Schüler-Propädeutikum Mathematik 2023
Vortrag 2: Primzahlen

Andreas Lochmann

10. November 2023

1 Knobelaufgaben von letzter Woche

Knobelaufgabe:
Zeigen Sie: Für $x \in \mathbb{Z}$ ist $x^2 + 2$ nie durch 5 teilbar.

Beweis:
Wir berechnen $(x^2 + 2) \ \% \ 5$. Für $x = 0, 1, 2, 3, 4$ erhalten wir nacheinander $2, 3, 1, 1, 3$. Zu keinem Zeitpunkt erhalten wir 0. Daher ist $x^2 + 2$ niemals durch 5 teilbar. □

Knobelaufgabe: Es sei n eine ungerade Zahl. Zeigen Sie, dass dann $2n + 5$ keine Quadratzahl sein kann.

Beweis:
Wir rechnen modulo 4. Da n ungerade ist, muss $n \ \% \ 4 = 1$ oder $n \ \% \ 4 = 3$ sein. Dann ist $(2n+5) \ \% \ 4 = (2 \cdot 1 + 5) \ \% \ 4 = 3$ oder $(2n+5) \ \% \ 4 = (2 \cdot 3 + 5) \ \% \ 4 = 3$, also in jedem Fall $(2n + 5) \ \% \ 4 = 3$. Schauen wir uns jetzt an, welche Reste eine Quadratzahl modulo 4 hinterlassen kann: Wir setzen $x = 0, 1, 2, 3$ nacheinander in $x^2 \ \% \ 4$ ein und finden nacheinander $0, 1, 0, 1$. Das heißt: $x^2 \ \% \ 4$ hat niemals Rest 3, und folglich kann $2n + 5$ keine Quadratzahl sein. □

2 Primzahlen

Definition:
Eine **Primzahl** ist eine positive ganze Zahl $p > 1$, die nur 1 und sich selbst als Teiler besitzt.

Beispiel:
Die ersten Primzahlen lauten 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.

Fundamentalsatz der Arithmetik
Jede natürliche Zahl $n > 1$ hat eine eindeutige Primfaktorzerlegung, das heißt es gibt eindeutig bestimmte Primzahlen $p_1 \leq p_2 \leq \cdots \leq p_r$, so dass

$$n \;=\; p_1 \cdot p_2 \cdots p_r.$$

Beispiele:

100	$2 \cdot 2 \cdot 5 \cdot 5$	105	$3 \cdot 5 \cdot 7$
101	prim	106	$2 \cdot 53$
102	$2 \cdot 3 \cdot 17$	107	prim
104	$2 \cdot 2 \cdot 2 \cdot 13$	108	$2 \cdot 2 \cdot 3 \cdot 3 \cdot 3$

Satz von Euklid:
Es gibt unendlich viele Primzahlen.

Beweisidee:
Gegeben sei eine endliche Liste von Primzahlen. Erzeuge daraus eine Zahl, die eine neue Primzahl als Faktor enthalten muss.

Beweis:
Angenommen, es gibt nur die Primzahlen p_1 bis p_n. Sei a das Produkt aller Primzahlen, plus 1, also

$$a \;=\; p_1 \cdot p_2 \cdot \cdots\cdots p_n + 1\,.$$

Offenbar ist $p_1 \equiv 0 \pmod{p_1}$ und damit $a \equiv 1 \pmod{p_1}$, a ist also nicht durch p_1 teilbar. Ebenso kann a auch durch keine andere der Primzahlen p_1 bis p_n teilbar sein. Folglich ist entweder a selber eine neue Primzahl, oder a ist zusammengesetzt aus neuen Primzahlen. □

Es gibt also unendlich viele Primzahlen insgesamt ... aber wie viele Primzahlen gibt es zwischen 1 und 100? Zwischen 1 und 1.000? Zwischen 1 und 1.000.000? Carl-Friedrich Gauß und Adrien-Marie Legendre haben Ende des 18ten Jahrhunderts dazu eine Vermutung aufgestellt, die 1859 von Bernhard Riemann bewiesen wurde: Der Primzahlsatz.

Primzahlsatz:
Mit $\pi(x)$ bezeichnen wir die Zahl der Primzahlen zwischen 1 und (einschließlich) x. Dann ist $\pi(x)$ ungefähr $x/\ln(x)$, in folgendem Sinn:

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

Dabei steht ln für den natürlichen Logarithmus.

Aufgabe: Vergleichen Sie mit den Schätzwerten:
$\pi(10) = 4$
$\pi(100) = 25$
$\pi(1.000) = 168$
$\pi(10.000) = 1229$
$\pi(100.000) = 9592$
$\pi(1.000.000) = 78.498$
$\pi(10.000.000) = 664.579$
$\pi(100.000.000) = 5.761.455$

Aufgabe:
Wie viele Primzahlen mit bis zu 100 Stellen gibt es ungefähr?
Wie viele SD-Karten bräuchte man zu ihrer Speicherung etwa?
(SD-Karten haben eine Kapazität von etwa 160 Terabyte pro Kilogramm.)

3 Euklidischer Algorithmus

Definition:
Sind a und b natürliche Zahlen, so bezeichnen wir mit $\mathrm{ggT}(a, b)$ den **größten gemeinsamen Teiler** von a und b, das ist die größte Zahl $t \in \mathbb{N}$ mit $t \mid a$ und $t \mid b$.

Satz:
Sind a und b natürliche Zahlen mit $a > b$, so ist $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b)$.

Beweis:
Ist t ein Teiler von a und b, also $a = x \cdot t$ und $b = y \cdot t$, so ist t auch ein Teiler von $a - b$, denn $a - b = (x - y) \cdot t$. Das geht auch umgekehrt: Ist t ein Teiler von $a - b$ und b, so ist t ein Teiler von $a - b + b = a$. □

Aufgabe:
Benutzen Sie $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b)$ wiederholt, um den größten gemeinsamen Teiler von 100 und 148.

Anschlussfrage:
Wie könnte man das beschleunigen?

Euklidischer Algorithmus:
Seien $a_1, a_2 \in \mathbb{N}$. Man kann $\mathrm{ggT}(a_1, a_2)$ wie folgt berechnen:
1. Sei $n = 1$.
2. Ist $a_n > a_{n+1}$, so sei $a_{n+2} = a_n \,\%\, a_{n+1}$, sonst sei $a_{n+2} = a_{n+1} \,\%\, a_n$.
3. Ist $a_{n+2} = 0$, so ist a_{n+1} der gesuchte ggT; beende dann den Algorithmus.
4. Erhöhe n um eins und gehe zu Schritt (2).