

Grundlagen der Mathematik II

Lösungsvorschlag zum 1. Übungsblatt

Aufgabe 1.

a) Geduldiges Ausdividieren von Faktoren liefert

$$\begin{aligned}487.872 &= 2 \cdot 243.936 = 2^2 \cdot 121.968 = 2^3 \cdot 60.984 = 2^4 \cdot 30.492 \\ &= 2^5 \cdot 15.246 = 2^6 \cdot 7.623 = 2^6 \cdot 3^2 \cdot 847 = 2^6 \cdot 3^2 \cdot 7 \cdot 121 \\ &= 2^6 \cdot 3^2 \cdot 7 \cdot 11^2,\end{aligned}$$

$$\begin{aligned}164.052 &= 2 \cdot 82.026 = 2^2 \cdot 41.013 = 2^2 \cdot 3^2 \cdot 4.557 = 2^2 \cdot 3^3 \cdot 1.519 = 2^2 \cdot 3^3 \cdot 7 \cdot 217 \\ &= 2^2 \cdot 3^3 \cdot 7^2 \cdot 31,\end{aligned}$$

$$\begin{aligned}7.128 &= 2 \cdot 3.564 = 2^2 \cdot 1.782 = 2^3 \cdot 891 = 2^3 \cdot 3^2 \cdot 99 \\ &= 2^3 \cdot 3^4 \cdot 11.\end{aligned}$$

Dabei sind die bekannten Teilbarkeitsregeln durch 2 (gerade Endziffer), 3 (Quersumme durch 3 teilbar), 5 (Endziffer 0 oder 5) und $9 = 3^2$ (Quersumme durch 9 teilbar) nützlich; wenn sie erschöpft sind, probiert man beispielsweise einfach die nächsten möglichen Primzahlen 7, 11, 13, ... durch.

Für die Anzahl der Teiler ergibt sich damit nach der Formel aus der Vorlesung:

$$|T(487.872)| = 2 \cdot (6 + 1) \cdot (2 + 1) \cdot (1 + 1) \cdot (2 + 1) = 2 \cdot 7 \cdot 3 \cdot 2 \cdot 3 = 252,$$

$$|T(164.052)| = 2 \cdot (2 + 1) \cdot (3 + 1) \cdot (2 + 1) \cdot (1 + 1) = 2 \cdot 3 \cdot 4 \cdot 3 \cdot 2 = 144,$$

$$|T(7.128)| = 2 \cdot (3 + 1) \cdot (4 + 1) \cdot (1 + 1) = 2 \cdot 4 \cdot 5 \cdot 2 = 80.$$

b) Den größten gemeinsamen Teiler (bzw. das kleinste gemeinsame Vielfache) zweier Zahlen erhält man, indem man für jeden Primfaktor beider Zahlen den kleineren (bzw. den größeren) der in den beiden Primfaktorzerlegungen auftretenden Exponenten wählt. Für mehr als zwei Zahlen wird aus „dem kleineren“ bzw. „dem größeren“ das Minimum bzw. Maximum der jeweiligen Exponenten.

Damit ergibt sich:

$$\text{ggT}(487.872, 164.052) = 2^2 \cdot 3^2 \cdot 7 = 252,$$

$$\text{kgV}(487.872, 164.052) = 2^6 \cdot 3^3 \cdot 7^2 \cdot 11^2 \cdot 31 = 317.604.672,$$

$$\text{ggT}(487.862, 7.128) = 2^3 \cdot 3^2 \cdot 11 = 792,$$

$$\text{kgV}(487.862, 7.128) = 2^6 \cdot 3^4 \cdot 7 \cdot 11^2 = 4.390.848,$$

$$\text{ggT}(164.052, 7.128) = 2^2 \cdot 3^3 = 108,$$

$$\text{kgV}(164.052, 7.128) = 2^3 \cdot 3^4 \cdot 7^2 \cdot 11 \cdot 31 = 10.827.432,$$

$$\text{ggT}(487.872, 164.052, 7.128) = 2^2 \cdot 3^2 = 36$$

$$\text{kgV}(487.872, 164.052, 7.128) = 2^6 \cdot 3^4 \cdot 7^2 \cdot 11^2 \cdot 31 = 952.814.016.$$

Aufgabe 2.

a) Dividiert man, wie im Tip vorgeschlagen, p mit Rest durch 6, so ergibt sich $p = 6k + r$ mit $k \in \mathbb{N}_0$ und $0 \leq r \leq 5$. Der Umstand, daß p eine Primzahl ist, reduziert jedoch die möglichen Werte von r :

