

Max Wisniewski , Alexander Steen

Tutor: David Müßig

Aufgabe 1 (Teilbarkeit)

Gegeben seien natürliche Zahlen $k, m, n \in \mathbb{N} \setminus \{0\}$, so dass $n = k \cdot m$.

a) Beweisen Sie folgende Aussage:

$$\forall a, b \in \mathbb{Z} : (a^m - b^m) | (a^n - b^n).$$

Beweis:

Seien $a, b \in \mathbb{Z}$.

Faktoriert man die Formel aus, so gilt:

$$(*) \quad a^n - b^n = (a - b) \cdot \sum_{s=0}^{n-1} a^s b^{n-1-s}$$

Nun können wir diese Formel verwenden.

$$\begin{aligned} & (a^m - b^m) \mid (a^n - b^n) \\ \stackrel{\text{Def.}}{\Leftrightarrow} & (a^m - b^m) \mid \left((a^m)^k - (b^m)^k \right) \\ \stackrel{\text{Fakt.}}{\Leftrightarrow} & (a^m - b^m) \mid (a^m - b^m) \cdot \sum_{s=0}^{k-1} (a^m)^s (b^m)^{k-1-s} \end{aligned}$$

Nach Eigenschaft 4 der Vorlesung ($\forall a, b \in \mathbb{Z} \forall c \in \mathbb{Z} \setminus \{0\} : a|b \Leftrightarrow a|(c \cdot b)$), dass die Aussage stimmen muss, da gilt $\forall p \in \mathbb{Z} : p|p$, was ebenfalls in der Vorlesung gezeigt wurde.

b) Zeigen Sie weiter:

$$k \text{ ungerade} \Rightarrow (\forall a, b \in \mathbb{Z} : (a^m + b^m) | (a^n + b^n))$$

Beweis:

Seien $a, b \in \mathbb{Z}$.

Faktoriert man die Formel aus, so gilt für ungerade n :

$$(**) \quad a^n + b^n = (a + b) \cdot \sum_{s=0}^{n-1} (-1)^s a^s b^{n-1-s}$$

Wenden wir diese Formel auf die Aussage an, kommen wir auf:

$$\begin{aligned} & (a^m + b^m) \mid (a^n + b^n) \\ \stackrel{\text{Def.}}{\Leftrightarrow} & (a^m + b^m) \mid \left((a^m)^k + (b^m)^k \right) \\ \stackrel{\text{Formel}}{\Leftrightarrow} & (a^m + b^m) \mid (a^m + b^m) \cdot \left(\sum_{s=0}^{k-1} (-1)^s (a^m)^s (b^m)^{k-1-s} \right) \end{aligned}$$

Nun gilt wieder nach den selben Überlegungen wie in **a)** muss diese Formel gelten.

c) Beweis (*)

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$.

Rechnen wir die Faktorisierte Form aus (von $n - 1$ aus anfangen):

$$\begin{aligned}
 & (a - b) \cdot \sum_{s=0}^{n-1} a^s b^{n-1-s} \\
 = & ((a^n - a^{n-1}b) + (a^{n-1}b - a^{n-2}b^2) + \dots + (a^2b^{n-2} - ab^{n-1}) + (ab^{n-1} - b^n)) \\
 = & a^n + (-a^{n-1}b + a^{n-1}b) + (-a^{n-2}b^2 + \dots) + \dots + (\dots + a^2b^{n-2}) + (-ab^{n-1} + ab^{n-1}) - b^n \\
 = & a^n - b^n
 \end{aligned}$$

Bis auf die äußeren beiden Elemente stehen je 2 aufeinanderfolgende Summanden, die sich gegenseitig auslöschen.

d) Beweis ()**

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $\exists k \in \mathbb{N} : n = 2 \cdot k + 1$.

Rechnen wir die Faktorisierte Form aus (von $n - 1$ aus anfangen):

$$\begin{aligned}
 & (a + b) \cdot \sum_{s=0}^{n-1} (-1)^s a^s b^{n-1-s} \\
 = & (a^n + a^{n-1}b) - (a^{n-1}b + a^{n-2}b^2) + \dots - (a^2b^{n-2} + ab^{n-1}) + (ab^{n-1}b^n) \\
 = & a^n + (a^{n-1}b - a^{n-1}b) + \dots + (ab^{n-1} - ab^{n-1}) + b^n \\
 = & a^n + b^n
 \end{aligned}$$

Wie bei c) löschen sich bis auf die äußersten beide alle Elemente gegenseitig aus.

Aufgabe 2 (Primzahlen)

- a) Bestimmen Sie mit dem Sieb des Erastrothenes alle Primzahlen zwischen 2 und 200. Das streichen der Elemente kann mit der Legende rechts der Zahlen nachvollzogen werden.

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	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Alle Primzahlen in diesem Intervall:

$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199\}$

b) Geben Sie die Primfaktorzerlegung der Zahl $-1.601.320$ an.

$$-1.601.320 = -1 \cdot 43 \cdot 19 \cdot 7^2 \cdot 5 \cdot 2^3$$

Aufgabe 3 (Teiler)

Für $n \in \mathbb{N}$ mit $n \geq 1$ sei $T_n := \{l \geq 1 \mid l \mid n\}$ die Menge ihrer Teiler.

a) Es sei $n = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$ die Primfaktorzerlegung von n . Geben Sie eine Formel für die Anzahl $\#T_n$ der Teiler von n an.

