

Lasse Rempe und Rebecca Waldecker

Zahlentheorie ◇ Algorithmik ◇ Kryptographie

Primzahltests für Einsteiger

Lösungen und Hinweise zu den Aufgaben
(24. Februar 2017)

Inhalt

1	Natürliche Zahlen und Primzahlen	1
2	Algorithmen	19
3	Zahlentheoretische Grundlagen	27
4	Primzahlen und Kryptographie	47
5	Der Ausgangspunkt: Fermat für Polynome	49
6	Der Satz von Agrawal, Kayal und Saxena	53

Kapitel 1

Natürliche Zahlen und Primzahlen

Aufgabe 1.1.6. (a) Sei $n \in \mathbb{N}$ und sei $M := \{m \in \mathbb{N} : 2m \geq n\}$. Das ist eine nicht-leere Teilmenge von $\mathbb{N}$ (z.B. ist n selbst ein Element von M), daher besitzt M nach dem Wohlordnungsprinzip ein kleinstes Element m_0 . Wir haben also $2m_0 \geq n$, aber $2m < n$ für alle natürlichen Zahlen $m < m_0$. Insbesondere ist $2m_0 - 2 = 2(m_0 - 1) < n$. Insgesamt ergibt das

$$2m_0 - 2 < n \leq 2m_0.$$

Das bedeutet, dass n mit $2m_0 - 1$ oder mit $2m_0$ übereinstimmt. Im ersten Fall ist n ungerade, im zweiten Fall ist n gerade.

Ist n gerade, etwa $n = 2m_1$, so kann n nicht gleichzeitig ungerade sein. Denn sonst wäre $n = 2m_2 - 1$ für irgendein m_2 . Aber dann folgt $2m_1 = 2m_2 - 1$, also $m_1 - m_2 = \frac{1}{2} \notin \mathbb{N}$. Das ist ein Widerspruch.

(b) Seien $n, m \in \mathbb{N}$ gerade Zahlen. Dann gibt es $a, b \in \mathbb{N}$ so, dass $n = 2a$ ist und $m = 2b$. Also haben wir $nm = (2a)(2b) = 2(2ab)$, und $2ab$ ist eine natürliche Zahl. Also ist nm gerade.

Seien nun $n, m \in \mathbb{N}$ ungerade. Dann gibt es $a, b \in \mathbb{N}$ so, dass $n = 2a - 1$ ist und $m = 2b - 1$. Also haben wir

$$\begin{aligned} nm &= (2a - 1)(2b - 1) = 4ab - 2b - 2a + 1 \\ &= (4ab - 2b - 2a + 2) - 1 = 2(ab - b - a + 1) - 1, \end{aligned}$$

und $ab - b - a + 1$ ist eine natürliche Zahl. Also ist nm ungerade.

Aufgabe 1.1.7. Es ist zu zeigen, dass eine nicht-leere und nach unten bzw. nach oben beschränkte Menge ganzer Zahlen ein kleinstes bzw. größtes Element besitzt.

Sei also zunächst $M \subseteq \mathbb{Z}$ nicht-leer und nach unten beschränkt. Außerdem sei $K \in \mathbb{Z}$ eine untere Schranke, also $K \leq x$ für alle $x \in M$. Setze

$$S := \{1 + x - K : x \in M\}.$$

Für alle $x \in M$ ist $x - K \in \mathbb{N}_0$ und daher $1 + (x - K)$ eine natürliche Zahl. S ist also eine Teilmenge von $\mathbb{N}$, und da M nicht-leer ist, ist auch S nicht-leer. Nach dem Wohlordnungsprinzip besitzt S ein kleinstes Element s_0 . Sei $m_0 := s_0 - 1 + K$. Dann ist $m_0 \in M$ nach Definition von S , und wir zeigen nun, dass m_0 das kleinste Element von M ist. Angenommen, es gibt ein Element $m \in M$, welches echt kleiner als m_0 ist. Dann ist $s := 1 + m - K \in S$, und wir haben $s = 1 + m - K < 1 + m_0 - K = s_0$, ein Widerspruch. Also ist m_0 das kleinste Element in M .

Sei jetzt $M \subseteq \mathbb{Z}$ nicht-leer und nach oben beschränkt und sei K eine obere Schranke, also $x \leq K$ für alle $x \in M$. Dann ist die Menge $M' := \{-x : x \in M\}$ eine nicht-leere Menge ganzer Zahlen und durch $-K$ nach unten beschränkt. Daher besitzt M' ein kleinstes Element m' , mit dem ersten Teil der Aufgabe. Aber dann ist $m^* := -m'$ das größte Element von M .

Die Aussagen gelten weder für $\mathbb{Q}$ noch für $\mathbb{R}$. In der Tat ist die Menge

$$M := \{x \in \mathbb{Q} : 0 < x < 1\}$$

sowohl nach unten als auch nach oben beschränkt, durch 0 bzw. 1. Sie besitzt aber weder ein kleinstes noch ein größtes Element. (Um das formal zu beweisen, sei $x \in M$. Dann gilt $0 < \frac{x}{2} < x < \frac{x+1}{2} < 1$. Also ist x weder kleinstes noch größtes Element von M .)

Aufgabe 1.1.8. Es sei $x \in \mathbb{R}$ mit $x \neq 1$.

Behauptung. Für alle $n \in \mathbb{N}$ gilt:

(a) $2^n \geq 2n$.

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

(c) $\sum_{k=0}^{n-1} x^k = \frac{1-x^n}{1-x}$.

(d) $\sum_{k=0}^{n-1} (k+1) \cdot x^k = \frac{nx^{n+1} - (n+1)x^n + 1}{(1-x)^2}$.

(e) $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$.

(f) $\sum_{i=0}^n (i \cdot i!) = (n+1)! - 1$.

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

Beweis von (a). INDUKTIONSANFANG: Es ist $2^1 = 2 \geq 2 \cdot 1$, also stimmt die Behauptung für $n = 1$.

INDUKTIONSVORAUSSSETZUNG: Sei n eine natürliche Zahl, so dass die Ungleichung für n wahr ist. Das bedeutet $2^n \geq 2n$.

