AKDIS Zahlentheorie und Anwendungen (SS 2008)

> "…both Gauss and lesser mathematicians may be justified in rejoicing that there is one science [number theory] at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean."
>
> - G.H.Hardy, A Mathematician's Apology, 1940

Wie obiges Zitat des berühmten Mathematikers Hardy belegt, galt die Zahlentheorie bis vor gar nicht langer Zeit als eines der "reinsten", d.h. den Anwendungen am fernstehendsten Teilgebiete der Mathematik. Dieser Auffassung mochten auch noch jene Verantwortlichen gewesen sein, welche anfangs der 80-er Jahre, also am Ende der sog. "new math"-Ära an unseren Schulen, die als "Mengenlehre" diskredidierten und ohnehin spärlichen Ansätze zur Algebra und Zahlentheorie wieder aus den Lehrplänen entfernten. Es muss daher als eine besondere Ironie des Schicksals angesehen werden, dass etwa um diese Zeit die wenig Jahre zuvor erfundenen sog. Public Key Kryptosysteme einen wahren Siegeszug um die Welt antraten, welche zu einem gutem Teil auf einfachen und für die Schule durchaus zugänglichen Sätzen der Algebra und Zahlentheorie beruhten und somit auch jene "Anwendungen" des abstrakten Stoffes geboten hätten, welche viele bis dahin vermissten. Insgesamt kann gesagt werden, dass parallel zu der in letzten Jahrzehnten ungeheuer angestiegenen Computerisierung die gesamte Diskrete Mathematik und mit ihr vor allem auch die Zahlentheorie stark an Bedeutung für die Anwendungen gewonnen hat, sodass heute von deren "remoteness from ordinary human activities" wie vielleicht noch zu Hardy's Zeiten keine Rede mehr sein kann.

Eines der ersten Public Key Kryptosysteme und zugleich das heute mit Abstand wichtigste ist das RSA-Verfahren ($\rightarrow$ Derive-Demo), benannt nach ihren Erfindern R.L.Rivest, A.Shamir and L.Adleman, welches es 1978 veröffentlichten, und das uns als "Aufhänger" für eine Reihe von wichtigen zahlentheoretischen Problemstellungen dienen wird. Insbesondere werden dafür effiziente Algorithmen für die Bereitstellung großer Primzahlen benötigt("groß" bedeutete nach heutigen Standards ca. 155 Stellen oder auch mehr!), während die Sicherheit von RSA ganz wesentlich davon abhängt, dass man solche "effizienten" Algorithmen für die Zerlegung einer ganzen Zahl, welche das Produkt von zwei solchen Primzahlen etwa gleicher Größe ist, derzeit noch nicht kennt. (Zumindest nicht für herkömmliche Computer, wohl aber bereits für sog. Quantencomputer, so es diese jemals geben wird!)

Dieser Themenkreis – Primzahltests und Faktorisierungalgorithmen - ist heute der Gegenstand intensiver Forschung und er ist auch einer der Schwerpunkte dieser Vorlesung. Gauß hätte daran seine Freude gehabt, schrieb er doch in seinen "Disquisitiones Arithmeticae" (1801) die folgenden denkwürdigen Sätze:

"Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letzere in ihre Primfaktoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowie der alten wie auch der neuen Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren. Trotzdem muss man gestehen,

dass alle bisher angewendeten Methoden entweder auf spezielle Fälle beschränkt oder so mühsam und weitläufig sind, dass sie auf größere Zahlen meistenteils kaum angewendet werden können. Außerdem aber dürfte es die Würde der Wissenschaft erheischen, alle Hilfsmittel zur Lösung jenes berühmten Problems fleißig zu vervollkommnen."

Dies ist im Übrigen auch ein besonders schönes Beispiel für den sog. "Erkenntnisvorlauf" in der Mathematik. Damit ist der generelle Trend gemeint, dass mathematische Untersuchungen, die ursprünglich ausschließlich um ihrer selbst willen betrieben wurden – siehe dazu nochmals die Einleitung - irgendwann auch einmal für die Anwendungen relevant werden.

Bevor wir uns im Sinne des obigen Gaußschen Zitats an die Arbeit machen, wollen wir noch vorher einige für das Folgende aus der Zahlentheorie benötigten Grundtatsachen in einem eigenem Kapitel voranstellen - etwa im Ausmaß der ersten drei Kapitel des Buchs "Zahlentheorie" von Nöbauer-Wiesenbauer (Prugg-Verlag, Eisenstadt, 1981).

