methodisch ein enormer Durchbruch, weil eine Reihe technischer Schwierigkeiten umgangen werden konnte. Verknüpft man dieses Ergebnis mit Methoden der Graphentheorie, so kann gezeigt werden, dass es Mengen A von Quadraten und B von vierten Potenzen gibt, so dass alle Kombinationen a^2+b^4 prim sind. Hierbei können die Mengen A und B im Intervall [1,N] mindestens logN/(2 log log N) viele Zahlen haben, können also fast genauso groß sein wie im vorigen Abschnitt ohne die Restriktion. Das folgende numerische Beispiel zeigt, dass diese Mengen auch algorithmisch ermittelt werden können. Für $A=\{35610^2, 82140^2, 114570^2, 601620^2, 819660^2, 945870^2, 1265820^2, 1319520^2, 1932720^2\}$ und $B=\{31^4, 61^4, 91^4, 121^4, 151^4, 181^4\}$ ist jedes Element aus A+B prim. Es wäre wünschenswert, den Ansatz von Friedlander und Iwaniec zu verallgemeinern, um auch Primzahlen der Form $27a^2+b^6$ bearbeiten zu können. Dies hätte nämlich Auswirkungen auf unser Wissen über elliptische Kurven, und dies wiederum hätte Anwendungen in der Kryptographie.[13]

Eine Anwendung auf ein Gitterpunktproblem

Wir haben bereits einiges Wissen über Primzahlen der Form $p=a^2+b^4$ und $p=a^2+b^2$ zusammengetragen. In diesem Abschnitt werden wir sehen, dass Mengen A und B von Quadraten, so dass alle Zahlen a^2+b^2 prim sind, Anwendungen haben können.

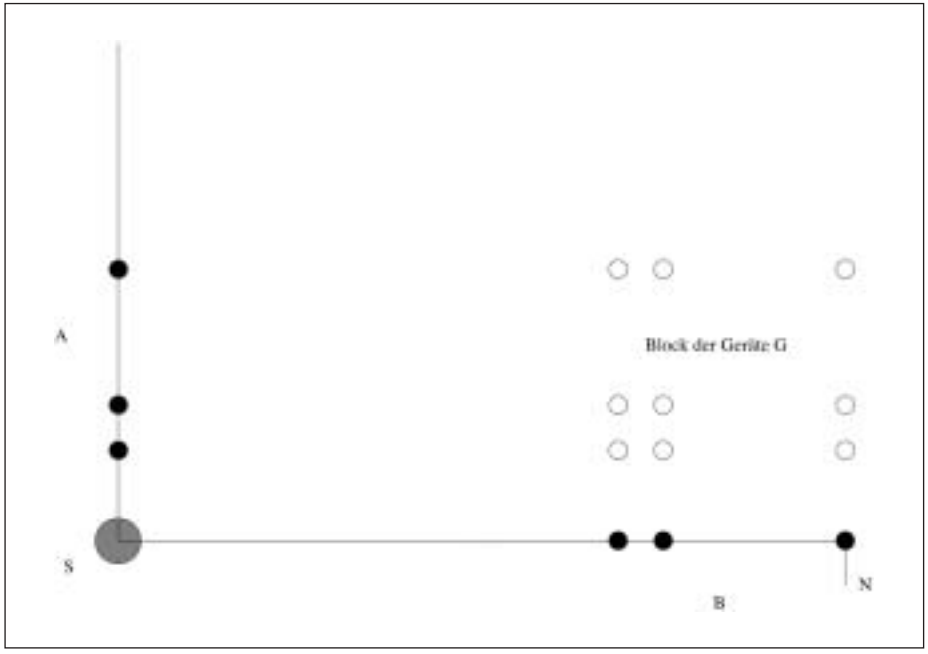
Es ist bekannt, dass manche angewandten Fragestellungen letztlich auf ein kombinatorisches Positionierungsproblem in der Ebene zurückgeführt werden können. Abstände zwischen Gitterpunkten der Ebene hängen aufgrund des Satzes von Pythagoras mit der Summe von zwei Quadraten ganzer Zahlen zusammen. Es ist also zu erwarten, dass eine gute Kenntnis derjenigen Zahlen, die als Summe von zwei Quadraten geschrieben werden können, bei ebenen Gitterpunktproblemen von Nutzen ist. Wir stellen ein idealisiertes Problem vor, bei dem wir technische Komplikationen vermeiden. Die Informationstheoretiker Golomb und Taylor berichten, dass ähnliche Probleme Anwendung bei der Signalverarbeitung von gemessenen Signalen haben.[14]