INDUKTIONSSCHRITT: Es ist

$$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot 2n$$

mit der Induktionsvoraussetzung. Wegen $n \geq 1$ ist $2n \geq n + 1$, also

$$2^{n+1} \geq 2 \cdot 2n \geq 2 \cdot (n + 1).$$

Damit sind wir fertig. ■

Beweis von (b). INDUKTIONSANFANG: Es ist

$$\sum_{k=1}^1 k = 1 = \frac{1(1+1)}{2},$$

also stimmt die Aussage für $n = 1$.

INDUKTIONSVORAUSSSETZUNG: Wir machen den Induktionsschritt hier von $n - 1$ nach n anstatt von n nach $n + 1$, weil das die Notation etwas einfacher macht (Induktionsvariante (a) aus Abschnitt 1.1). Sei also $n \geq 2$ eine natürliche Zahl so, dass die Gleichung für $n - 1$ wahr ist. Das bedeutet

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

INDUKTIONSSCHRITT: Wir teilen die Summe auf, um die Induktionsvoraussetzung anzuwenden:

$$\begin{aligned} \sum_{k=1}^n k &= \sum_{k=1}^{n-1} k + n = \frac{(n-1)n}{2} + n \\ &= \frac{n^2 - n}{2} + \frac{2n}{2} = \frac{n^2 - n + 2n}{2} = \frac{n^2 + n}{2} = \frac{n(n+1)}{2}. \end{aligned} \quad \blacksquare$$

Beweis von (c). INDUKTIONSANFANG: Für $n = 1$ steht auf der linken Seite

$$\sum_{k=0}^{n-1} x^k = \sum_{k=0}^0 x^k = x^0 = 1$$

und auf der rechten Seite $\frac{1-x^n}{1-x} = \frac{1-x^1}{1-x} = 1$, also stimmen beide Seiten überein, und die Behauptung ist für $n = 1$ richtig.

INDUKTIONSVORAUSSETZUNG: Sei n eine natürliche Zahl, für die die Behauptung richtig ist. Das bedeutet

$$\sum_{k=0}^{n-1} x^k = \frac{1-x^n}{1-x}.$$

INDUKTIONSSCHRITT: Auf der linken Seite der Gleichung für $n+1$ bekommen wir

$$\sum_{k=0}^n x^k = \sum_{k=0}^{n-1} x^k + x^n = \frac{1-x^n}{1-x} + x^n,$$

wenn wir die Induktionsvoraussetzung einsetzen. Also ist

$$\sum_{i=0}^n x^i = \frac{1-x^n}{1-x} + x^n = \frac{1-x^n+x^n(1-x)}{1-x} = \frac{1-x^n+x^n-x^{n+1}}{1-x} = \frac{1-x^{n+1}}{1-x}$$

wie behauptet, und der Beweis ist abgeschlossen. ■

Beweis von (d). INDUKTIONSANFANG: Es gilt

$$\sum_{k=0}^0 (k+1) \cdot x^k = 1 \cdot x^0 = 1 \quad \text{und} \quad \frac{1 \cdot x^2 - 2 \cdot x^1 + 1}{(1-x)^2} = \frac{x^2 - 2x + 1}{x^2 - 2x + 1} = 1,$$

die Behauptung ist also für $n = 1$ richtig.

INDUKTIONSVORAUSSETZUNG: Sei $n \in \mathbb{N}$ mit

$$\sum_{k=0}^{n-1} (k+1) \cdot x^k = \frac{nx^{n+1} - (n+1)x^n + 1}{(1-x)^2}.$$

INDUKTIONSSCHRITT: Es gilt

$$\begin{aligned} \sum_{k=0}^n (k+1) \cdot x^k &= \left(\sum_{k=0}^{n-1} (k+1) \cdot x^k \right) + (n+1) \cdot x^n \\ &= \frac{nx^{n+1} - (n+1)x^n + 1}{(1-x)^2} + (n+1) \cdot x^n \\ &= \frac{nx^{n+1} - (n+1)x^n + 1 + (n+1)x^n(1-x)^2}{(1-x)^2} \\ &= \frac{nx^{n+1} - (n+1)x^n + 1 + (n+1)x^n(x^2 - 2x + 1)}{(1-x)^2} \\ &= \frac{nx^{n+1} - (n+1)x^n + 1 + (n+1)x^{n+2} - (2n+2)x^{n+1} + (n+1)x^n}{(1-x)^2} \\ &= \frac{(n+1)x^{n+2} - (n+2)x^{n+1} + 1}{(1-x)^2}. \end{aligned}$$

Damit ist die Induktion abgeschlossen.

(Wer sich mit der Differentialrechnung auskennt, kann diesen Teil der Aufgabe auch alternativ durch Bilden der Ableitungen der linken und rechten Seite von Teil (c) beweisen.) ■

Beweis von (e). INDUKTIONSANFANG: Für $n = 1$ gilt $\sum_{k=1}^n k^2 = \sum_{k=1}^1 k^2 = 1^2 = 1$ und

$$\frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} = \frac{1(1+1)(2 \cdot 1 + 1)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = 1,$$

also ist die Gleichung dann wahr.

INDUKTIONSVORAUSSETZUNG: Sei $n \geq 2$ eine natürliche Zahl derart, dass die Gleichung für $n - 1$ richtig ist. Das heißt, es gilt

$$\sum_{k=1}^{n-1} k^2 = \frac{(n-1)n(2n-1)}{6}.$$

INDUKTIONSSCHRITT: Wir formen die linke Seite um und setzen die Induktionsvoraussetzung ein (immer der gleiche Trick ...):

$$\begin{aligned} \sum_{k=1}^n k^2 &= \sum_{k=1}^{n-1} k^2 + n^2 = \frac{(n-1)n(2(n-1)+1)}{6} + n^2 \\ &= \frac{(n-1)n(2(n-1)+1) + 6n^2}{6} = \frac{n(2n^2 - 2n - n + 1 + 6n)}{6} \\ &= \frac{n(2n^2 + 3n + 1)}{6} = \frac{n(n+1)(2n+1)}{6}, \end{aligned}$$

und damit sind wir fertig. ■

Beweis von (f). INDUKTIONSANFANG: Es ist

$$\sum_{i=0}^1 (i \cdot i!) = 0 \cdot 0! + 1 \cdot 1! = 1 = 2 - 1 = (1+1)! - 1,$$

also ist die Behauptung wahr für $n = 1$.