I. ZAHLENTHEORETISCHE GRUNDLAGEN

§1. Teilbarkeit im Ring der ganzen Zahlen

Def. 1.1: Seien $a,b \in \mathbf{Z}$ (= Menge der ganzen Zahlen). Man sagt dann "a ist Teiler von b" (oder "b ist Vielfaches von a"), i.Z. $a \mid b$, falls es ein $u \in \mathbf{Z}$ gibt, sodass $au = b$. Ein solches u (welches für $a \neq 0$ stets eindeutig bestimmt ist!) wird Komplementärteiler zu a genannt.

Einige einfache Eigenschaften des Teilbarkeitsbegriffs, welche mehr oder weniger unmittelbar aus der Definition folgen, sind zusammengestellt in

Satz 1.2: Für beliebige $a,b,c,d \in \mathbf{Z}$ gilt:

(1) $\pm 1, \pm a$ sind stets Teiler von a (die sog. "trivialen Teiler" von a).

(2) Es gilt stets $a \mid 0$, jedoch $0 \mid a$ nur für $a = 0$.

(3) Die einzigen Teiler von 1 sind ± 1.

(4) $a \mid b \wedge b \mid c \Rightarrow a \mid c$ (Transitivität von $\mid$).

(5) $a \mid b \Rightarrow ac \mid bc$, wobei für $c \neq 0$ auch die Umkehrung gilt.

(6) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$ (Verträglichkeit von $\mid$ und $\cdot$)

(7) $a \mid b \wedge b \mid a \Rightarrow a = \pm b$.

(8) $a \mid b \wedge a \mid c \Rightarrow \forall\, x,y \in \mathbf{Z}$: $a \mid (xb+yc)$.

(9) $a \mid b \Leftrightarrow |a| \mid |b|$.

(10) $a \mid b \wedge b \neq 0 \Rightarrow -|b| \leq a \leq |b|$.

Nicht ganz so trivial, aber für das folgende sehr wichtig ist

Satz 1.3: Seien a,b ∈ **Z** und b ≠ 0 beliebig. Es gibt dann eindeutig bestimmte und in endlich vielen Schritten berechenbare Zahlen q,r ∈ **Z** (genannt "Quotient" bzw. "Rest" bei der "Division von a durch b"), sodass

$$a = qb + r \text{ und } 0 \le r < |b|.$$

Def 1.4: Seien a,b ∈ **Z**. d ∈ **N** (= Menge der natürlichen Zahlen inkl. 0) heißt dann größter gemeinsamer Teiler von a und b, i.Z. d = ggT(a,b), wenn gilt:

(1) $d \mid a \wedge d \mid b$ (d.h. d ist "gemeinsamer Teiler von a und b").

(2) $\forall\, t \in \mathbf{Z}: t \mid a \wedge t \mid b \Rightarrow t \mid d$.

Ist dabei speziell d = 1, so heißen a und b teilerfremd.

Bem. 1.5: (1) Aus 1.2(10) und 1.4(2) folgt sofort, dass d in obiger Definition außer für a = b = 0 tatsächlich "größter" gemeinsamer Teiler (im Sinne der natürlichen Ordnung ≤) ist. Daraus oder auch aus 1.2(7) und 1.4(2) folgt insbesondere auch die Eindeutigkeit des ggT(a,b).

(2) Allgemeiner ist in Analogie zu 1.4. der $\text{ggT}(a_1,a_2,...,a_n)$ von $a_1,a_2,...,a_n \in \mathbf{Z}$ definiert als gemeinsamer Teiler von $a_1,a_2,...,a_n$, der von jedem anderen gemeinsamen Teiler von $a_1,a_2,...,a_n$ geteilt wird.

Zur Frage der Existenz von größten gemeinsamen Teilern in **Z** gilt

Satz 1.6: Für beliebige a,b ∈ **Z** existiert d = ggT(a,b) und es gibt darüberhinaus x,y ∈ **Z**, sodass d = xa +yb, d.h., d ist als Linearkombination von a und b über **Z** darstellbar.