- Im Fall $r = 0$ wäre $p = 6k$ durch 6 teilbar, hätte also zwei verschiedene Primfaktoren (2 und 3) und wäre damit keine Primzahl.
- Im Fall $r = 2$ wäre $p = 6k + 2$ durch 2 teilbar; da p aber selbst eine Primzahl ist, müßte dann $p = 2$ sein im Widerspruch zu $p \geq 5$.
- Im Fall $r = 3$ wäre $p = 6k + 3$ durch 3 teilbar; da p aber selbst eine Primzahl ist, müßte dann $p = 3$ sein im Widerspruch zu $p \geq 5$.
- Im Fall $r = 4$ wäre $p = 6k + 4 = 2 \cdot (3k + 2)$ ebenfalls durch 2 teilbar, und dies hatten wir schon ausgeschlossen.

Es bleiben also nur die Möglichkeiten $r = 1$ und $r = 5$ übrig. Im ersten Fall gilt also $p = 6k + 1$, und es muß $k \geq 1$ sein (sonst wäre $p = 1$); im zweiten Fall gilt $p = 6k + 5 = 6k + 6 - 1 = 6(k + 1) - 1$, und wegen $k \in \mathbb{N}_0$ ist $k + 1 \in \mathbb{N}$.

b) Nach a) gilt $p = 6k \pm 1$ für ein $k \in \mathbb{N}$. Die binomische Formel besagt dann

$$p^2 - 1 = (6k \pm 1)^2 - 1 = (36k^2 \pm 12k + 1) - 1 = 36k^2 \pm 12k = 12k \cdot (3k \pm 1).$$

Dies zeigt schon einmal, daß $p^2 - 1$ durch 12 teilbar ist. Wir wären fertig, wenn wir nun noch zeigen könnten, daß $k \cdot (3k \pm 1)$ stets durch 2 teilbar ist (denn dann ist $12k \cdot (3k \pm 1)$ durch $12 \cdot 2 = 24$ teilbar). Ist k gerade, so ist das klar, weil dann der erste Faktor durch 2 teilbar ist; ist aber k ungerade, so ist auch $3k$ ungerade und damit $3k \pm 1$ gerade. Insgesamt ist also $k \cdot (3k \pm 1)$ in jedem Fall durch 2 teilbar, und wir haben gewonnen.

c) Nach Definition ist

$$\binom{p}{n} = \frac{p!}{n! \cdot (p-n)!}.$$

Seit dem ersten Semester ist bekannt, daß dieser Bruch einen ganzzahligen Wert hat, was bedeutet, daß jeder Primfaktor des Nenners mindestens ebensooft im Zähler auftaucht wie im Nenner.

Sehen wir nun genauer hin: Der Zähler $p! = 1 \cdot 2 \cdot \dots \cdot p$ enthält den den Primfaktor p genau einmal, da keine der Zahlen $1, 2, \dots, p-1$ durch p teilbar sein kann. Der Nenner dagegen enthält den Primfaktor p überhaupt nicht: Denn nach Voraussetzung ist $n < p$ und $p-n < p$ (beachte $n \geq 1$), also taucht weder in $n!$ noch in $(p-n)!$ der Primfaktor p auf. Also bleibt der Zähler $p!$ auch nach Division durch den Nenner $n! \cdot (p-n)!$ durch p teilbar.

Aufgabe 3. Nach der Gaußschen Summenformel, die im ersten Semester behandelt wurde, gilt

$$p = \sum_{k=1}^n k = \frac{n(n+1)}{2}.$$

Diese Zahl ist genau dann eine Primzahl, wenn $n(n+1) = 2q$ mit einer Primzahl q ist (und zwar ist dann $p = q$). Wir müssen also untersuchen, wie sich die beiden Primfaktoren 2 und q auf die Faktoren n und $n+1$ verteilen können:

- Enthält jeder der Faktoren n und $n+1$ einen Primfaktor, so müssen beide Primzahlen sein; wegen $n < n+1$ und $2 \leq q$ muß dann $n = 2$ und $n+1 = q$, also $q = 3$ sein. Tatsächlich ist für $n = 2$ die Zahl $p = 1 + 2 = 3$ eine Primzahl.