INDUKTIONSVORAUSSETZUNG: Sei $n \geq 2$ eine natürliche Zahl so, dass die Gleichung für $n - 1$ wahr ist. Das bedeutet $\sum_{i=0}^{n-1} (i \cdot i!) = n! - 1$.

INDUKTIONSSCHRITT: Umformen und einsetzen liefert

$$\sum_{i=0}^n (i \cdot i!) = \sum_{i=0}^{n-1} (i \cdot i!) + n \cdot n! = n! - 1 + n \cdot n! = (1+n)n! - 1 = (n+1)! - 1. \quad \blacksquare$$

Beweis von (g). INDUKTIONSANFANG: Es ist

$$\sum_{k=1}^1 \frac{1}{k(k+1)} = \frac{1}{2} = \frac{1}{1+1},$$

also stimmt die Behauptung für $n = 1$.

INDUKTIONSVORAUSSETZUNG: Sei $n \geq 2$ eine natürliche Zahl so, dass die Gleichung für $n - 1$ wahr ist. Das bedeutet

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

INDUKTIONSSCHRITT: Wieder formen wir um, setzen die Gleichung für $n - 1$ ein und erhalten

$$\begin{aligned} \sum_{k=1}^n \frac{1}{k(k+1)} &= \sum_{k=1}^{n-1} \frac{1}{k(k+1)} + \frac{1}{n(n+1)} = \frac{n-1}{n} + \frac{1}{n(n+1)} \\ &= \frac{(n-1)(n+1) + 1}{n(n+1)} = \frac{n^2 - n + n - 1 + 1}{n(n+1)} = \frac{n^2}{n(n+1)} = \frac{n}{n+1} \end{aligned}$$

wie behauptet. ■

Aufgabe 1.1.9.

Behauptung (a). Für alle $n \in \mathbb{N}$ ist $n^5 - n$ durch 5 teilbar.

Beweis. Wir beweisen das mit vollständiger Induktion.

INDUKTIONSANFANG: Für $n = 1$ haben wir $n^5 - n = 1 - 1 = 0$, und 0 ist durch 5 teilbar.

INDUKTIONSVORAUSSETZUNG: Sei $n \geq 1$ so, dass die Aussage richtig ist, dass also $n^5 - n$ durch 5 teilbar ist.

INDUKTIONSSCHRITT: Wir verwenden den Binomischen Lehrsatz (1.1.5):

$$\begin{aligned} (n+1)^5 - (n+1) &= (n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1) - (n+1) \\ &= (n^5 - n) + 5 \cdot (n^4 + 2n^3 + 2n^2 + n). \end{aligned}$$

Nach Induktionsvoraussetzung ist $n^5 - n$ durch 5 teilbar, und $5 \cdot (n^4 + 2n^3 + 2n^2 + n)$ ist natürlich auch durch 5 teilbar. Damit ist $(n+1)^5 - (n+1)$ durch 5 teilbar, wie behauptet. ■

Für Teil (b) geben wir ein Gegenbeispiel an: $2^4 - 2 = 16 - 2 = 14$ ist *nicht* durch 4 teilbar.

Beim Versuch, den Beweis aus (a) nachzuahmen, fällt uns auf, dass in (a) alle nicht-trivialen Binomialkoeffizienten durch 5 teilbar waren, aber hier sind die nicht-trivialen Binomialkoeffizienten die Zahlen 4 und 6, und 6 ist *nicht* durch 4 teilbar. Daher können wir nicht wie in (a) argumentieren. (Das ist ein allgemeines Phänomen, wie wir in Hilfssatz 3.2.3 sehen.)

Aufgabe 1.1.10. Gegeben seien n paarweise nicht parallele Geraden $g_1, \dots, g_n$ in der Ebene, wobei sich in keinem Punkt der Ebene mehr als zwei Geraden schneiden sollen. Wir fragen uns, in wie viele Teile die Ebene von diesen n Geraden zerteilt wird. Die Idee hier ist wie folgt (und dabei hilft es, ein Bildchen zu malen):

Eine Gerade g_1 teilt die Ebene in zwei Teile E_1 und E_2 . Eine weitere, nicht zu g_1 parallele Gerade g_2 schneidet g_1 genau einmal und teilt deshalb E_1 und E_2 jeweils einmal. Nun haben wir also die Ebene in vier Teile zerlegt. Eine weitere Gerade g_3 , die weder zu g_1 noch zu g_2 parallel ist, hat mit g_1 und g_2 jeweils genau einen Schnittpunkt, und nach Voraussetzung sind diese verschieden. Wir haben also zwei neue Schnittpunkte und deshalb werden drei der vorherigen Ebenenstücke erneut geteilt. Das ergibt zusammen sieben Teile, in die die Ebene von g_1, g_2 und g_3 zerlegt wird.

Behauptung. Definiere $k_n := \frac{n \cdot (n+1)}{2} + 1$. Dann wird die Ebene von n paarweise nicht parallelen Geraden, von denen sich niemals mehr als zwei im gleichen Punkt der Ebene schneiden, stets in k_n Stücke zerteilt.

Beweis. Für $n = 1$, also genau eine Gerade, ist das wahr, denn $k_1 = \frac{1 \cdot 2}{2} + 1 = 2$.

Für den Induktionsschritt müssen wir etwas nachdenken. Es sei $n \geq 2$ so, dass die Behauptung für $n - 1$ richtig ist. Wir müssen sie nun für n nachweisen.

Gegeben seien dazu n Geraden wie in der Behauptung. Die ersten $n - 1$ davon zerteilen die Ebene dann nach Induktionsvoraussetzung in k_{n-1} Teile. Die nächste Gerade schneidet dann jede dieser $n - 1$ Geraden genau einmal, und dabei werden n der bereits vorhandenen Teilstücke der Ebene erneut zerteilt, also wird die Ebene insgesamt in

$$\begin{aligned} k_{n-1} + n &= \frac{n \cdot (n-1)}{2} + 1 + n \\ &= \frac{n \cdot (n-1) + 2n}{2} + 1 = \frac{n \cdot (n-1+2)}{2} + 1 = \frac{n \cdot n + 1}{2} + 1 = k_n \end{aligned}$$

Stücke zerteilt, wie behauptet. ■

Wenn doch einige der Geraden parallel sein dürfen, verringert sich die Anzahl der Stücke, in die die Ebene zerlegt wird. Um eine Idee für die Lösung zu bekommen, schlagen wir vor, zuerst den Fall zu betrachten, dass immer genau zwei Geraden parallel sein dürfen, dann drei,...