Bem. 1.7: Zur Bestimmung von d = ggT(a,b) bzw. der ganzen Zahlen x,y mit d= xa + yb wird üblicherweise der sog. Euklidische Algorithmus verwendet. Wegen ggT(a,b) = ggT(b,a), ggT(a,0) = $|a|$ und ggT(a,b) = ggT($|a|,|b|$) genügt es dabei den Fall a ≥ b > 0 zu betrachten. Man stellt dazu folgendes Divisionsschema auf, was aufgrund der streng absteigenden Reste in den nachfolgenden Divisionen sicher stets möglich ist:

$$\begin{aligned}
a &= q_1 b + r_1 \text{ mit } 0 < r_1 < b,\\
b &= q_2 r_1 + r_2 \text{ mit } 0 < r_2 < r_1,\\
&\dots\\
r_{i-2} &= q_i r_{i-1} + r_i \text{ mit } 0 < r_i < r_{i-1},\\
&\dots\\
r_{n-2} &= q_n r_{n-1} + r_n \text{ mit } 0 < r_n < r_{n-1},\\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

Setzt man noch $r_{-1} := a$ und $r_0 := b$, so sieht man leicht, dass r_n, d.h. der letzte nichtverschwindende Rest, die Bedingungen (1) und (2) aus 1.4 für den ggT(a,b) erfüllt. Ferner können auch x,y leicht mittels der durch

$$\begin{aligned}
x_{-1} &= 1,\ x_0 = 0,\ x_i = x_{i-2} - q_i x_{i-1}\\
y_{-1} &= 0,\ y_0 = 1,\ y_i = y_{i-2} - q_i y_{i-1}
\end{aligned}$$

rekursive definierten Folgen (x_i) und (y_i) gefunden werden, indem man $x := x_n$ und $y := y_n$ setzt. (Beachte: Alle 3 Folgen $(x_i),(y_i)$ und (r_i) genügen der gleichen

Rekursion, aber mit jeweils verschiedenen Startwerten!) Obige Methode zur Auffindung von x und y wird auch Erweiterter Euklidischer Algorithmus (EEA) oder Berlekamp-Algorithmus genannt. Insgesamt ist der Euklidische Algorithmus einer der schnellsten Algorithmen, welche die Mathematik kennt ($\rightarrow$ Derive-Demo), wie sich auch aus dem nachfolgenden Satz unmittelbar ergibt.

Satz 1.8: Die Anzahl der notwendigen Divisionen für den Euklidischen Algorithmus für ganze Zahlen a,b mit $a \geq b > 0$ ist $\leq {}_{\lambda}\log a$ mit $\lambda = (1+\sqrt{5})/2$, d.h. sie wächst nur linear mit der Stellenanzahl von a.

Bem. 1.9: Es ist ${}_{\lambda}\log a \approx 4.8 \cdot {}_{10}\log a$. Die Durchschnittsanzahl der notwendigen Divisionen beträgt jedoch nur etwa $1.94 \cdot {}_{10}\log a$. Stellt man ferner in Rechnung, dass der Aufwand für die Divisionen höchstens quadratisch mit der Stellenanzahl von a wächst, so wächst die Anzahl der Elementarrechenoperationen wie $O(({}_{10}\log a)^3)$, d.h. es liegt jedenfalls ein sog. Polynomialzeitalgorithmus vor. Tatsächlich sind aber die auftretenden Quotienten (mit ev. Ausnahme des ersten!) beim Euklidischen Algorithmus gewöhnlich so klein, dass die Divisionen in der Regel durch eine geringe Anzahl von Subtraktionen des Divisors vom Dividenden ersetzt werden können, was den Gesamtrechenaufwand weiter auf $O(({}_{10}\log a)^2)$ verringert.

Gemeinsame Teiler von a und b kann man aus dem ggT(a,b) gewissermaßen "herausheben". Genauer gilt

Satz 1.10: Seien $a,b \in \mathbf{Z}$. Für jeden gemeinsamen Teiler $t > 0$ von a und b gilt dann $ggT(a,b) = t\ ggT(a/t,b/t)$. Insbesondere ist t genau dann ggT(a,b), wenn gilt $ggT(a/t,b/t)=1$.

