

Vorlesung Einführung in die Zahlentheorie

ez2: Hauptsatz der Arithmetik

Stichworte: Primzahl, Unendlichkeit der Primzahlfolge, Sieb des Eratosthenes, Lemma von Euklid, Satz von der eindeutigen PFZ/Hauptsatz der Arithmetik, Primfaktorzerlegung, PFZ des ggT und kgV

2.1. Einführung:

Die Primzahlen als multiplikative Bausteine der ganzen Zahlen bilden eine wichtige Teilmenge von $\mathbb{N}$. Der Hauptsatz der Arithmetik besagt, dass jede natürliche Zahl in ein Produkt von Primzahlen zerlegt ("faktorisiert") werden kann, wobei die Darstellung bis auf die Reihenfolge der Primfaktoren eindeutig ist.

- 2.2. Def.: (1) $p \in \mathbb{N}$ heißt Primzahl (oder prim), wenn $p > 1$ ist und nur die natürlichen Teiler 1 und p besitzt (d.h. wenn die Anzahl der natürlichen Teiler von p gleich 2 ist).
 $\mathbb{P} := \{p \in \mathbb{N}; p \text{ prim}\}$ ist die Menge aller Primzahlen, also $\mathbb{P} = \{2, 3, 5, 7, 11, 13, \dots\}$.
 (2) $m \in \mathbb{N} \setminus \{1\}$ heißt zusammengesetzt, wenn m keine Primzahl ist.

Wir zeigen nun auf 3 verschiedene Weisen die Unendlichkeit von $\mathbb{P}$.

- 2.3. Satz (Unendlichkeit von $\mathbb{P}$): Es existieren unendlich viele Primzahlen, d.h. $\#\mathbb{P} = \infty$.
 2.4. 1. Bew. (nach Euklid): Jedes $n \in \mathbb{N} \setminus \{1\}$ besitzt mindestens einen Primteiler (also Teiler, der Primzahl ist), z.B. den kleinsten Teiler d von n mit $1 < d \leq n$.

Sei $k \in \mathbb{N}$ und seien $p_1, \dots, p_k \in \mathbb{P}$ verschiedene Primzahlen.

Dann ist jeder Primteiler von $n := 1 + p_1 \cdots p_k > 1$ von $p_1, \dots, p_k$ verschieden.

┌ Denn aus $q \in \mathbb{P}$ mit $q | n$ und $q = p_i$ folgte $q | n - p_1 \cdots p_k = 1$, $\nexists$. ┘

Auf diese Weise können unendlich viele Primzahlen gewonnen werden. $\square$

- 2.5. Bem.: $a_m := p_1 \cdots p_m + 1$ ist Primzahl für $m \leq 5$, aber nicht allgemein:

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509 \text{ ist zusammengesetzt!}$$

2.6. Bem.: $p_n \leq 2^{2^{n-1}}$: I.A.: $p_1 = 2 = 2^{2^0}$, $p_{n+1} \stackrel{\text{Euklid}}{\leq} p_1 \cdots p_n + 1 \stackrel{\text{I.V.}}{\leq} 2^{1+2^1+2^2+\dots+2^{n-1}} + 1 = 2^{2^n} + 1 \leq 2^{2^{n+1}} = 2^{2^{(n+1)-1}}$ ✓
 Also: $\#\{p \leq 2^{2^{n-1}}\} \geq n$, und $\#\{p \leq x\} \geq \log_2 \log_2(x) + 1 \geq \log \log(x) \xrightarrow{x \rightarrow \infty} \infty$. (Miserable Abschätzung!)

2.7. 2. Beweis (nach Euler): Angenommen, es gibt ein $k \in \mathbb{N}$ und $p_1, \dots, p_k$ prim so, dass $\mathbb{P} = \{p_1, \dots, p_k\}$, d.h. $p_1, \dots, p_k$ seien alle Primzahlen. Dann ist das Produkt
$$\prod_{p \in \mathbb{P}} (1 - \frac{1}{p})^{-1} = \prod_{p \in \mathbb{P}} \sum_{l=0}^{\infty} (\frac{1}{p})^l$$
 konvergent, da es endlich ist.