Aufgabe 1.1.11. Es seien $k, n \in \mathbb{N}_0$ mit $k \leq n$. Der Binomialkoeffizient $\binom{n}{k}$ zählt nach unserer intuitiven „Definition“, wie viele Möglichkeiten es gibt, k paarweise verschiedene Zahlen aus $1, \dots, n$ auszuwählen.

Zuerst ein Kommentar zu Teil (a): Wenn wir k paarweise verschiedene Zahlen aus der Menge $\{1, \dots, n+1\}$ auswählen, dann gibt es zwei Fälle. Entweder kommt die Zahl $n+1$ in unserer Auswahl vor oder nicht. Im ersten Fall wählen wir dann $k-1$ Elemente aus $\{1, \dots, n\}$ aus und ergänzen die Zahl $n+1$. Dies ergibt $\binom{n}{k-1}$ Möglichkeiten. Im

zweiten Fall brauchen wir die Zahl $n+1$ gar nicht und kommen daher auf $\binom{n}{k}$ zusätzliche Möglichkeiten.

Für (b) beginnen wir intuitiv. Hier ist eine Möglichkeit, eine Auswahl von k paarweise verschiedenen Zahlen aus der Menge $\{1, \dots, n\}$ vorzunehmen: Wir schreiben die Zahlen $1, \dots, n$ in beliebiger Reihenfolge hintereinander auf, und nehmen dann die ersten k Zahlen. Nun gibt es $n!$ Möglichkeiten (verschiedene Reihenfolgen), die Zahlen $1, \dots, n$ hinzuschreiben. Damit zwei solche Reihen die gleiche ausgewählte Menge von k Zahlen repräsentieren, muss Folgendes erfüllt sein:

- Die ersten k Zahlen müssen genau die ausgewählten sein, unabhängig von ihrer Reihenfolge.
- Die Elemente auf den Plätzen $k+1$ bis n in der Reihe müssen genau die nicht ausgesuchten Zahlen sein, wieder unabhängig von der Reihenfolge.

Das liefert also für jede Wahl von k Zahlen genau $k!(n-k)!$ Reihen, die alle diese gewisse Auswahl repräsentieren. Die Anzahl der Möglichkeiten, k Zahlen aus $1, \dots, n$ auszuwählen, ist also die Anzahl $n!$ aller verschiedenen Reihen geteilt durch $k!(n-k)!$:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (1.1)$$

Jetzt beweisen wir, für Teil (c), die Formel (1.1) formal mit Hilfe der rekursiven Definition von Binomialkoeffizienten, an die wir uns noch einmal kurz erinnern:

$$\binom{0}{0} = 1, \quad \binom{0}{k} = 0 \ (k \neq 0) \quad \text{und} \quad \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

für alle $n, k \in \mathbb{N}_0$.

INDUKTIONSANFANG: Für $n = 0$ ist $\binom{0}{0} = 1$ und andererseits $\frac{0!}{0! \cdot 0!} = 1$.

INDUKTIONSVORAUSSSETZUNG: Sei $n \in \mathbb{N}$ so, dass $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ gilt für alle $k \leq n$.

INDUKTIONSSCHRITT: Es sei $k \in \mathbb{N}_0$ mit $k \leq n+1$. Ist $k = 0$ oder $k = n+1$, so ist

$$\binom{n+1}{k} = 1 = \frac{(n+1)!}{0!(n+1)!} = \frac{(n+1)!}{k!(n+1-k)!}.$$

Sei also $1 \leq k \leq n$. Nach der Induktionsvoraussetzung und unserer Rekursionsformel gilt dann

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-(k-1))!}.$$

Also folgt

$$\begin{aligned}
 \binom{n+1}{k} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-(k-1))!} \\
 &= \frac{(n-k+1) \cdot n! + k \cdot n!}{k!(n-k+1)!} \\
 &= \frac{n \cdot n! - k \cdot n! + n! + k \cdot n!}{k!(n-k+1)!} \\
 &= \frac{n \cdot n! + n!}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n-k+1)!},
 \end{aligned}$$

und wir sind fertig.

Aufgabe 1.1.12. Es seien $n, k, \ell \in \mathbb{N}_0$.

Behauptung. Es gilt:

- (a) $\binom{n+\ell}{k} \geq \binom{n}{k}$;
- (b) $\binom{n+\ell}{k+\ell} \geq \binom{n}{k}$;
- (c) $\binom{2n}{n} \geq 2^n$.

Beweisskizze. Die ersten beiden Behauptungen besagen: Gehen wir im Pascalschen Dreieck (Abbildung 1.1) diagonal nach links bzw. rechts unten, so werden die Einträge nicht kleiner. Das ist klar: Jeder Eintrag ist die Summe der beiden diagonal über ihm stehenden, und es gibt keine negativen Einträge. Einen formalen Beweis führt man durch Induktion über ℓ und unter Verwendung der Rekursionsformel für die Binomialkoeffizienten – wir überlassen das der Leserin.

Teil (c) beweisen wir jetzt durch Induktion mit Hilfe der ersten beiden Teilaufgaben. Für $n = 0$ ist die Ungleichung richtig, denn es gilt $\binom{0}{0} = 1$ und $2^0 = 1$. Das ist der Induktionsanfang.

Jetzt nehmen wir an, dass die Behauptung für n richtig ist, und wollen sie für $n+1$ daraus ableiten. Es gilt

$$\begin{aligned}
 \binom{2(n+1)}{n+1} &= \binom{2n+1}{n} + \binom{2n+1}{n+1} \geq \binom{2n}{n} + \binom{2n}{n} \\
 &= 2 \cdot \binom{2n}{n} \geq 2 \cdot 2^n = 2^{n+1}.
 \end{aligned}$$

Dabei haben wir in der ersten Zeile die rekursive Definition und die ersten beiden Aufgabenteile angewendet und in der zweiten die Induktionsvoraussetzung. ■

Aufgabe 1.1.13. Es seien $n, m \in \mathbb{N}_0$. Die Anzahl der Möglichkeiten, ohne Berücksichtigung der Reihenfolge bis zu m (nicht notwendigerweise verschiedene) Zahlen zwischen 1 und n auszuwählen, werde mit $a(n, m)$ bezeichnet.

