Einführung in die Algebra und Diskrete Mathematik
Übungsblatt 2

19.03.2015

1. Seien $a, b, x \in \mathbb{N}$ und $u, v \in \mathbb{Z}$ so, dass $x = ua + vb$. Zeigen Sie: Wenn sowohl $x \mid a$ als auch $x \mid b$, dann gilt $x = \mathrm{ggT}(a, b)$. Können Sie aus der Gleichung $ab + cd = 1$ $(a, b, c, d \in \mathbb{Z})$ Aussagen über $\mathrm{ggT}(a, b)$, $\mathrm{ggT}(a, c)$, $\mathrm{ggT}(a, d)$, $\mathrm{ggT}(b, c)$, $\mathrm{ggT}(b, d)$ und $\mathrm{ggT}(c, d)$ ableiten?

   Lösung. Da x ein gemeinsamer Teiler von a und b ist, gilt auch $x \mid \mathrm{ggT}(a, b)$ wegen Satz 1.10, (2). Aus $x = ua + vb = \mathrm{ggT}(a, b)\left(u\frac{a}{\mathrm{ggT}(a,b)} + v\frac{b}{\mathrm{ggT}(a,b)}\right)$ folgt außerdem $\mathrm{ggT}(a, b) \mid x$, somit gilt wegen der Antisymmetrie der Teilerrelation auch $x = \mathrm{ggT}(a, b)$. Da 1 jede der vier Zahlen a, b, c, d teilt, folgt aus der Gleichung $ab+cd = 1$, dass $\mathrm{ggT}(a, c) = \mathrm{ggT}(a, d) = \mathrm{ggT}(b, c) = \mathrm{ggT}(b, d) = 1$. Über $\mathrm{ggT}(a, b)$ und $\mathrm{ggT}(c, d)$ lässt sich aber nichts aussagen. □

2. Finden Sie ganzzahlige Lösungen der Gleichung $71u + 79v = \mathrm{ggT}(71, 79)$. Ist diese Lösung eindeutig? Falls nein, geben Sie eine weitere Lösung an.

   Lösung. Der erweiterte euklidische Algorithmus liefert in wenigen Schritten $u = 9$ und $v = -10$ sowie $\mathrm{ggT}(79, 71) = 1$. Diese Lösung ist nicht eindeutig, da etwa wegen $79(9 + 71) + 71(-10 - 79) = 1$ die Werte $u = 80$ und $v = -89$ eine weitere Lösung bilden. □

3. Wir betrachten die sogenannten *Fibonacci-Zahlen* F_n, die folgendermaßen rekursiv definiert sind:

$$F_0 = 1, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \text{ für } n \geq 2.$$

   Begründen Sie, dass die Zahlen F_n und F_{n+1} für alle $n \in \mathbb{N}_0$ teilerfremd sind. Gilt das für beliebige Startwerte F_0 und F_1?

   Lösung. Wir verwenden Satz 1.13., wonach für ganze Zahlen a, b, die nicht beide 0 sind, für ein $z \in \mathbb{Z}$ die Gleichheit $\mathrm{ggT}(a, b) = \mathrm{ggT}(a+zb, b)$ gilt. Wir wählen $z = -1$ und erhalten so Schritt für Schritt unter Verwendung der Rekursionsvorschrift für die Fibonacci-Zahlen

$$\begin{aligned}\mathrm{ggT}(F_{n+1}, F_n) &= \mathrm{ggT}(F_{n+1} - F_n, F_n) = \mathrm{ggT}(F_{n-1}, F_n) = \mathrm{ggT}(F_{n-1}, F_n - F_{n-1}) \\ &= \mathrm{ggT}(F_{n-1}, F_{n-2}) = \cdots = \mathrm{ggT}(F_1, F_0) = 1.\end{aligned}$$

   Allgemein gilt offensichtlich $\mathrm{ggT}(F_{n+1}, F_n) = \mathrm{ggT}(F_1, F_0)$, was für andere Werte für F_0 und F_1 natürlich auch größer als 1 sein kann. □

4. Seien $a, b \in \mathbb{N}$ mit $a < b$. Wir nehmen an, dass der Euklidische Algorithmus zur Bestimmung von $\mathrm{ggT}(a, b)$ genau n Schritte (Divisionen) benötigt. Zeigen Sie, dass dann $a \geq F_n$ gilt, wobei F_n wieder die n-te Fibonacci-Zahl bezeichnet. Beweisen Sie zudem die Ungleichung $F_n \geq \frac{1}{2}\left(\frac{3}{2}\right)^n$ und leiten Sie damit eine obere Schranke für n in Abhängigkeit von a her. Wie hängt diese Schranke mit der Anzahl der Ziffern von a zusammen?