Mit dem Satz 2.14 zur Eindeutigkeit der PFZ (= Hauptsatz der Arithmetik), zu dessen Beweis die Unendlichkeit der Primzahlenmenge nicht benutzt wird (!), sieht man, dass das (Cauchy-)Produkt mit $\sum_{n=1}^{\infty} \frac{1}{n}$ übereinstimmt. Die Divergenz der harmonischen Reihe $1 + \frac{1}{2} + (\frac{1}{3} + \frac{1}{4}) + (\frac{1}{5} + \dots + \frac{1}{8}) + (\frac{1}{9} + \dots + \frac{1}{16}) + (\frac{1}{17} + \dots)$ ergibt einen Widerspruch. $\square$
 $\underbrace{2 \cdot \frac{1}{4} = \frac{1}{2}}_{> 2 \cdot \frac{1}{4} = \frac{1}{2}} \quad \underbrace{(\frac{1}{5} + \frac{1}{8})}_{> 4 \cdot \frac{1}{18} = \frac{1}{2}} \quad \underbrace{(\frac{1}{9} + \dots + \frac{1}{16})}_{> 8 \cdot \frac{1}{16} = \frac{1}{2}} \quad \underbrace{(\frac{1}{17} + \dots)}_{> 16 \cdot \frac{1}{32} = \frac{1}{2}} \dots$

2.8. 3. Beweis (mit Fermatzahlen): Im Zusammenhang mit der Frage nach der Konstruierbarkeit des regulären n -Ecks ($n \in \mathbb{N}$) mit Zirkel und Lineal taucht das Problem auf, welche der Zahlen $2^m + 1$ mit $m \in \mathbb{N}$ prim sind. (Vgl. Vorlesung Algebra, A26.13 ff.) Weil für alle $k \in \mathbb{N}$ und $l \in \mathbb{N}$ mit $2 \nmid l$ gilt, dass $2^{kl} + 1 = (2^k + 1) \cdot (2^{k(l-1)} - 2^{k(l-2)} + \dots + 1)$ zerlegbar ist, kann dies nur der Fall sein, wenn m selbst eine 2er-Potenz ist. Die Zahlen $F_n := 2^{2^n} + 1$ mit $n \in \mathbb{N}_0$ heißen Fermat-Zahlen.

Beh.: Diese Zahlen sind paarweise teilerfremd: $\forall m, n \in \mathbb{N}, m \neq n: (F_m, F_n) = 1$.

ü

Jede unendliche Folge paarweise teilerfremder Zahlen liefert unendlich viele Primzahlen. $\square$

2.9. Bem.: Die Tatsache, dass $F_1, \dots, F_4$ prim sind, führte Fermat zur Vermutung, dass dies für alle F_n zutrifft. Euler konnte dies durch die Zerlegung $F_5 = 641 \cdot 6700417$ widerlegen. Ebenso sind F_6, F_7, F_8 Produkte aus zwei Primzahlen. Bis heute ist kein weiteres primales F_n bekannt. Aber auch nicht, ob es unendlich viele zusammengesetzte Fermatzahlen gibt.

Ein einfaches Verfahren zur Aufstellung von Primzahl Listen / Primzahlüberprüfung ist folgender

2.10. Algorithmus (Sieb des Eratosthenes): Sei $N \in \mathbb{N} \setminus \{1\}$.

1) Schreibe die Zahlen $2, 3, \dots, N$ auf.

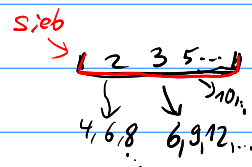
2₁) Streiche die echten Vielfachen von 2. ("Fallen durch das Sieb")

2₂) Gehe zur nächsten nicht gestrichenen Zahl

und streiche hiervon alle echten Vielfachen usw. ("Fallen durch das Sieb")

3) Stoppe, wenn die nächste ungestrichene Zahl $> \sqrt{N}$ ist.

Ergebnis/Beh.: Die nicht gestrichenen Zahlen ("die im Sieb behielten") sind genau alle Primzahlen $\leq N$.



Korrektheit/Bew.: Es geht keine Primzahl verloren, denn es werden nur echte Vielfache von Zahlen ≥ 2 gestrichen.

