§1. Teilbarkeit und Primzahlen

$\mathbb{N} := \{1, 2, 3, \dots\}$ die natürlichen Zahlen

$\mathbb{N}_0 := \mathbb{N} \cup \{0\}$

$\mathbb{Z}$ die ganzen Zahlen

$\mathbb{Q}$ die rationalen Zahlen

$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q}$

1.1 Definition: Seien $a, b \in \mathbb{Z}$, $b \neq 0$. a ist durch b teilbar $:\Leftrightarrow$ $\exists c \in \mathbb{Z}: a = bc$. b heißt dann ein Teiler von a und a ein Vielfaches von b. Notation: $b|a$.

c ist dann eindeutig bestimmt. Warum?

1.2 Definition: Sei $p \in \mathbb{N}$, $p \geq 2$. p heißt Primzahl $:\Leftrightarrow$ $[\forall d \in \mathbb{N}: d|p \Rightarrow d \in \{1, p\}]$.
Sonst heißt p zusammengesetzt.

Beispiel: 2, 3, 5 weiter bis ≤ 100?
aber nicht 1

1.3 Proposition: Sei $a \in \mathbb{N}$, $a \neq 1$. Dann ist a ein Produkt von Primzahlen (nicht notwendig verschieden), d.h. $a = p_1 \cdots p_n$ für $p_1, \dots, p_n$ prim, $n \geq 1$.

Beweis: falls a selbst prim ✓

allgemein: vollständige Induktion nach a

$a = 1$ ✓ $a = 2$ ✓

$a > 2$: a prim ✓ sonst $\exists b, c < a: a = b \cdot c$, $b, c \neq 1$

Induktionsvoraussetzung: Behauptung gilt für alle natürlichen Zahlen $< a$ also auch für b und c $\Rightarrow$ b und c sind Produkte von Primzahlen $\Rightarrow$ a auch $\square$

Folgerung: jede natürliche Zahl $\neq 1$ hat einen Primteiler

1.4 Theorem (Euklid): Es gibt unendlich viele verschiedene Primzahlen.

Beweis: Angenommen, es gibt nur endlich viele verschiedene Primzahlen $p_1 = 2, p_2 = 3, \dots, p_\ell$ für ein $\ell \in \mathbb{N}$. Sei $a := p_1 \cdot p_2 \cdots p_\ell + 1 \in \mathbb{N}$. $a > 1$

Nach 1.3 ist a ein Produkt von Primzahlen $\Rightarrow \exists q$ prim mit $q \mid a$

q prim $\Rightarrow q \in \{p_1, p_2, \dots, p_\ell\}$; $\exists j: q = p_j$, $a = p_j \cdot b$ für ein $b \in \mathbb{N}$

Aber auch $a = p_1 \cdot p_2 \cdots p_j \cdots p_\ell + 1 = p_j \cdot c + 1$ für $c = p_1 p_2 \cdots \hat{p_j} \cdots p_\ell$ ← d.h. p_j wird ausgelassen

$\Rightarrow 1 = a - p_j \cdot c = p_j \cdot b - p_j \cdot c = p_j \cdot (b - c)$ ↯ □

Folgerung aus dem Beweis: Seien $p_1, p_2, \dots, p_n, \dots$ die Primzahlen, der Größe nach geordnet. Dann ist $p_{n+1} < p_1 \cdot p_2 \cdots p_n + 1$. warum?

Wie häufig sind Primzahlen unter den natürlichen Zahlen?

1.5 Definition: Sei $\mathcal{P} := \{p \in \mathbb{N} : p \text{ prim}\}$. Für $x \in \mathbb{R}$ sei $\pi(x) := \#\{p : p \in \mathcal{P} \text{ und } p \leq x\}$. π heißt Primzahlfunktion (oder Anzahlfunktion der Primzahlen).