- Enthält einer der Faktoren beide Primfaktoren, so muß der andere den Wert 1 haben. Wegen $n < n + 1$ ist das nur möglich, wenn $n = 1$ ist; dann ist aber $n + 1 = 2$ ebenfalls nicht das Produkt von zwei Primfaktoren. Tatsächlich ist für $n = 1$ auch $p = 1$, und dies ist keine Primzahl.

Mehr Möglichkeiten gibt es nicht: Also ist $n = 2$ die einzige Zahl der gesuchten Art.

Aufgabe 4.

- a) Vollständige Induktion nach k : Für $k = 0$ ist einerseits $F_k - 2 = 2^{2^0} + 1 - 2 = 2^1 - 1 = 1$, und das leere Produkt auf der rechten Seite der behaupteten Gleichung hat ebenfalls den Wert 1. Die Behauptung stimmt also.

Für den Induktionsschritt $k \rightarrow k - 1$ sei schon bekannt, daß $F_k - 2 = F_0 \cdot F_1 \cdot \dots \cdot F_{k-1}$ ist. Dann ist aber

$$\begin{aligned}
 F_{k+1} - 2 &= 2^{2^{k+1}} + 1 - 2 = 2^{2^k \cdot 2} - 1 \\
 &= \left(2^{2^k}\right)^2 - 1^2 && (\dots 3. \text{ Binomische Formel. } \dots) \\
 &= \left(2^{2^k} - 1\right) \cdot \left(2^{2^k} + 1\right) && (\dots \text{ Definition von } F_k \dots) \\
 &= (F_k - 2) \cdot F_k && (\dots \text{ Induktionsvoraussetzung. } \dots) \\
 &= F_0 \cdot F_1 \cdot \dots \cdot F_{k-1} \cdot F_k,
 \end{aligned}$$

wie behauptet.

Etwas einfacher ist die Rechnung möglicherweise, wenn man mit der rechten Seite der behaupteten Gleichung beginnt: Dann ergibt sich die gleiche Rechnung wie bei uns, nur von unten nach oben gelesen, und in dieser Richtung sind einige der Umformungsschritte evtl. näherliegend.)

- b) Wir können gefahrlos annehmen, daß $\ell < k$ ist (andernfalls vertauschen wir nur die Benennungen). Dann taucht F_ℓ im Produkt aus a) auf, es ist also

$$F_k - 2 = F_0 \cdot F_1 \cdot \dots \cdot F_\ell \cdot \dots \cdot F_{k-1}.$$

Diese Beziehung zeigt, daß jeder gemeinsame Primfaktor von F_k und F_ℓ auch ein Primfaktor von 2 sein muß, d.h. der einzige mögliche gemeinsame Primfaktor beider Zahlen ist 2 selbst. Nun sind aber alle Fermat-Zahlen nach ihrer Definition *ungerade*: Denn $F_k = 2^{2^k} + 1$, und wegen $2^k \geq 1$ ist 2^{2^k} stets gerade. Also gibt es in Wirklichkeit überhaupt keine gemeinsamen Primfaktoren von F_k und F_ℓ .

- c) In der Vorlesung wurde (ohne Rückgriff auf die Existenz unendlich vieler Primzahlen) bewiesen, daß sich jede natürliche Zahl > 1 im Wesentlichen eindeutig als Produkt von Primzahlen schreiben läßt. Nun bilden aber die Fermatzahlen

$$F_0, F_1, F_2, F_3, \dots$$

eine unendliche Folgen natürlicher Zahlen > 1 . Da aber nach b) keine Fermatzahl mit irgendeiner anderen einen gemeinsamen Primfaktor besitzt, jedoch jede von ihnen durch mindestens eine Primzahl teilbar sein muß (denn sie sind alle > 1), muß es „mindestens so viele Primzahlen geben wie Fermatzahlen“, d.h. es gibt unendlich viele Primzahlen.

Dieses Argument zeigt allgemeiner: Sobald man eine unendliche Folge paarweise teilerfremder natürlicher Zahlen > 1 gefunden hat, ist die Existenz unendlich vieler Primzahlen bewiesen. Anstelle der Fermatzahlen könnte man beispielsweise auch die „Sylvester-Folge“ $(a_n)_{n \in \mathbb{N}}$ nehmen, die rekursiv definiert ist durch

$$\begin{aligned}
 a_n &= 2, \\
 a_{n+1} &= a_1 \cdot \dots \cdot a_n + 1 \quad \text{für alle } n \in \mathbb{N}.
 \end{aligned}$$