• Jedes zusammengesetzte $n \in \mathbb{N}$ mit $n \leq N$ wird gestrichen, denn es hat einen Primteiler $p \leq \sqrt{n}$.

(Hätte n sonst nur Primteiler $> \sqrt{n}$, etwa p_1 und p_2 , wäre bereits $p_1 \cdot p_2 > (\sqrt{n})^2 = n$ s.)

• Ein $p \leq \sqrt{N}$ wird nicht gestrichen, jedes n als echtes Vielfaches von p wird gestrichen ("fällt durch das Sieb"). $\square$

2.11. Bsp.: 101 ist prim, denn $\sqrt{101} \approx 10.05$, haben ≤ 10 die PZn $2, 3, 5, 7 \nmid 101$ $\neg 2, 3, 5 \mid 101$, $7 \nmid 14 \cdot 7 + 3 = 101$

2.12. Bsp.: Die Primzahlen zwischen 1 und 30 erzeugt man mit den kleinen PZn $p \leq \sqrt{30} \approx 5.5$ so:

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20,

21, 22, 23, 24, 25, 26, 27, 28, 29, 30 Ungestrichen: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

Mit diesem Verfahren werden insbesondere die Primzahlen im großen Bereich

zwischen $\sqrt{N}$ und N effektiv gefunden. (Dann damit die zwischen N und N^2 , weiter zw. N^2 und N^4 ...)

Wir zeigen jetzt den Hauptsatz der Arithmetik, der grundlegend zur multiplikativen Struktur von $\mathbb{Z}$ ist.

Ein Hilfssatz zum Beweis ist folgendes Lemma, das das Lemma von Bézout 1.13 benutzt.

2.13. Lemma von Euklid: $p \in \mathbb{N} \setminus \{1\}$ ist genau dann eine Primzahl, wenn gilt:

$$\forall a, b \in \mathbb{N}: (p \mid ab \Rightarrow p \mid a \vee p \mid b).$$

Bew.: " $\Rightarrow$ ": Sei $p \in \mathbb{P}$, seien $a, b \in \mathbb{N}$ mit plb . Ist $d := (p, a) > 1$, so muss $d = p$ sein.

Dann folgt $pl a$. Im Fall $(p, a) = 1$ folgt $pl b$ nach dem Gauß Lemma 1.16. (2).

" $\Leftarrow$ ": Sei $m \in \mathbb{N} \setminus \{1\}$ zusammengesetzt. Dann gibt es $n_1, n_2 \in \mathbb{N} \setminus \{1\}$ mit $m = n_1 n_2$.

mit Bezout!

Insbesondere gilt $m | n_1 n_2$. Wegen $n_1 > 1, n_2 > 1$ ist $m > \max\{n_1, n_2\}$, so dass $m \nmid n_1$ und $m \nmid n_2$. $\square$

2.14. Satz von der eindeutigen Primfaktorzerlegung / Hauptsatz der Arithmetik:

Jedes $n \in \mathbb{N}, n > 1$, besitzt genau eine Darstellung

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

mit $r \in \mathbb{N}, e_1, \dots, e_r \in \mathbb{N}$ und $p_1, \dots, p_r \in \mathbb{P}$ mit $p_1 < p_2 < \dots < p_r$.

Anders formuliert: Es gibt genau eine Funktion $\alpha: \mathbb{P} \times \mathbb{N} \rightarrow \mathbb{N}_0, (p, m) \mapsto \alpha_{p,m}$

mit $n = \prod_{p \in \mathbb{P}} p^{\alpha_{p,n}}$ für alle $n \in \mathbb{N}$. Dabei ist das Produkt über alle Primzahlen erstreckt, und $\alpha_{p,n} \neq 0$ gilt bei festem n nur für endlich viele $p \in \mathbb{P}$.

2.15. Bem.: Es ist $\alpha_{p,n} = 0$ für alle $p \in \mathbb{P}$.

2.16. Def.: Die Darstellung in 2.14 heißt Primfaktorzerlegung (Kurz: PFZ) bzw. kanonische Zerlegung.

2.17. Bem.: Obwohl der Satz von der eind. PFZ intuitiv wesentlich früher benutzt wurde, ist er erst von Gauß in exakter Form angegeben (und bewiesen) worden.