Wir behaupten, dass $a(n, m)$ die Rekursionsformel

$$a(n, m) = a(n-1, m) + a(n, m-1)$$

erfüllt. Wenn wir nämlich bis zu m (nicht notwendigerweise verschiedene) Zahlen zwischen 1 und n aussuchen, dann gibt es zwei Möglichkeiten: Entweder ist n dabei oder nicht. Falls n bei den ausgesuchten Zahlen vorkommt, dann gibt es einen freien Platz weniger für die restlichen Zahlen und daher ist die Anzahl dieser Möglichkeiten $a(n, m-1)$. (Wir erinnern daran, dass die gleiche Zahl mehrmals ausgesucht werden darf – deshalb steht hier n und nicht $n-1$.)

Falls n nicht in der Auswahl vorkommt, dann ist es so, als würden wir nur aus den Zahlen $1, \dots, n-1$ aussuchen, daher ist die Anzahl dieser Möglichkeiten $a(n-1, m)$. Die Anzahl aller Möglichkeiten muss dann die Summe dieser beiden Ausdrücke sein.

Behauptung. Es gilt $a(n, m) = \binom{n+m}{m}$ für alle $n, m \in \mathbb{N}_0$.

Beweis. Wir führen Induktion über $n+m$. Das heißt, wir beweisen folgende Aussage für alle $\ell \in \mathbb{N}_0$: Sind $n, m \in \mathbb{N}_0$ mit $n+m = \ell$, so gilt

$$a(n, m) = \binom{n+m}{m}.$$

INDUKTIONSANFANG: Es gilt $a(0, 0) = 1 = \binom{0}{0}$, also ist die Behauptung für $\ell = 0$ richtig.

INDUKTIONSVORAUSSETZUNG: Es sei $\ell \geq 1$ derart, dass die Behauptung für $\ell-1$ richtig ist. Insbesondere gilt dann: Sind $m, n \geq 1$ mit $m+n = \ell$, so ist

$$a(n-1, m) = \binom{n+m-1}{m} \quad \text{und} \quad a(n, m-1) = \binom{n+m-1}{m-1}.$$

INDUKTIONSSCHRITT: Seien jetzt $m, n \in \mathbb{N}_0$ mit $\ell = m+n$. Ist $m = 0$ oder $n = 0$, so gilt $a(n, m) = 1$ und $\binom{n+m}{m} = 1$, also ist die Behauptung in diesem Fall richtig.

Andernfalls können wir die Rekursionsformel für $a(n, m)$, die Induktionsvoraussetzung und die Rekursionsformel für Binomialkoeffizienten anwenden:

$$\begin{aligned} a(n, m) &= a(n-1, m) + a(n, m-1) \\ &= \binom{n+m-1}{m} + \binom{n+m-1}{m-1} = \binom{n+m}{m}. \end{aligned}$$

■

Aufgabe 1.1.14.

Behauptung. Für die Folge f_n der Fibonacci-Zahlen gilt:

$$f_n = \frac{(1 + \sqrt{5})^n - (1 - \sqrt{5})^n}{2^n \cdot \sqrt{5}}.$$

Beweis. Wir argumentieren mit vollständiger Induktion, Variante (c).

INDUKTIONSANFANG: Es gilt

$$f_1 = 1 = \frac{2 \cdot \sqrt{5}}{2 \cdot \sqrt{5}} = \frac{(1 + \sqrt{5}) - (1 - \sqrt{5})}{2 \cdot \sqrt{5}}$$

und

$$f_2 = 1 = \frac{4 \cdot \sqrt{5}}{4 \cdot \sqrt{5}} = \frac{(1 + 2\sqrt{5} + 5) - (1 - 2\sqrt{5} + 5)}{4 \cdot \sqrt{5}} = \frac{(1 + \sqrt{5})^2 - (1 - \sqrt{5})^2}{2^2 \cdot \sqrt{5}}.$$

Damit ist die Behauptung für $n = 1$ und $n = 2$ richtig.

INDUKTIONSVORAUSSETZUNG: Sei $n \geq 3$ so, dass $f_k = \frac{(1+\sqrt{5})^k - (1-\sqrt{5})^k}{2^k \cdot \sqrt{5}}$ ist für alle natürlichen Zahlen $k < n$ (und damit insbesondere für $k = n - 2$ und $k = n - 1$).

INDUKTIONSSCHRITT: Nach Definition und Induktionsvoraussetzung ist

$$\begin{aligned} f_n &= f_{n-2} + f_{n-1} = \frac{(1 + \sqrt{5})^{n-2} - (1 - \sqrt{5})^{n-2}}{2^{n-2} \cdot \sqrt{5}} + \frac{(1 + \sqrt{5})^{n-1} - (1 - \sqrt{5})^{n-1}}{2^{n-1} \cdot \sqrt{5}} \\ &= \frac{(4(1 + \sqrt{5})^{n-2} - 4(1 - \sqrt{5})^{n-2}) + (2(1 + \sqrt{5})^{n-1} - 2(1 - \sqrt{5})^{n-1})}{2^n \cdot \sqrt{5}} \\ &= \frac{4(1 + \sqrt{5})^{n-2} + 2(1 + \sqrt{5})^{n-1} - 4(1 - \sqrt{5})^{n-2} - 2(1 - \sqrt{5})^{n-1}}{2^n \cdot \sqrt{5}} \\ &= \frac{((1 + \sqrt{5})^{n-2} \cdot 2(2 + (1 + \sqrt{5}))) - ((1 - \sqrt{5})^{n-2} \cdot (2(2 + (1 + \sqrt{5}))))}{2^n \cdot \sqrt{5}} \\ &= \frac{((1 + \sqrt{5})^{n-2} \cdot (6 + 2\sqrt{5})) - ((1 - \sqrt{5})^{n-2} \cdot (6 - 2\sqrt{5}))}{2^n \cdot \sqrt{5}}. \end{aligned}$$