Tabelle:

x	$\pi(x)$	$x/\ln(x)$ (zum Vergleich), ungefähr
1	?	?
10	?	?
100	?	?
1000	168	145
10^{10}	4.118.054.813	3.948.131.654

Asymptotisches Verhalten von $\pi(x)$?

In der analytischen Zahlentheorie beweist man den Primzahlsatz

$$\lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1$$

(vermutet von Gauss 1793 und von Legendre 1798

bewiesen, mit komplexer Analysis von Hadamard 1896 und de la Vallée Poussin 1896, mit reeller Analysis von Erdős und Selberg 1949)

Die Zerlegung in 1.3 ist eindeutig.

1.6 Theorem (Fundamentalsatz der Arithmetik, Gauss 1801):
Sei $n \in \mathbb{N}$. Dann existiert eine eindeutige Funktion ~~mit~~ $e: \mathcal{P} \to \mathbb{N}_0$
sodaß $n = \prod_{p \in \mathcal{P}} p^{e(p)}$. (Fast alle $e(p)$ sind Null.) Das heißt, n hat eine eindeutige Zerlegung als Produkt von Primzahlen, den Primfaktoren von n.

Beweis: Existenz folgt aus 1.3, die Eindeutigkeit ist zu zeigen.
Was bedeutet Eindeutigkeit genau? Sei $m = \prod_{e(p)>0} p^{e(p)}$. Sei q eine Primzahl mit $q | m$.
Dann muß q eines der p mit $e(p) > 0$ in der gegebenen Zerlegung sein, falls diese eindeutig ist.
Denn: $q | m \Rightarrow m = q \cdot m'$, m' hat auch eine Zerlegung $m' = \prod p^{e'(p)}$ (vielleicht andere p) $\Rightarrow m = \prod_{p \in \mathcal{P}} p^{e''(p)}$ mit $e''(p) = \begin{cases} e'(p)+1, & p = q \\ e'(p) & \text{sonst} \end{cases}$

Eindeutigkeit bedeutet: $e(p) = e''(p)\ \forall p \Rightarrow e(q) = e''(q) = e'(q)+1 > 0 \Rightarrow$
q kommt in der Zerlegung vor

Jetzt beginnt der Beweis der Eindeutigkeit, mit Induktion nach n: $n = 1$ ✓
n prim ✓ Sei $n > 1$: Sei $n = p_1 \cdots p_r = q_1 \cdots q_s$, zwei Zerlegungen von n als Produkt von (nicht notwendig verschiedenen) Primzahlen
Wollen: $r = s$, p's $= q$'s (nach Umordnung)

Erster Fall: $\exists i,j: p_i = q_j$, dh $\exists$ gemeinsamer Primfaktor in beiden Zerlegungen
$\Rightarrow n = p_1 \cdots \underset{\shortparallel}{p_i} \cdots p_r \Rightarrow \frac{n}{p_i} = \frac{n}{q_j}$, also $p_1 \cdots \hat{p_i} \cdots p_r < n$

$= q_1 \cdots q_j \cdots q_s \qquad\qquad = q_1 \cdots \hat{q_j} \cdots q_s$

Induktion $\Rightarrow r-1 = s-1$, p's $= q$'s (nach Umordnung)

Zweiter Fall: $\forall i,j: p_i \neq q_j$, dh es gibt keinen gemeinsamen Primfaktor in den beiden Zerlegungen
Wir sortieren die p's der Größe nach, also $p_1 \leq p_2 \leq \ldots$, ebenso die q's, $q_1 \leq q_2 \leq \ldots$
n nicht prim $\Rightarrow$ mindestens zwei Faktoren in jeder Zerlegung
$\Rightarrow n \geq p_1^2$ und $n \geq q_1^2$.
$p_1 \neq q_1$, z.B. $p_1 < q_1 \Rightarrow p_1 q_1 < q_1^2 \leq n$ (ebenso, wenn $q_1 < p_1$)
$\Rightarrow n - p_1 q_1 > 0$, Bezeichnung: $\ell := n - p_1 q_1 \in \mathbb{N}$