• $\mathbb{N} \cong \prod_{p \in \mathbb{P}} \mathbb{N}_0^{(p)} = \{(e_p)_{p \in \mathbb{P}}; e_p \in \mathbb{N}_0, e_p = 0 \text{ für alle } p \text{ bis auf endlich viele Ausnahmen}\}.$

2.18. Bew. (von 2.14): 1. Existenz: Der Beweis verläuft induktiv.

Falls $m \in \mathbb{N}$ nicht prim ist, zerfällt es in zwei Faktoren $m_1, m_2 \in \mathbb{N} \setminus \{1\}$ mit $m = m_1 m_2$.

Wegen $\min\{m_1, m_2\} > 1$ und $m = m_1 m_2$ ist $\max\{m_1, m_2\} < m$.

Nach Induktionsvoraussetzung sind m_1 und m_2 Produkte von Potenzen von Primzahlen.

Also ist auch $m = m_1 m_2$ ein Produkt aus Potenzen von Primzahlen.

2. Eindeutigkeit: Es gebe Zahlen mit (mind.) zwei Darstellungen, sei $m \in \mathbb{N} \setminus \{1\}$ die kleinste unter diesen. Seien $p_1, \dots, p_k \in \mathbb{P}$, $q_1, \dots, q_\ell \in \mathbb{P}$ und $\alpha_1, \dots, \alpha_k \in \mathbb{N}$, $\beta_1, \dots, \beta_\ell \in \mathbb{N}$ mit $m = p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_\ell^{\beta_\ell} \quad (*)$.

Es ist $p_i \neq q_j$ für alle $j \leq \ell$, da sonst in $(*)$ durch p_i dividiert werden könnte und man ein kleineres $\tilde{m}$ mit zwei Darstellungen erhielte. Also ist $(p_i, q_j) = 1$ (wäre dies > 1 , folgte $p_i = q_j \cdot \tilde{q}$).

Aus $(*)$ folgt nun: $p_1 \mid (q_1^{\beta_1-1} \cdot q_2^{\beta_2} \dots q_\ell^{\beta_\ell}) = q_1^{\beta_1-1} \cdot q_2^{\beta_2} \dots q_\ell^{\beta_\ell} \cdot \tilde{m}$, wo $\tilde{m} := q_1^{\beta_1-1} \cdot q_2^{\beta_2} \dots q_\ell^{\beta_\ell}$.

Beacht! $\rightarrow$

Aus dem Euklid-Lemma 2.13 und $(p_1, q_1) = 1$ folgt nun $p_1 \mid \tilde{m}$.

Dies lässt sich fortführen. Das führt schließlich zu $p_1 \mid q_\ell$, was wegen $(p_1, q_\ell) = 1$ ausgeschlossen ist. $\square$

2.19. Hinweis/Vereinbarung: Wird im Folgenden $m = p_1^{e_1} \dots p_r^{e_r}$ oder $m = \prod_{p \in \mathbb{P}} p^{e_p}$ geschrieben, so ist stets die eindeutige PFZ im Sinne von 2.14 gemeint. Die Abhängigkeit der p_j bzw. r und $e_1, \dots, e_r$ bzw. e_p von m wird nicht mehr explizit genannt.

2.20. Bem.: Für $m, d \in \mathbb{N}$ mit $m = \prod_{p \in \mathbb{P}} p^{a_p}$ und $d = \prod_{p \in \mathbb{P}} p^{b_p}$ gilt: $d \mid m \Leftrightarrow \forall p: b_p \leq a_p$.

Bew.: " $\Leftarrow$ ": $\checkmark$

" $\Rightarrow$ ": Es gelte $d \mid m$ und $b_p > a_p$ für (mindestens) ein $p \in \mathbb{P}$.

Seien $m := \frac{m}{d}$ und $c := \frac{d}{p^{b_p}}$, mit $m, c \in \mathbb{N}$.

Damit folgt $m = md = m c p^{b_p}$, und somit $m p^{-a_p} = c p^{b_p - a_p} m$.

Auf der l.S. steht eine nat. Zahl, in deren PFZ p nicht vorkommt,

während p auf der r.S. mit einem Exponenten von mindestens $b_p - a_p > 0$ auftritt.