Aber $(1 + \sqrt{5})^2 = 1 + 2\sqrt{5} + 5 = 6 + 2\sqrt{5}$ und genauso ist $(1 - \sqrt{5})^2 = 6 - 2\sqrt{5}$, also folgt insgesamt

$$\begin{aligned} f_n &= f_{n-2} + f_{n-1} = \frac{((1 + \sqrt{5})^{n-2} \cdot (6 + 2\sqrt{5})) - ((1 - \sqrt{5})^{n-2} \cdot (6 - 2\sqrt{5}))}{2^n \cdot \sqrt{5}} \\ &= \frac{(1 + \sqrt{5})^n - (1 - \sqrt{5})^n}{2^n \cdot \sqrt{5}} \end{aligned}$$

wie behauptet. ■

Aufgabe 1.1.17. Die rekursiven Definitionen von $n+m$, $n \cdot m$ und n^m mit Hilfe der Nachfolgerfunktion bauen aufeinander auf. Nach Voraussetzung ist $n+1$ für jede natürliche Zahl bereits definiert; rekursiv können wir dann

$$n + (m + 1) := (n + m) + 1$$

setzen. (Das heißt, den Nachfolger einer Zahl m zu n zu addieren ist dasselbe, wie erst m und n zu addieren und dann den Nachfolger zu bilden.)

Für die rekursive Definition von $n \cdot m$ können wir jetzt die gerade definierte Addition verwenden:

$$n \cdot 1 := n; \quad n \cdot (m + 1) := n \cdot m + n.$$

Genauso verfahren wir für die Potenzbildung:

$$n^1 := n; \quad n^{m+1} := n \cdot n^m.$$

Aufgabe 1.1.18. *Hinweis.* Es sei A eine Menge natürlicher Zahlen, welche kein kleinstes Element enthält. Beweise dann durch Induktion, dass keine natürliche Zahl Element von A sein kann; d.h. A ist leer.

(Für einen direkteren Beweis kann man auch alternativ durch Induktion folgende Aussage beweisen: Ist A eine Teilmenge von $\mathbb{N}$ mit $n \in A$, so hat A ein kleinstes Element.)

Aufgabe 1.1.22. Wir haben nicht genau gesagt, was es bedeutet, „eine natürliche Zahl durch einen Satz zu beschreiben“. Welche Sätze sind erlaubt, und wenn beschreiben sie eine natürliche Zahl? Es gibt zwar viele Möglichkeiten, das festzulegen, aber das Problem ist die „Selbstreferenz“ unseres Beispiels: Einen Widerspruch erhielten wir nur dann, wenn dann auch der Satz „die kleinste natürliche Zahl, die nicht durch einen weniger als zweihundert Buchstaben umfassenden Satz beschrieben werden kann“ im Sinne unserer Definition wieder eine natürliche Zahl beschreibt. Der „Beweis“ zeigt dann gerade, dass dies – unabhängig von dieser Definition – niemals der Fall sein kann.

Dieses Beispiel, welches (unter anderem) zeigt, dass man manchmal mit informellen mathematischen Argumenten vorsichtig sein muss, wird als das **Berry-Paradoxon** bezeichnet. Es ist eng verwandt mit den Sätzen von Turing und Gödel, die wir in Abschnitt 2.2 und den dortigen weiterführenden Anmerkungen ansprechen werden.

Aufgabe 1.2.5. (a) Falsch. Gegenbeispiel: 4 teilt $8 = 3 + 5$, aber 4 teilt weder 3 noch 5.

(b) Falsch. Gegenbeispiel: 6 teilt $12 = 3 \cdot 4$, aber 6 teilt weder 3 noch 4.

(c) Falsch, mit dem gleichen Gegenbeispiel wie in (b).

(d) Richtig. Beweis: Wir haben vorausgesetzt, dass m durch k teilbar ist, n aber nicht.

Angenommen, k sei ein Teiler von $m+n$. Dann seien $c, d \in \mathbb{Z}$ so, dass $m+n = k \cdot c$ ist und $m = k \cdot d$. Nun folgt $n = (m+n) - m = k \cdot c - k \cdot d = k \cdot (c-d)$, also ist n doch durch k teilbar, ein Widerspruch.

- (e) Falsch. Gegenbeispiel: 3 teilt 6 und nicht 5, aber 3 teilt $6 \cdot 5 = 30$. Dahinter steckt ein allgemeines Resultat, nämlich dass jeder Teiler k von m auch jedes Vielfache von n teilt.

Beweis dafür: Sei $c \in \mathbb{Z}$ mit $m = k \cdot c$ und sei v ein Vielfaches von m , also $v = a \cdot m$ mit geeignetem $a \in \mathbb{Z}$. Dann ist $v = a \cdot m = a \cdot (k \cdot c)$, und damit ist auch v durch k teilbar.

- (f) Richtig. Beweis: m und n werden von k mit Rest 1 geteilt, seien also $c, d \in \mathbb{Z}$ so, dass $n = c \cdot k + 1$ ist und $m = d \cdot k + 1$. Dann haben wir $n \cdot m = (c \cdot k + 1)(d \cdot k + 1) = c \cdot d \cdot k^2 + c \cdot k + d \cdot k + 1$, und deshalb ist auch $n \cdot m$ mit Rest 1 durch k teilbar.

- (g) Falsch. Gegenbeispiel: 3 teilt 4 und 7 jeweils mit Rest 1, aber 3 teilt $4 + 7 = 11$ mit Rest 2.

Zu (f) und (g) vergleiche auch Aufgabe 1.2.7.

Aufgabe 1.2.6.

Behauptung. Es sei n eine natürliche Zahl.

- (a) Ist $n > 1$, so gibt es eine Primzahl p mit $p \mid n$.
 (b) Ist $n > 1$ eine zusammengesetzte Zahl, so gibt es einen nicht-trivialen Teiler k von n mit $k^2 \leq n$.

Beweis von (a). Wegen $n > 1$ gibt es genau zwei Möglichkeiten:

- n ist eine Primzahl oder
- n ist zusammengesetzt.