$l < n$, also hat l nach Induktion eine eindeutige Zerlegung in Primfaktoren

$p_1 | n$ und $p_1 | p_1 q_1 \Rightarrow p_1 | n - p_1 q_1 = l$

ebenso $q_1 | l$

Die Zerlegung von l ist eindeutig, also kommen nach der Bemerkung oben (für $m = l$) p_1 und q_1 in der Zerlegung vor, $l = p_1 \cdot q_1 \cdot$ (weitere Faktoren)

Also: $p_1 q_1 | l$ und $p_1 q_1 | p_1 q_1 \Rightarrow p_1 q_1 | \underset{p_1 (p_2 \cdots p_r)}{\underset{\shortparallel}{n}} = l + p_1 q_1$

Kürzen $\Rightarrow q_1 | p_2 \cdots p_r$

Aber $p_2 \cdots p_r < n$, also wieder Induktionsvoraussetzung anwendbar

$\Rightarrow p_2 \cdots p_r$ hat eindeutige Zerlegung $\Rightarrow q_1$ kommt vor, $q_1 \in \{p_2, \ldots, p_r\}$ $\lightning$ zur Voraussetzung im zweiten Fall

$\Rightarrow$ der zweite Fall tritt nie auf $\square$

Eine Anwendung von 1.6 ist eine untere Schranke für eine durch Primzahlen definierte Funktion einer reellen Variablen:

<u>1.7 Proposition:</u> Sei $x \in \mathbb{R}$, $x \geq 2$. Dann gilt $\sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{p} > \ln(\ln x) - \frac{1}{2}$

Konsequenz: es gibt unendlich viele Primzahlen. warum?

(Das illustriert die enge Verbindung zwischen Analysis und Zahlentheorie im Kontext von Primzahlen.)

Beweis von 1.7 (Euler, 1737): Sei $\tilde{\mathbb{P}} \subset \mathbb{P}$, $|\tilde{\mathbb{P}}| < \infty$, d.h. $\tilde{\mathbb{P}}$ ist eine endliche Menge von Primzahlen. Sei $\mathcal{N}(\tilde{\mathbb{P}}) := \{ n \in \mathbb{N} \mid p | n \Rightarrow p \in \tilde{\mathbb{P}} \}$, d.h. die Menge aller n, deren Primfaktoren alle in $\tilde{\mathbb{P}}$ liegen, inklusive $1 \in \mathcal{N}(\tilde{\mathbb{P}})$.

Behauptung: Für $s \in \mathbb{R}_{>0}$ ist $\prod_{p \in \tilde{\mathbb{P}}} (1 - \frac{1}{p^s})^{-1} = \prod_{p \in \tilde{\mathbb{P}}} \sum_{k=0}^{\infty} \frac{1}{p^{ks}} = \sum_{n \in \mathcal{N}(\tilde{\mathbb{P}})} \frac{1}{n^s}$

Beweis der Behauptung:

$(1 - \frac{1}{p^s})^{-1}$ lässt sich als geometrische Reihe schreiben:

$$\frac{1}{1 - \frac{1}{p^s}} = \sum_{k=0}^{\infty} \left(\frac{1}{p^s}\right)^k$$

Details nachprüfen, Voraussetzungen

Ausmultiplizieren von $\prod_{p \in \tilde{\mathbb{P}}} \sum_{k=0}^{\infty} \frac{1}{p^{ks}}$ liefert Summanden $\frac{1}{p_1^{k_1 s}} \cdot \frac{1}{p_2^{k_2 s}} \cdots \frac{1}{p_r^{k_r s}}$

wenn $\tilde{\mathbb{P}} = \{p_1, \ldots, p_r\}$

wie wird absolute Konvergenz verwendet?

Dabei kommt jeder Tupel $\{k_1, \dots, k_r\}$ von Exponenten genau einmal vor

$\Rightarrow$ für jedes $n \in \mathbb{N}$ kommt $\frac{1}{n^s}$ genau einmal in der Reihe vor

$\Rightarrow$ Behauptung   wie wird 1.6 verwendet?