Dies widerspricht dem Satz von der eind. PFZ 2.14. $\square$

2.21. Kor.: Es gilt: $\# \{d \in \mathbb{N}; d \mid \prod_{j=1}^k p_j^{a_j}\} = \prod_{j=1}^k (a_j + 1)$.

Bsp.: $\# \{d \mid 7^2 \cdot 5^7 \cdot 11^{12}\} = 3 \cdot 8 \cdot 13$

2.22. Kor. (PFZen von ggt und kgV):

Seien $k \in \mathbb{N}$, $n_j = \prod_{p \in \mathbb{P}} p^{e_{p,j}}$ geg. für $j=1, \dots, k$. Seien $A_p := \min \{e_{p,j} ; j \leq k\}$
und $B_p := \max \{e_{p,j} ; j \leq k\}$.

Dann gilt $(n_1, \dots, n_k) = \prod_{p \in \mathbb{P}} p^{A_p}$ und $[n_1, \dots, n_k] = \prod_{p \in \mathbb{P}} p^{B_p}$.

Bew.: Zum ggt: Nach Bem. 2.20 ist $\prod_{p \in \mathbb{P}} p^{A_p}$ für alle $j \leq k$ ein Teiler von n_j .

Ist $c := \prod_{p \in \mathbb{P}} p^{\alpha_{p,c}}$ nun ein gemeinsamer Teiler der $n_1, \dots, n_k$,
so ist $\alpha_{p,c} \leq e_{p,j}$ für alle $j \leq k$ und $p \in \mathbb{P}$.

Bem. 2.20 zeigt $c \mid \prod_{p \in \mathbb{P}} p^{A_p}$, und mit Folgerung 1.14(1) folgt $(n_1, \dots, n_k) = \prod_{p \in \mathbb{P}} p^{A_p}$.

Zum kgV: Nach Bem. 2.20 ist $\prod_{p \in \mathbb{P}} p^{B_p}$ für alle $j \leq k$ ein Vielfaches von n_j .

Ist $m := \prod_{p \in \mathbb{P}} p^{\alpha_{p,m}}$ nun ein gemeinsames Vielfaches der $n_1, \dots, n_k$,
so ist $\alpha_{p,m} \geq e_{p,j}$ für alle $j \leq k$ und $p \in \mathbb{P}$.

Damit folgt $\alpha_{p,m} \geq B_p = \max \{e_{p,j} ; j \leq k\}$.

Dies zeigt $\prod_{p \in \mathbb{P}} p^{B_p} \mid m$, und mit Bem. 1.20(b) folgt $[n_1, \dots, n_k] = \prod_{p \in \mathbb{P}} p^{B_p}$. □

2.23. Bsp.: $(2^2 \cdot 3^5 \cdot 7^2 \cdot 11, 3^2 \cdot 7^5 \cdot 11^2) = 3^2 \cdot 7^2 \cdot 11$

$$[2^2 \cdot 3^5 \cdot 7^2 \cdot 11, 3^2 \cdot 7^5 \cdot 11^2] = 2^2 \cdot 3^5 \cdot 7^5 \cdot 11^2$$

2.24. Bem.: Der Satz von der eindeutigen PFZ besagt, dass jedes nicht-Null-Element des Ringes $\mathbb{Z}$ eindeutig als Produkt von unzerlegbaren ("irreduziblen") Elementen $p \in \mathbb{P}$ und einer Einheit $e \in \{1, -1\}$ geschrieben werden kann.

Die nächst-einfachen Bereiche sind die Ringe

$$\mathbb{Z}[\sqrt{a}] := \{b_1 + b_2 \sqrt{a} ; b_1, b_2 \in \mathbb{Z}\} \text{ für } a \in \mathbb{Z} \setminus \{k^2 ; k \in \mathbb{Z}\}.$$

Hier können in naheliegender Weise Einheiten und Primelemente definiert werden.

Wie das Beispiel $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ zeigt,

kann die Eigenschaft der eindeutigen Zerlegbarkeit in Primfaktoren verloren gehen.

Diese Probleme bilden den Ausgangspunkt zur algebraischen Zahlentheorie.