Sehr häufig verwendet wird im folgenden

Satz 1.11: ("Lemma von Euklid") Für beliebige $a,b,c \in \mathbf{Z}$ gilt:

$$a \mid bc \wedge ggT(a,b)=1 \Rightarrow a \mid c.$$

In Analogie zur Definition des ggT(a,b) in 1.4 definiert man das kgV(a,b) in folgender Weise:

Def. 1.12: Seien $a,b \in \mathbf{Z}$. $v \in \mathbf{N}$ heißt dann ein kleinstes gemeinsames Vielfaches von a und b, i.Z. v = kgV(a,b)), wenn gilt:

(1) $a \mid v \wedge b \mid v$ (d.h. v ist "gemeinsames Vielfaches von a und b").

(2) $\forall\ w \in \mathbf{Z}$: $a \mid w \wedge b \mid w \Rightarrow v \mid w$.

Das in 1.5 Bemerkte gilt mutatis mutandis auch für obige Definition. Die Frage der Existenz von kleinsten gemeinsamen Vielfachen kann auf die von größten gemeinsamen Teilern in folgender Weise zurückgeführt werden:

Satz 1.13: Für beliebige $a,b \in \mathbf{Z}$ existiert v = kgV(a,b) und es ist

$$v = \begin{cases} 0, \text{falls } a = b = 0 \\ |ab| / ggT(a,b) \text{ sonst} \end{cases}$$

Daraus ergibt sich insbesondere die wichtige

Folgerung 1.14: Für beliebige $a,b,c \in \mathbf{Z}$ gilt:

$$a \mid c \wedge b \mid c \wedge ggT(a,b) = 1 \Rightarrow ab \mid c.$$

Für das Folgende grundlegend ist

Def. 1.15: Eine natürliche Zahl p > 1 heißt Primzahl, wenn sie nur die trivialen Teiler (s. 1.2(1)) besitzt. Die Menge der Primzahlen wird mit **P** bezeichnet.

Eine wichtige Eigenschaft von Primzahlen, welche diese sogar charakterisiert, ist der Inhalt von

Satz 1.16: Eine natürliche Zahl p > 1 ist genau dann Primzahl, wenn gilt:

$$\forall\, a,b \in \mathbf{Z}\colon p \mid ab \Rightarrow p \mid a \vee p \mid b\,.$$

Dieser Satz lässt sich natürlich sofort auf beliebige endliche Produkte verallgemeinern. Insbesondere lässt sich damit leicht zeigen, dass die Primzahlen die multiplikativen Bausteine von **N*** (= Menge der natürlichen Zahlen ohne 0) bilden oder in der Sprache der Algebra: (**N***, ·) ist eine freie Halbgruppe mit **P** als Basis, d.h. es gilt

Satz 1.17: (Hauptsatz der Elementaren Zahlentheorie) Jedes $n \in \mathbf{N}^*$ lässt sich in bis auf die Reihenfolge der Faktoren eindeutiger Weise als Produkt von Primzahlen schreiben.

Bem. 1.18: Aus vorstehendem Satz folgt insbesondere sofort, dass sich jedes $n \in \mathbf{N}^*$ auf genau eine Art in der Form

$$n = \prod_{p \in \mathbf{P}} p^{\nu_p} \quad (\nu_p \in \mathbf{N},\ \nu_p > 0 \text{ nur für endlich viele } p \in \mathbf{P})$$

schreiben lässt, wobei die Primzahlen p in aufsteigender Reihenfolge durchlaufen werden. (Das rechtsstehende formal unendliche Produkt ist natürlich als entsprechendes endliches Produkt über die von 1 verschiedenen Faktoren zu interpretieren. Das "leere Produkt" ist dabei wie üblich als 1 definiert.)

Mit der in 1.18 eingeführten Notation gilt dann:

Satz 1.19: Seien $a,b \in \mathbf{Z} \setminus \{0\}$ und

$$|a| = \prod_{p} p^{\alpha_p} \text{ bzw. } |b| = \prod_{p} p^{\beta_p}$$

die Primfaktorzerlegungen ihrer Absolutbeträge. Es gilt dann

$$a \mid b \Leftrightarrow \forall p \in \mathbf{P}\colon \alpha_p \le \beta_p\,.$$

Insbesondere ist daher

$$ggT(a,b) = \prod_{p \in \mathbf{P}} p^{\min(\alpha_p,\beta_p)} \text{ und } kgV(a,b) = \prod_{p \in \mathbf{P}} p^{\max(\alpha_p,\beta_p)}\,.$$

Eine weitere einfache Folgerung aus 1.17 ist

Satz 1.20: Ist ggT(a,b)=1 und ggT(a,c) = 1, dann auch ggT(a,bc)=1 für beliebige ganze Zahlen a,b,c.