Jetzt wird $\tilde{P}$ genauer gewählt: Für $x \geq 2$ sei $\tilde{P} := \{p \in P : p \leq x\}$

Alle $n \in \mathbb{N}$ mit $n \leq x$ liegen in $N(\tilde{P})$ warum?

und viele n mit $n > x$ auch.

Also: $$\prod_{p \leq x} \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n \leq x} \frac{1}{n^s} + \sum_{\substack{n > x \\ n \in N(\tilde{P})}} \frac{1}{n^s} \qquad (+)$$

Speziell für $s = 1$: $$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{n \leq x} \frac{1}{n} + \sum_{\substack{n > x \\ n \in N(\tilde{P})}} \frac{1}{n} > \sum_{n \leq x} \frac{1}{n} > \underbrace{\int_1^x \frac{1}{y}\, dy}_{\text{warum?}} = \ln x - \underbrace{0}_{\ln 1}$$

(warum folgt daraus, daß es unendlich viele Primzahlen gibt?)

$\ln$ monoton $\Rightarrow$ $$\underbrace{\ln\left(\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1}\right)}_{\sum_{p \leq x} \ln\left(1 - \frac{1}{p}\right)^{-1}} > \ln(\ln x) \qquad (*)$$

Für $|y| < 1$ ist $$\ln \frac{1}{1-y} = \sum_{k=1}^{\infty} \frac{y^k}{k}$$ Taylorreihe berechnen

$y := \frac{1}{p}$ $\Rightarrow$ $$\sum_{p \leq x} \ln\left(1 - \frac{1}{p}\right)^{-1} = \sum_{p \leq x} \sum_{k=1}^{\infty} \frac{1}{k p^k} = \sum_{p \leq x} \frac{1}{p} + \underbrace{\sum_{p \leq x} \sum_{k=2}^{\infty} \frac{1}{k p^k}}_{\leq \frac{1}{2} \sum_{p \leq x} \underbrace{\sum_{k=2}^{\infty} \frac{1}{p^k}}} \leq$$

$$\leq \sum_{p \leq x} \frac{1}{p} + \frac{1}{2} \left(\sum_{p \leq x} \underbrace{\left(\frac{1}{1 - \frac{1}{p}} - \frac{1}{p} - 1\right)}\right)$$

Vgl geometrische Reihe $\frac{1}{1-\frac{1}{p}} - \frac{1}{p^0} - \frac{1}{p^1} = \left(\sum_{k=0}^{\infty} \frac{1}{p^k}\right) - \frac{1}{p^0} - \frac{1}{p^1}$

$$= \frac{1}{\frac{p-1}{p}} - \frac{1}{p} - 1 = \frac{p}{p-1} - \frac{1}{p} - 1$$

$$= 1 + \frac{1}{p-1} - \frac{1}{p} - 1 = \frac{1}{p(p-1)}$$

$$\Rightarrow \sum_{p \leq x} \ln\left(1 - \frac{1}{p}\right)^{-1} \leq \sum_{p \leq x} \frac{1}{p} + \frac{1}{2} \sum_{p \leq x} \frac{1}{p(p-1)} \leq$$

$$\leq \sum_{p \leq x} \frac{1}{p} + \frac{1}{2} \sum_{m=2}^{\infty} \underbrace{\frac{1}{m(m-1)}}_{= \frac{1}{m-1} - \frac{1}{m}} = \left(\sum_{p \leq x} \frac{1}{p}\right) + \frac{1}{2} \cdot 1$$

zeige $\sum_{m=2}^{\infty} \frac{1}{m(m-1)} = 1$

Mit $(*)$ ergibt sich

$$\ln(\ln x) < \sum_{p \leq x} \ln\left(1 - \frac{1}{p}\right)^{-1} \leq \left(\sum_{p \leq x} \frac{1}{p}\right) + \frac{1}{2}, \text{ also}$$