Im ersten Fall setzen wir $p := n$ und sind fertig. (Jede Zahl teilt sich selbst!) Ist n zusammengesetzt, so betrachten wir die Menge $T := \{k \in \mathbb{N} : k > 1 \text{ und } k \mid n\}$. Das ist eine nicht-leere Menge, denn sie enthält sicherlich n . Nach dem Wohlordnungsprinzip besitzt sie ein kleinstes Element k_0 . Wegen $k_0 \neq 1$ ist k_0 entweder prim oder zusammengesetzt. Sei $m \neq 1$ ein Teiler von k_0 . Dann ist m auch ein Teiler von n und daher liegt m selbst in T . Da wir k_0 als kleinstes Element von T gewählt haben, muss $m = k_0$ sein. Wir haben gezeigt, dass k_0 genau zwei verschiedene Teiler besitzt, nämlich 1 und sich selbst. Daher ist k_0 prim. Also ist k_0 eine Primzahl, die n teilt, wie behauptet. ■

Beweis von (b). Sei jetzt $n > 1$ eine zusammengesetzte natürliche Zahl. Dann finden wir $a, b \in \mathbb{N}$ mit $a, b \neq 1$ und so, dass $n = a \cdot b$ ist. Im Falle $a \leq b$ gilt $a^2 \leq a \cdot b = n$, also ist a ein nicht-trivialer Teiler mit der gewünschten Eigenschaft. Genauso argumentieren wir, falls $b < a$ ist, dann ist nämlich b wie gefordert. ■

Aufgabe 1.2.7. Nach Voraussetzung existieren $c, d \in \mathbb{Z}$ mit $a = c \cdot k + r$ und $b = d \cdot k + s$.

Behauptung. k teilt $a + b$ mit Rest $r + s$ oder $r + s - k$, k teilt $a - b$ mit Rest $r - s$ oder $r - s + k$; d.h. $a + b$ und $a - b$ haben beim Teilen durch k den gleichen Rest wie $r + s$ bzw. $r - s$. Ebenso hat $a \cdot b$ beim Teilen durch k den gleichen Rest wie $r \cdot s$.

Beweis. $a + b = (c \cdot k + r) + (d \cdot k + s) = c \cdot k + d \cdot k + r + s$, und beim Teilen durch k bleibt zunächst die Zahl $r + s$ übrig. Das muss aber nicht zwangsläufig der Rest sein! Etwa sind 8 und 9 mit Resten 3 bzw. 4 durch 5 teilbar, aber $17 = 8 + 9$ hat beim Teilen durch 5 den Rest 2 und nicht $7 = 3 + 4$. Der Rest ist also $r + s$, falls diese Zahl echt kleiner als k ist, andernfalls ist der Rest $r + s - k$.

$a - b = (c \cdot k + r) - (d \cdot k + s) = c \cdot k - d \cdot k + r - s$ hat zunächst den Rest $r - s$ beim Teilen durch k . Falls das eine negative Zahl ist, dann ist der Rest von $a - b$ beim Teilen durch k aber $r - s + k$.

Schließlich ist $a \cdot b = (c \cdot k + r) \cdot (d \cdot k + s) = c \cdot d \cdot k^2 + c \cdot k \cdot s + d \cdot k \cdot r + r \cdot s$, und beim Teilen durch k bleibt $r \cdot s$ übrig. Also ist der Rest von $a \cdot b$ beim Teilen durch k der gleiche wie der von $r \cdot s$. ■

Aufgabe 1.2.8. Falls n selbst durch 3 teilbar ist, sind wir fertig. Andernfalls teilen wir n mit Rest durch 3. Nun gibt es zwei Möglichkeiten - der Rest ist entweder 1 oder 2. Im ersten Fall hat (mit Aufgabe 1.2.7 oben) $n + 2$ beim Teilen durch 3 den Rest $1 + 2 = 3$, also ist $n + 2$ durch 3 teilbar. Genauso ist im zweiten Fall $n + 1$ durch 3 teilbar. Da eine Zahl nur entweder Rest 0, 1 oder 2 beim Teilen durch 3 haben kann, tritt genau einer der genannten Fälle ein, d.h. genau eine der Zahlen n , $n + 1$ oder $n + 2$ ist durch 3 teilbar.

Aufgabe 1.2.9. Da n ungerade ist, ist n nicht durch 2 teilbar. Insbesondere ist n nicht durch 4 teilbar. Wir teilen n mit Rest durch 4 und schreiben $n = 4a + r$ mit $a, r \in \mathbb{Z}$ und $0 < r < 4$. Dann ist $r \in \{1, 2, 3\}$. Angenommen, $r = 2$. Dann ist $n = 4a + 2$ durch 2 teilbar, also gerade, ein Widerspruch. Deshalb muss $r = 1$ sein oder $r = 3$. Im ersten Fall ist $r - 1 = 0$ durch 4 teilbar (also auch $n - 1$), im zweiten Fall ist $r + 1$ durch 4 teilbar (also auch $n + 1$), mit Aufgabe 1.2.7. Da n beim Teilen durch 4 nur genau einen Rest haben kann, tritt auch nur genau einer der genannten Fälle ein.

Aufgabe 1.2.10.

Behauptung. Es seien a, b, c, d ganze Zahlen mit $a \mid b$ und $c \mid d$. Dann gilt $ac \mid bd$.

Beweis. Nach Voraussetzung existieren ganze Zahlen s, t so, dass $as = b$ ist und $ct = d$. Daraus folgt $bd = asct = (ac)(st)$, und da st eine ganze Zahl ist, bedeutet das, dass ac ein Teiler ist von bd . ■

Aufgabe 1.2.11. Seien $a, b \in \mathbb{Z}$. Zuerst setzen wir voraus, dass $2a + b$ durch 7 teilbar ist und zeigen, dass dann $100a + b$ durch 7 teilbar ist. Anschließend beweisen wir die Umkehrung.

Sei $c \in \mathbb{Z}$ so, dass $7c = 2a + b$ ist. Dann ist $2a = 7c - b$, also $100a = 50(7c - b) = 350c - 50b$. Daraus folgt nun $100a + b = 350c - 49b = 7(50c - 7b)$, und diese Zahl ist durch 7 teilbar.