Wir wenden uns nun Fragen der Primzahlenverteilung zu und beginnen mit dem klassischen

Satz 1.21: (Euklid) Es gibt keine größte Primzahl, d.h. **P** ist unendlich.

Bezeichnet man mit $\pi(x)$ für jede reelle Zahl $x > 0$ die Anzahl der Primzahlen $\leq x$, so gilt der folgende bereits von Legendre und Gauß vermutete, jedoch erst 1896 von Hadamard und de la Vallée Poussin unabhängig voneinander bewiesene

Satz 1.22: (1.Primzahlsatz) $\pi(x)$ kann asymptotisch dargestellt werden durch $x/\ln x$, i.Z. $\pi(x) \sim x/\ln x$, d.h. es gilt $\lim_{x\to\infty} \pi(x) / (x / \ln x) = 1$.

Eine im allgemeinen noch bessere Näherung für $\pi(x)$ ist der sog. Integrallogarithmus

$$\mathrm{li}(x) := \int_0^x dt / \ln t \, .$$

(Gelegentlich wird hier als untere Grenze des Integrals auch 2 genommen, um die Singularität bei t=1 zu vermeiden, doch ist die Differenz von ≈ 1.045 für unsere Zwecke irrelevant.) Auch mit dieser Näherung gilt wieder

Satz 1.23: (2.Primzahlsatz) $\pi(x) \sim \mathrm{li}(x)$, d.h. $\pi(x)$ kann asymptotisch dargestellt werden durch $\mathrm{li}(x)$.

Bem 1.24: Speziell in der 2. Version des Primzahlsatzes wird besonders deutlich, dass die "Primzahldichte" in der Nähe einer positiven reellen Zahl x etwa $1/\ln x$ beträgt. So sollte z.B. in der Nähe von 10^{100} wegen $\ln 10^{100} \approx 230.3$ etwa jede 230-ste Zahl eine Primzahl sein. Versucht man also durch zufälliges Herausgreifen eine etwa 100-stellige Primzahl zu bestimmen, so muss man mit mehreren hundert Fehlversuchen rechnen.

Bem. 1.25: (Riemannsche Vermutung) Für viele Fragen der Primzahlverteilung spielt die die Riemann benannte ζ-Funktion eine große Rolle. Sie ist zunächst nur für $s \in \mathbf{C}$ (= Menge der komplexen Zahlen) mit $\mathrm{Re}(s) > 1$ definiert und zwar durch die konvergente Reihe

$$\zeta(s) = \sum_{n=1}^{\infty} 1/n^s \, ,$$

lässt sich aber auf die gesamte komplexe Zahlenebene analytisch fortsetzen mit Ausnahme eines Pols von der Ordnung 1 bei s=1. Die Riemannsche Vermutung, nach dem Urteil vieler Mathematiker das herausragendste ungelöste Problem der Mathematik, besagt nun, dass die Nullstellen von ζ im sogenannten "kritischen Streifen" $0 \leq \mathrm{Re}(s) \leq 1$ alle den Realteil 1/2 haben, d.h. auf dessen Mittelgeraden liegen ($\rightarrow$ Derive-Demo). Für die ersten 10 Billionen absolut kleinsten Nullstellen ist dies tatsächlich erfüllt, wie X.Gourdon und P.Demichel im Okt. 2004 basierend auf einen neuen Algorithmus von Odlyzko und Schönhage nachgewiesen haben.

Die gleiche Vermutung ausgesprochen für die sog. Dirichletschen L-Funktionen, welche für $\mathrm{Re}(s) > 1$ definiert sind durch

$$L_\chi(s) = \sum_{n=1}^{\infty} \chi(n) / n^s$$

(sonst wieder durch analytische Fortsetzung), wobei die Funktionen χ: $\mathbf{Z} \rightarrow \mathbf{C}$ sog. "Charaktere" auf $\mathbf{Z}$ sind, welche später erklärt werden, wird auch "Verallgemeinerte Riemannsche Vermutung" genannt.