$$\sum_{p \leq x} \frac{1}{p} > \ln(\ln x) - \frac{1}{2} \quad \square$$

Mit viel mehr Analysis kann man bessere Abschätzungen und Aussagen direkt über $\pi(x)$ herleiten. Das ist nicht Gegenstand dieser Vorlesung, sondern der analytischen Zahlentheorie. Dort spielt die Riemannsche ζ-Funktion (ζ = zeta) $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ (für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$). Die Riemannsche Vermutung ist eine Aussage über ζ, aus der eine Verstärkung des Primzahlsatzes folgen würde. (Für den Beweis gibt es eine Belohnung von 1 Million US-Dollar. Diese Belohnung wurde bisher nicht abgeholt.)

Aus dem Beweis von 1.7 folgt:

1.8 Korollar: Für $s \in \mathbb{R}$, $s > 1$ gilt: $\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} = \underbrace{\sum_{n \in \mathbb{N}} \frac{1}{n^s}}$

warum konvergiert diese Reihe?

Beweis: Im Beweis von 1.7 wurde (†) gezeigt:

$$\begin{array}{ccccc} \prod_{p \le x} \left(1 - \frac{1}{p^s}\right)^{-1} & = & \sum_{n \le x} \frac{1}{n^s} & + & \sum_{\substack{n > x \\ n \in \mathbb{N}(\mathbb{P})}} \frac{1}{n^s} \\ \downarrow {\scriptstyle x \to \infty} & & \downarrow {\scriptstyle x \to \infty} & & \downarrow {\scriptstyle x \to \infty} \\ \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} & & \sum \frac{1}{n^s} & & 0 \end{array}$$

warum?

$\square$

In $\sum_{n \in \mathbb{N}} \frac{1}{n^s}$ kommt $\mathbb{P}$ nicht vor, oder doch?

Für $s \to 1$ nähert sich $\sum_{n \in \mathbb{N}} \frac{1}{n^s}$ der harmonischen Reihe. Folgerung: $|\mathbb{P}| = \infty$

Wegen $\left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{k \ge 0} \frac{1}{p^{ks}}$ ergibt sich

$$\prod_{p \in \mathbb{P}} \left(\sum_{k=0}^{\infty} \frac{1}{p^{ks}} \right) = \sum_{n \in \mathbb{N}} \frac{1}{n^s} \quad \text{(Euler-Produkt)}$$

direkter Beweis?

Jetzt kehren wir zurück zur elementaren Zahlentheorie und betrachten Grundbegriffe zur Teilbarkeit.

Aus dem Hauptsatz der Arithmetik, 1.6, ergibt sich die Bestimmung der Teiler von $n \in \mathbb{N}$:

$n \in \mathbb{N}$ hat eine eindeutige Primfaktorzerlegung $n = p_1^{d_1} \cdots p_e^{d_e}$

$d = p_1^{e_1} \cdots p_e^{e_e} q_1^{a_1} \cdots q_t^{a_t} \mid n \Leftrightarrow e_i \leq d_i$ für $i = 1, \dots, e$ und $a_j = 0 \ \forall j$ warum?

Auch die gemeinsamen Teiler von $a, b \in \mathbb{N}$ kann man bestimmen:

$$a = p_1^{a_1} \cdots p_e^{a_e} \text{ mit } a_i \geq 0$$

$$b = p_1^{b_1} \cdots p_e^{b_e} \text{ mit } b_i \geq 0$$

$\Rightarrow c = p_1^{c_1} \cdots p_e^{c_e} q_1^{d_1} \cdots q_t^{d_t}$ teilt a und b $\Leftrightarrow c_i \leq \min(a_i, b_i) \ \forall i$ und $d_j = 0 \ \forall j$

und c ist ein gemeinsames Vielfaches von a und b $\Leftrightarrow c_i \geq \max(a_i, b_i) \ \forall i$

Begründung?