Für diese Formel reicht uns ein einfaches kombinatorisches Argument. Wir haben s verschiedene Elemente mit jeweils k_i vorkommen. Diese wollen wir nun in allen kombination Möglichkeiten haben. Dies führt zur Formel:

$$\#T_n = \prod_{j=0}^s (k_j + 1)$$

b) Charakterisieren Sie diejenigen Zahlen, für die $\#T_n$ ungerade ist.

Lemma Seien $n, t_1, t_2 \in \mathbb{N} \setminus \{0\}$ mit $n = t_1 \cdot t_2$. Dann ist (t_1, t_2) ein Teilerpaar, d.h. es existiert keine andere Zahl t_3 für die gilt: $n = t_1 \cdot t_3$ oder $n = t_2 \cdot t_3$. Die Teilerbeziehung ist jeweils eindeutig.

Beweis Gelten die Bezeichner aus dem Lemma.

Nehmen wir an, es gäbe o.B.d.A. zu t_1 nicht nur t_2 sondern auch t_3 .

$$t_1 \cdot t_2 = t_1 \cdot t_3 \Leftrightarrow t_1 \cdot (t_2 - t_3) = 0$$

Da $t_1 \neq 0$ ist, da es Teiler ist, muss $t_2 = t_3$ gelten. Damit ist es eindeutig.

Vermutung: $\#T_n$ ungerade $\Leftrightarrow \exists a \in \mathbb{N} : a^2 = n$.

Beweis:

" \Rightarrow "

Da wir eine ungerade Zahl an Teilern haben, muss es eine Zahl a geben, die keinen von sich verschiedenen Partner hat, d.h. anderen nach Lemma einen eindeutigen Partner haben. Da aber gilt $a \mid n$, kann nur $n = a \cdot a$ gelten, womit n eine Quadratzahl ist.

" \Leftarrow "

Da n Quadratzahl ist, gibt es den Teiler a , der sein eingetragenes Teilerpaar darstellt. Korollar zum Lemma gilt, dass es keine zweite Zahl b gibt mit $b \neq a \wedge n = b \cdot b$. Wir haben also einen Teiler und jeder weitere Teiler kommt als Teilerpaar.

Damit haben wir $2k + 1$ Teiler. $\Rightarrow \#T_n$ ist ungerade.

□

Aufgabe 4 (Die Amnestie)

Ein Herrscher hält 500 Personen in Einzelzellen gefangen, die von 1 bis 500 durchnummeriert sind. Anlässlich seines fünfzigsten Geburtstags gewährt er eine Amnestie nach folgenden Regeln:

- Am ersten Tag werden alle Zellen aufgeschlossen.
- Am Tag i wird der Schlüssel der Zellen $i, 2i, 3i$ usw. einmal umgedreht, d. h. Zelle j wird versperrt, wenn sie offen war, und geöffnet, wenn sie verschlossen war, $j = i, 2i, 3i$ usw., $i = 2, \dots, 500$.

Wie viele Gefangene kommen frei? Ist der Insasse von Zelle 179 unter den Freigelassenen?

Eigenschaft: Der Schlüssel einer Zelle wird genau dann umgedreht, wenn der Tag Teiler der Zahl ist.

Beweis:

” \Leftarrow ”

1. Tag, werden alle Zellen geöffnet. $k \neq 0 \Rightarrow 1|k$. Da die Zellen im Bereich $[1, 500]$ liegen ist $k \neq 0$. Am Tag j gilt: $\forall k \in \mathbb{N} : k \cdot i$ wird geöffnet. $k \cdot i$.

Hat Zelle z nun den Teiler j , so gilt: $\exists k' \in \mathbb{N} : z = j \cdot k'$. Dies erfüllt die drehen Voraussetzung.

” \Rightarrow ”

Sei z Zelle und j Tag und es gilt $j \nmid z \Rightarrow \exists k, r \in \mathbb{N} : k \cdot j + r = z \wedge 0 < r < j$.

Da aber nur $t \cdot j$ für beliebige t gedreht wird, kann bei der Zelle das Schloss nicht nochmal gedreht werden. \square

Vermutung: Die Zelle z ist am Ende offen, genau dann wenn $\#T_z$ ungerade ist.

Beweis:

” \Leftarrow ”

$$\exists k \in \mathbb{N} : z = 2 \cdot k + 1$$

Am ersten Tag werden alle Türen geöffnet. Bleibe $2 \cdot k$ Drehvorgänge. Da aber nach Beschreibung sich 2 Vorgänge paarweise aufheben, wird die Tür am Ende geöffnet sein.

” \Rightarrow ”

$\exists k \in \mathbb{N} : z = 2 \cdot k + 2$ ist möglich, da 0 keine unserer Türen ist.

Am ersten Tag wird die Tür wieder geöffnet. Bleiben $2 \cdot k + 1$ Drehvorgänge, von denen sich $2 \cdot k$ gegenseitig aufheben. Bleib uns ein Drehvorgang, der die Tür abschließt. \square

Nach 3b) müssen wir jetzt nur noch sehen, welche der Zellen Quadratzahlen sind:

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144

169, 196, 225, 256, 289, 324, 361, 400, 484

Da die 179 keine Quadratzahl ist, wird die Zelle am Ende der 500 Tage geschlossen sein.