16.05.18

Satz 3.13 (Fundamentalsatz der Arithmetik)

Sei $n \geq 2$ eine ganze Zahl

(a) Die Zahl n kann als Produkt von Primzahlen geschrieben werden

(b) Die Zerlegung aus (a) ist eindeutig bis auf Reihenfolge.

Beweis:

(a) Wir zeigen (a) per Induktion.

I.A.: Für $n=2$ ist (a) richtig, da 2 Primzahl ist.

I.B.: Die Aussage aus (a) gelte für alle $n < N$.

I.S.: Wir zeigen, dass (a) auch für N gilt.

Falls N eine Primzahl ist gilt (a).

Andernfalls hat N einen nicht-trivialen Teiler $m_1 \neq 1, N$. Also $N = m_1 \cdot m_2$ mit $1 < m_1, m_2 < N$

Nach I.B können wir m_1 und m_2 aber als ein Produkt von Primzahlen schreiben, also auch $N = m_1 \cdot m_2$.

(b) Angenommen $n \geq 2$ hat zwei Primfaktorzerlegungen $n = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_\ell$

O.E. $m \leq \ell$.

Da $p_1 | n$ folgt mit Lemma 3.12, dass p_1 auch eine der Primzahlen q_i teilt.

Da die q_i Primzahlen sind, existiert ein Index i_1 mit $p_1 = q_{i_1}$.

Kürzt man p_1 und q_{i_1} in beiden Primfaktorzerlegungen, so liefert das gleiche Argument

die Existenz von einem Index i_2 mit $p_2 = q_{i_2}$.
Wir kürzen wieder und verfahren induktiv bis $p_n = q_{i_n}$.
Wäre $m < l$, so sagt die gekürzte Gleichung, dass 1 ein Produkt aus $(l-m)$ vielen Primzahlen ist.
Da dies unmöglich ist, folgt $m = l$
$\Rightarrow$ Die q_i's sind nur eine Umordnung der p_i

□

Jede natürliche Zahl $n \geq 1$ lässt sich als eindeutiges Produkt

$$n = \prod_{p \in \mathbb{P}} p^{n_p} \quad \text{mit} \quad n_p \geq 0$$

schreiben.

Wir bemerken, dass dieses Produkt über **alle** Primzahlen läuft. Ist $n = 1$, so ist $n_p = 0 \ \forall p \in \mathbb{P}$.
Schon Euklid bewies in seinem Buch "die Elemente" (3. Jhd. v. Chr.), dass es unendlich viele Primzahlen gibt.

Satz 3.14 (Euklid)
Es gibt unendlich viele Primzahlen.

Beweis:
/A: Es gibt nur endlich viele Primzahlen.
$p_1, \dots, p_n$.
Betrachten $N = p_1 \cdot \dots \cdot p_n + 1$. N ist durch keine der Primzahlen p_i $(i = 1, \dots, n)$ teilbar, da sonst auch 1 durch diese Primzahl teilbar wäre.
Da nach dem Fundamentalsatz der

Arithmetik aber jede Zahl ≥ 2 einen Primteiler hat, muss es eine weitere Primzahl p_{n+1} geben. ↯

Bemerkung: N muss nicht Primzahl sein, z.B.

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$$

Definition 3.15

Das kleinste gemeinsame Vielfache von a und b ($\in \mathbb{Z}$) ist die kleinste positive Zahl, die sowohl durch a als auch durch b teilbar ist.

Wir bezeichnen diese Zahl mit $kgV(a,b)$.

Lemma 3.16

Seien $n = \prod_{p \in \mathbb{P}} p^{n_p}$ und $\prod_{p \in \mathbb{P}} p^{m_p}$ natürliche Zahlen.

(a) Es ist $ggT(n,m) = \prod_{p \in \mathbb{P}} p^{\max(n_p, m_p)}$ & $kgV(n,m) = \prod_{p \in \mathbb{P}} p^{\min(n_p, m_p)}$

(b) $kgV(n,m) = \frac{n \cdot m}{ggT(n,m)}$

Beweis: Übung

Beispiel 3.17: $n = 93$, $m = 42$

Wir bestimmen den ggT:

$$93 = 2 \cdot 42 + 9$$
$$42 = 4 \cdot 9 + 6$$
$$9 = 1 \cdot 6 + \boxed{3}$$
$$6 = 2 \cdot 3$$

$$\Rightarrow kgV(93,42) = \frac{93 \cdot 42}{3} = 31 \cdot 42 = 1302.$$

Der Fundamentalsatz der Arithmetik sagt, dass sich jede Zahl als ein Produkt von Primzahlen schreiben lässt. Wie man diese Primfaktorzerlegung findet (v.a. für große Zahlen) ist ein anderes Problem. Die Tatsache, dass es extrem schwierig ist, große Zahlen zu faktorisieren, wird heutzutage in der Kryptographie verwendet (dazu später mehr)

Eine Möglichkeit eine Primfaktorzerlegung zu finden ist die so genannte Probedivision:

Wir bemerken hierzu zunächst, "dass wenn" wir einen Primteiler einer Zahl n finden möchten, müssen wir lediglich Primzahlen $\leq \sqrt{n}$ betrachten.
Dies liegt daran, dass wenn $n = a \cdot b$, so ist $a \leq \sqrt{n}$ oder $b \leq \sqrt{n}$.
Für den folgenden Algorithmus gehen wir davon aus, dass wir eine Liste alles Primzahlen $\leq \sqrt{n}$ haben. Wie man so eine Liste findet, sehen wir später.