Insbesondere:

1.9 Proposition: Seien $a, b \in \mathbb{N}$, $a = p_1^{a_1} \cdots p_e^{a_e}$ und $b = p_1^{b_1} \cdots p_e^{b_e}$ (mit Primzahlen p_i, paarweise verschieden, und Exponenten $a_i, b_i \in \mathbb{N}_0$).

Dann $\exists!\, d \in \mathbb{N}: d \mid a, d \mid b$ und $\forall e \in \mathbb{N}: e \mid a$ und $e \mid b \Rightarrow e \mid d$. d heißt größter gemeinsamer Teiler von a und b. Bezeichnung: $d = ggT(a, b)$.

Außerdem $\exists!\, k \in \mathbb{N}: a \mid k, b \mid k$ und $\forall j \in \mathbb{N}: a \mid j$ und $b \mid j \Rightarrow k \mid j$. k heißt kleinster gemeinsamer Vielfaches von a und b. Bezeichnung $k = kgV(a, b)$.

Es gilt die Gleichung $a \cdot b = ggT(a,b) \cdot kgV(a,b)$.

Beweis

Aber wenn a und b gegeben sind, ist es im Allgemeinen schwierig, die Faktorisierung in Produkte von Primzahlen zu bestimmen. Die Bestimmung von $ggT(a,b)$ (und damit auch von $kgV(a,b)$) geht viel leichter mit dem Euklidischen Algorithmus, der auf Division mit Rest beruht:

Seien $a, b \in \mathbb{N}$, $a > b$.

Falls $b \mid a$: $ggT(a,b) = b$ ✓

Sonst (oder ganz allgemein): $\mathbb{N} = \{1, \dots, b-1\} \cup \{b, \dots, 2b-1\} \cup \{2b, \dots, 3b-1\} \cup \dots$ (disjunkte Vereinigung). $a \in \mathbb{N}$ liegt in genau einer solchen Menge,

$a \in \{qb, \dots, (q+1)b - 1\} \Rightarrow a = qb + r_0$ mit $0 \leq r_0 < b$

$r_0 = 0$ bedeutet $a = qb$, $b \mid a$. Allgemein: Division von a durch b mit Rest r_0.

Behauptung: $ggT(a,b) = ggT(b, r_0)$

Beweis: $d \mid a$ und $d \mid b \Rightarrow d \mid (a - qb) = r_0$

$d \mid b$ und $d \mid r_0 \Rightarrow d \mid (qb + r_0) = a$ warum?

$\Rightarrow$ Die gemeinsamen Teiler von a und b sind genau die gemeinsamen Teiler von b und r_0 $\Rightarrow$ Behauptung

$r_0 < b < a$, der Algorithmus dividiert nun b durch r_0 mit Rest, usw mit immer kleineren Zahlen

Also: $b = q_1 r_0 + r_1$. $r_1 = 0 \Leftrightarrow r_0 | b \Rightarrow r_0 = ggT(b, r_0) = ggT(a,b)$

$0 \leq r_1 < r_0$. Falls $r_1 \neq 0$: weiter mit r_0 und r_1: $r_0 = q_2 r_1 + r_2$, etc

$a > b > r_0 > r_1 > \ldots$ alle in $\mathbb{N}_0 \Rightarrow \exists i: r_{i-1} = q_i r_i + r_{i+1}$ mit $r_{i+1} = 0$ (aber $r_i \neq 0$)

$\Rightarrow r_i | r_{i-1}$ und $r_i = ggT(r_{i-1}, r_i) = ggT(r_{i-2}, r_{i-1}) = \ldots = ggT(b, r_0) = ggT(a,b)$

Ergebnis: Der letzte von 0 verschiedene Rest im Euklidischen Algorithmus ist $ggT(a,b)$.