   Lösung. Wir setzen $b = a_{n+1}$ und $a = a_n$. Da der Euklidische Algorithmus genau n Schritte benötigt, ergibt sich also eine Sequenz von Divisionen

$$\begin{aligned} a_{n+1} &= q_n a_n + a_{n-1} \\ a_n &= q_{n-1} a_{n-1} + a_{n-2} \\ &\vdots \\ a_3 &= q_2 a_2 + a_1 \\ a_2 &= q_1 a_1, \end{aligned}$$

   wobei $a_n > a_{n-1} > \cdots > a_2 > a_1 > 0$, $q_1 \geq 2$ und $q_i \geq 1$ für alle $i \in \{2, \ldots, n\}$. Den kleinstmöglichen Wert für a_n erhalten wir offenbar, wenn $a_1 = 1$, $q_1 = 2$ und $q_i = 1$ für alle $i \in \{2, \ldots, n\}$ ist. Dann ergeben sich von unten beginnend die Abschätzungen

$$\begin{aligned} a_2 &\geq 2, \\ a_3 &\geq 1 \cdot 2 + 1 = 3, \\ a_4 &\geq 3 \cdot 1 + 2 = 5, \\ &\vdots \end{aligned}$$

   Dies lässt sich induktiv weiterspinnen zur Bedingung $a_n \geq F_n$, also $a \geq F_n$. Die Ungleichung $F_n \geq \frac{1}{2}\left(\frac{3}{2}\right)^n$ lässt sich induktiv zeigen, da sie offenbar für F_0 und für F_1 gilt und man dann unter der Annahme, dass die Aussage für alle natürlichen Zahlen $\leq n$ gilt,

$$F_{n+1} = F_n + F_{n-1} \geq \frac{1}{2}\left(\frac{3}{2}\right)^n + \frac{1}{2}\left(\frac{3}{2}\right)^{n-1} = \frac{1}{2}\left(\frac{3}{2}\right)^n \left(1 + \frac{2}{3}\right) \geq \frac{1}{2}\left(\frac{3}{2}\right)^{n+1}$$

   herleiten kann. Also haben wir insgesamt gezeigt, dass $a \geq F_n \geq \frac{1}{2}\left(\frac{3}{2}\right)^n$, was sich umformen lässt zu

$$n \leq \frac{\log_{10} 2a}{\log_{10}(3/2)} \leq 6 \log_{10} a + 2.$$

   Da sich die Anzahl der Ziffern einer Zahl a wie $\log_{10} a$ verhält (genau: $\lfloor \log_{10} a \rfloor + 1$ Ziffern), kann man also sagen, dass die Anzahl der Schritte beim Euklidischen Algorithmus proportional ist zur Ziffernanzahl der kleineren der beiden Zahlen. □

5. Wir betrachten die sogenannten *Fermat-Zahlen* $f_k = 2^{2^k} + 1$ für $k \in \mathbb{N}_0$.

   (a) Zeigen Sie die Rekursionsformel $f_n = \prod_{i=0}^{n-1} f_i + 2$ mittels vollständiger Induktion.

(b) Verwenden Sie diese Formel um zu zeigen, dass zwei verschiedene Fermatzahlen stets teilerfremd sind, also $\mathrm{ggT}(f_k, f_l) = 1$ für $l \neq k$.

(c) Warum folgt aus Punkt (b), dass es unendlich viele Primzahlen gibt?

Lösung. (a) Für $n = 1$ gilt $f_1 = 2^{2^1} + 1 = 5 = 2^{2^0} + 1 + 2 = f_0 + 2$ und der Induktionsanfang ist getan. Wir machen den Schritt von n nach $n+1$:

$$f_{n+1} - 2 = 2^{2^{n+1}} - 1 = 2^{2^n + 2^n} - 1 = 2^{2^n} 2^{2^n} - 1 = (f_n - 1)(f_n - 1) - 1$$
$$= f_n^2 - 2f_n = f_n(f_n - 2) \overset{IH}{=} f_n \prod_{i=0}^{n-1} f_i = \prod_{i=0}^{n} f_i.$$

(b) Sei o. B. d. A $k < l$. Dann ist

$$\mathrm{ggT}(f_k, f_l) = \mathrm{ggT}(f_k, f_{l-1} \dots f_k \dots f_0 + 2) = \mathrm{ggT}(f_k, 2) = 1,$$

wobei wir einerseits Satz 1.13. mit $z = -\prod_{i=0,\, i\neq k}^{l-1} f_i$ und andererseits die Tatsache, dass alle Fermatzahlen ungerade sind, verwendet haben.

(c) Angenommen, es gibt nur die n Primzahlen $p_1, \dots, p_n$. Da jede natürliche Zahl ≥ 2 mindestens einen Primteiler hat und alle Fermatzahlen paarweise teilerfremd sind, muss jede Fermatzahl einen Primteiler aufweisen, den sonst keine andere Fermatzahl hat. Also gibt es für jedes $i \in \{1, \dots, n\}$ genau ein $k \in \{0, \dots, n-1\}$, sodass $p_i \mid f_k$. Da aber sämtliche Primfaktoren von f_n aus der Menge $\{p_1, \dots, p_n\}$ stammen müssen, ist sie mit mindestens einer Zahl aus der Menge $\{f_0, \dots, f_{n-1}\}$ nicht teilerfremd, was ein Widerspruch zu (b) ist.

□