Algorithmus 3.18 (Probedivision)

Input: $n \in \mathbb{N}$
Wollen Primfaktorzerlegung von n.

(1) Wir fangen mit $p = 2$ an und gehen die Liste aller Primzahlen $\leq \sqrt{n}$ durch. Für jede Primzahl testen wir, ob $p | n$. Dies kann mittels Division mit Rest überprüft werden.

(2) Falls $p \mid n$, so berechnen wir die höchste Potenz p^e mit $p^e \mid n$ und ersetzen n durch $\frac{n}{p^e}$.
Anschließend gehen wir in unserer Primzahlenliste weiter und testen die nächste Primzahl.

(3) Sobald $p^2 > n$, sind wir fertig.

Beispiel 3.19

Wollen 1746 faktorisieren.
1746 ist durch $p=2$ teilbar, aber $2 \nmid \frac{1746}{2} = 873$
(wir sind mit $p=2$ fertig)
873 ist durch 3 teilbar mit $\frac{873}{3} = 291$,
was wieder durch 3 teilbar ist mit $\frac{291}{3} = 97$.
97 ist ebenso nicht durch 5 und 7 teilbar.
Die nächste Primzahl $p=11$ ist schon größer als $\sqrt{97} < \sqrt{100} = 10$. Also sind wir fertig.
$\Rightarrow 1746 = 2 \cdot 3^2 \cdot 97$

Als nächstes überlegen wir uns, wie wir alle Primzahlen p finden, die kleiner als eine vorgegebene Schranke $B > 0$ sind.
Wir verwenden hierzu das "Sieb des Eratosthenes" (gr. Mathematiker 276 v. Chr. – 194 v. Chr.)

Algorithmus 3.20 (Sieb des Eratosthenes)

Sei $B > 2$.

(0) Wir machen eine Liste aller Zahlen 2 bis B.

(1) Wir fangen mit der ersten "nicht-durchgestrichenen" Zahl an. Am Anfang ist die 2.

(2) Man markiert diese Zahl als Primzahl und streicht alle Vielfachen der Zahl durch.

(3) Man wiederholt Schritt (1) und (2) bis nur noch durchgestrichene Zahlen übrig bleiben oder solche, die man als Primzahl markiert hat.

Beispiel 3.21

Wir möchten alle Primzahlen $\leq B = 49$ finden. Hierzu erstellen wir zunächst eine Liste der Zahlen 2 bis 49 und streichen alle Vielfachen dieser ersten Primzahl $p = 2$ durch.

~~1~~	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~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~
~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~

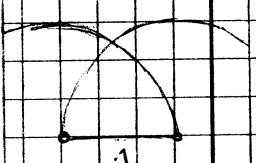
Bemerkung 3.22

Einige besonders prominente Klassen von Primzahlen haben häufig einen eigenen Namen.

(a) (**Mersenne Primzahlen**) sind Primzahlen der Form $p = 2^n - 1$. Dies ist z.B. prim für $n = 2, 3, 5, 7, 13$.
Die größte bekannte Mersenne Primzahl (gefunden 2017) ist $2^n - 1$ für $n = 77\,232\,917$. Dies ist die 50. bekannte Mersenne Primzahl.

(b) (**Fermat Primzahlen**) sind Primzahlen der Form $F_n = 2^{2^n} + 1$.
Die einzigen bekannten Fermat-Primzahlen sind $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 65537$.
⌜Fakt: $2^n + 1$ kann nur prim sein, wenn $n = 2^k$ ⌟

Fakt:
Ein regelmäßiges n-Eck ist genau dann mit Zirkel und Lineal (ohne Skala) konstruierbar, wenn $n = 2^m \cdot F_{i_1} \cdot \ldots \cdot F_{i_k}$, wobei F_{i_j} paarw. verschiedene Fermat-Primzahlen sind.



(c) (**Primzahlzwillinge**) sind Paare (p, q) von Primzahlen mit $|p - q| = 2$, z.B. $(3, 5)$, $(5, 7)$, ...
Es wird vermutet, dass es unendlich viele Primzahlzwillinge gibt.

Fakt: $\sum_{p \in \mathbb{P}} \frac{1}{p}$ divergiert (Euler)

Viggo Brun (1919): $\sum_{p, p+2 \text{ prim}} \left(\frac{1}{p} + \frac{1}{p+2}\right)$

konvergiert gegen $B_2 = 1,90216\ldots$

Zhang '13: Es gibt unendlich viele Paare von Primzahlen (p,q) mit $|p-q| \leq 70.000.000$.

Zurzeit durch Verbesserung der Methoden von Zhang hat man: $\exists$ unendlich viele Paare von Primzahlen (p,q) mit $|p-q| \leq 246$

Ebenso interessieren sich die Zahlentheoretiker für Primzahldrillinge, -vierlinge, usw.

Primzahlen (p,q) mit $|p-q| = 6$ heißen auch Sexy-Primzahlen.

Lemma 3.23

(a) Sind $d, n \in \mathbb{N}$ mit $d \mid n$, so gilt:

$$(2^d - 1) \mid (2^n - 1)$$

(b) Ist $2^n - 1$ prim, dann ist auch n prim.

Beweis: Übung