Beispiel: $7200 = 2 \times 3132 + 936$

$3132 = ?$

$?$

$? = 1 \times 288 + 36$

$288 = 8 \times 36 \qquad \Rightarrow ggT(7200, 3132) = 36$

Aber es gilt zudem: $36 = 324 - 1 \times 288$

$= -936 + 3 \times 324 = ? = -10 \times 7200 + 23 \times 3132$

$\Rightarrow ggT(a,b)$ ist eine ganzzahlige Linearkombination von a und b. Beweis

Dabei können (müssen?) negative Koeffizienten auftreten.

Anwendung: Seien $a, b, n \in \mathbb{N}$. Gesucht sind ganzzahlige Lösungen x, y der Gleichung $ax + by = n$.

(Gleichungen in ganzen Zahlen heißen Diophantische Gleichungen.)

Für $n = ggT(a,b)$ ist die Gleichung lösbar, wie gerade beobachtet. nämlich?

Für $n = c \cdot ggT(a,b)$ auch. wie?

Falls $ggT(a,b) \nmid n$ ist die Gleichung unlösbar. Denn: $d | a$ und $d | b \Rightarrow$ $d | ax + by$ $\forall x, y$, also $d | n \Rightarrow ggT(a,b) | n$

Ergebnis: $ax + by = n$ ist lösbar mit $x, y \in \mathbb{Z} \Leftrightarrow ggT(a,b) | n$

Diophantische Gleichungen werden später ein Thema der Vorlesung sein.

Der Beweis des Fundamentalsatzes der Arithmetik, 1.6, hat die vorangehenden Ergebnisse nicht verwendet, sondern war völlig unabhängig.

Aus dem Euklidischen Algorithmus kann man 1.6 neu beweisen:

Behauptung 1: Für $a, b, n \in \mathbb{N}$ ist $ggT(na, nb) = n \cdot ggT(a,b)$

(Das folgt auch aus 1.6, aber 1.6 dürfen wir nicht verwenden.)

Beweis: $a = qb + r_0 \Rightarrow na = q(nb) + nr_0,\ nr_0 < nb$

$$\begin{array}{ccc} a = qb + r_0 & & na = q(nb) + nr_0 \\ \Big\downarrow & \text{Eukl. Alg} & \Big\downarrow \\ r_i = ggT(a,b) & & nr_i = ggT(na,nb) \end{array}$$

Behauptung 2: p prim, $p \mid a \cdot b \Rightarrow [p \mid a$ oder $p \mid b]$ vgl Definition prim in Algebra

Beweis: $ggT(p,a) \mid p \Rightarrow ggT(p,a) \in \{1, p\}$.

Falls $ggT(p,a) = p$: $p \mid a$ ✓

Falls $ggT(p,a) = 1$: Behauptung 1 $\Rightarrow ggT(bp, ab) = 1 \cdot b = b$

$p \mid ab$ nach Voraussetzung, $p \mid bp \Rightarrow$ ~~ggT(bp~~ $p \mid ggT(bp, ab) = b$ ✓

Daraus leiten wir die Eindeutigkeit der Primfaktorzerlegung ab, also den schwierigen Teil von 1.6:

Sei $n = p_1 \cdots p_r = q_1 \cdots q_s$, alle p's und q's Primzahlen.

$p_1 \mid n = q_1 \cdots q_s \underset{\text{Beh2}}{\Rightarrow} p_1 \mid q_1$ oder $p_1 \mid q_2 \cdots q_s$. Falls $p_1 \mid q_1$ prim: $p_1 = q_1$

Falls $p_1 \mid q_2 \cdots q_s$: $p_1 \mid q_2$, also $p_1 = q_2$, oder $p_1 \mid q_3 \cdots q_s$, usw

Also: $\exists i: p_1 = q_i$, Kürzen: $p_2 \cdots p_r = q_1 \cdots \hat{q_i} \cdots q_s$ usw

$\Rightarrow$ bis auf Umordnung gilt $p_i = q_i\ \forall i \Rightarrow$ die Zerlegung ist eindeutig