Nehmen wir an, dass eine Firma ein Messexperiment machen will oder dass ein Telekommunikationsunternehmen dauerhaft eine Reihe von Sendern und Empfängern positionieren will. (Ob es sich jeweils um Sender, Empfänger oder beides handelt, kann je nach Problem spezifiziert werden.) Dabei gebe es ein ausgezeichnetes (teures) Gerät S, das mit vielen anderen kleineren Geräten $G_1,\ldots,G_r$ kommunizieren soll. Wir legen das Gerät S in den Nullpunkt eines Koordinatensystems und die Geräte G_i als rechteckigen Block der Seitenlängen |A| bzw. |B| auf ganzzahlige Gitterpunkte. Wenn z.B. die Geräte die Koordinaten (1, 1), (1, 2), (2, 1) und (2, 2) haben, so ist vom Ursprung (0, 0) aus der Punkt (2, 2) durch den Punkt (1, 1) verdeckt. Außerdem ist der Weg von (2, 2) nach (0, 0) genau doppelt so weit wie von (1,1) aus. Das könnte den Nachteil haben, dass einerseits keine direkte Kommu- ▸

[12] „Fast jede Primzahl" heißt hier „jede Primzahl bis auf endlich viele Ausnahmen".

[13] Friedlander, J., Iwaniec, H.: Using a parity-sensitive sieve to count prime values of a polynomial. Proc. Natl. Acad. Sci. USA 94, 1054-1058, 1997.

[14] Golomb, S.W. und Taylor, H.: Two-dimensional Synchronization patterns for minimum ambiguity, IEEE Transactions on information theory 28, 1982, 600-604.
Bertram-Kretzberg, C. und Lefmann, H.: The algorithmic aspects of uncrowded hypergraphs. Siam J. Comp. 29, 1999, 201-230, Bemerkung vor Theorem 5.5.



nikation möglich ist und dass andererseits Interferenzen auftreten. Diese Gitteranordnung wäre also ungünstig.

Stellt man nun eine Wunschliste für eine gute Anordnung von Gitterpunkten zusammen, so sieht diese vielleicht wie folgt aus.

1) Blockanordnung der kleinen Geräte G_i aus Kostengründen.
2) Alle Richtungen vom Ursprung aus sind verschieden.
3) Alle Weglängen sind verschieden, wodurch bereits aus der Laufzeit eines Signals das Gerät eindeutig identifiziert ist.
4) Die Weglängen haben zueinander irrationale Verhältnisse, um Interferenzen zu vermeiden.

Diese Bedingungen lassen sich erfüllen, wenn die Geräte G_i in Punkten mit den Koordinaten (a_i, b_j) positioniert sind, wobei alle $a_i^2+b_j^2$ prim sind (siehe Graphik). Wie im vorhergehenden Abschnitt erläutert, ist dies sogar in einem viel schwierigeren Fall realisierbar. Ist eine der obigen Bedingungen nicht notwendig, kann sie einfach weggelassen werden. Es können sicher einige weitere Bedingungen zusätzlich gestellt werden. Ob sich diese dann mit obigem Ansatz behandeln lassen, hängt aber vom Einzelfall ab.

Hierbei handelt es sich also um ein Problem der diskreten ganzzahligen Optimierung, das mit kombinatorischen Methoden (u. a. Graphentheorie) konstruktiv gelöst werden kann.

Durch die Entwicklung neuer Methoden (bzw. durch die Kombination von Methoden aus verschiedenen mathematischen Gebieten) ist es gelungen, die Fragestellungen über Primzahlen weit voranzutreiben. Wie wir gesehen haben, sind die Methoden allgemein genug, um auch bei Fragen außerhalb der Zahlentheorie erfolgreich eingesetzt zu werden.

PD Dr. rer. nat. habil. Christian Elsholtz
Institut für Mathematik
Erzstraße 1
38678 Clausthal-Zellerfeld
Tel.: 05323/72-2406
Fax: 05323/72-2304
E-Mail:elsholtz@math.tu-clausthal.de
http://www.math.tu-clausthal.de/~mace/