Setzen wir nun umgekehrt voraus, dass $100a + b$ von 7 geteilt wird, dass wir also schreiben können $100a + b = 7d$ mit einer geeigneten Zahl $d \in \mathbb{Z}$. Dann ist $2a = 100a - 98a = 7d - b - 98a$, also $2a + b = 7d - 98a = 7(d - 14a)$ durch 7 teilbar wie behauptet.

Aufgabe 1.2.12. Sei $n \in \mathbb{N}$ und p eine Primzahl, die n nicht teilt. Wir setzen $d := \text{ggT}(p, n)$. Dann ist d ein Teiler von p , nach Definition von Primzahlen also $d = p$ oder $d = 1$. Im ersten Fall ist p jedoch ein Teiler von n , ein Widerspruch. Also muss $d = 1$ sein, was zu zeigen war.

Aufgabe 1.3.4. $600 = 2^3 \cdot 3 \cdot 5^2$, $851 = 23 \cdot 37$ und $1449 = 3^2 \cdot 7 \cdot 23$.

Aufgabe 1.3.5. Die Primfaktorzerlegungen sind $1961 = 37 \cdot 53$ und $1591 = 37 \cdot 43$, also ist $\text{ggT}(1961, 1591) = 37$. Man findet die Zerlegungen, indem man nach und nach durch die ersten Primzahlen (2, 3, 5, 7, 11, ...) teilt.

Aufgabe 1.3.6. Es seien $a, b \in \mathbb{Z}$. Setze $d := \text{ggT}(a, b)$ und $k := \text{kgV}(a, b)$.

Behauptung. (a) $\frac{a}{d}$ und $\frac{b}{d}$ sind teilerfremd.

(b) Ist v ein gemeinsames Vielfaches von a und b , so gilt $k \mid v$.

(c) Es gilt $d \cdot k = |a \cdot b|$. Ist $d = 1$, so gilt insbesondere $k = |a \cdot b|$.

Beweis von (a). Es sei $m \in \mathbb{N}$ ein gemeinsamer Teiler von $\frac{a}{d}$ und $\frac{b}{d}$. Dann ist $m \cdot d$ ein gemeinsamer Teiler von a und b . Da d der ggT ist, gilt also $m \cdot d \leq d$, und daher $m = 1$. Es folgt $\text{ggT}(\frac{a}{d}, \frac{b}{d}) = 1$, wie behauptet. ■

Beweis von (b). Wir teilen v mit Rest durch k , schreiben also

$$v = q \cdot k + r$$

mit $0 \leq r < k$. Wir können das umschreiben als

$$r = v - q \cdot k.$$

Da v und k beide von a geteilt werden, ist a auch ein Teiler von r . Ebenso ist b ein Teiler von r . Also ist r ein gemeinsames Vielfaches von a und b . Nach Definition von $k = \text{kgV}(a, b)$ und Wahl von r kann dann r keine natürliche Zahl sein, d.h. es gilt $r = 0$. Daher ist $v = q \cdot k$ und damit $k \mid v$, wie behauptet. ■

Beweis von (c). Wir müssen zeigen, dass

$$d = \frac{|a \cdot b|}{k}$$

gilt. Zunächst einmal ist $|a \cdot b|$ ein gemeinsames Vielfaches von a und b , also ist k nach (b) ein Teiler von $|a \cdot b|$. Daher ist $m := \frac{|a \cdot b|}{k}$ eine natürliche Zahl.

Es ist

$$\frac{a \cdot b}{d} = a \cdot \frac{b}{d} = b \cdot \frac{a}{d}$$

ein gemeinsames Vielfaches von a und b . Also gilt $\frac{|a \cdot b|}{d} \geq k$ und daher $d \leq m$.

Wir wollen zeigen, dass m ein gemeinsamer Teiler von a und b ist. Dazu schreiben wir $k = a \cdot b_1$ mit $b_1 \in \mathbb{Z}$. Dann ist

$$m = \frac{a \cdot b}{k} = \frac{a \cdot b}{a \cdot b_1} = \frac{b}{b_1},$$

und daher ist $b = m \cdot b_1$, und somit m ein Teiler von b .

Auf dieselbe Art und Weise sehen wir, dass m ein Teiler von a ist. Also ist m ein gemeinsamer Teiler von a und b mit $m \geq d$ und $m \in \mathbb{N}$. Nach Definition des größten gemeinsamen Teilers gilt also $m = d$, wie behauptet. ■

Aufgabe 1.3.7.

Behauptung. Seien a, b, c ganze Zahlen, wobei c das Produkt $a \cdot b$ teilt.

Dann ist c auch ein Teiler von $\text{ggT}(a, c) \cdot \text{ggT}(b, c)$.

Beweis. Mit dem Lemma von Bézout gibt es ganze Zahlen k, l, m, n derart, dass $\text{ggT}(a, c) = ka + lc$ ist und $\text{ggT}(b, c) = mb + nc$. Dann haben wir

$$\text{ggT}(a, c) \cdot \text{ggT}(b, c) = (ka + lc)(mb + nc) = kmab + knac + lmcb + lnc^2.$$

Die letzten drei Terme sind durch c teilbar, und nach Voraussetzung teilt c auch ab , also den ersten Term und damit das Produkt auf der linken Seite. ■

Aufgabe 1.4.4. Zuerst berechnen wir $\text{ggT}(135, 36)$ und dessen Darstellung:

$$135 = 3 \cdot 36 + 27, \quad 36 = 27 + 9,$$

und 27 ist durch 9 teilbar. Also ist $\text{ggT}(135, 36) = 9$ und

$$9 = 36 - 27 = 36 - (135 - 3 \cdot 36) = 4 \cdot 36 - 135.$$

Für $\text{ggT}(851, 1449)$ erhalten wir:

$$1449 = 851 + 598, \quad 598 = 2 \cdot 253 + 92, \quad 253 = 2 \cdot 92 + 69 \quad \text{und} \quad 92 = 69 + 23.$$

Da 69 durch 23 teilbar ist, folgt $\text{ggT}(135, 36) = 23$. Weiter ist

$$\begin{aligned} 23 &= 92 - 69 = 92 - (253 - 2 \cdot 92) = 3 \cdot 92 - 253 = 3 \cdot (598 - 2 \cdot 253) - 253 \\ &= 3 \cdot 598 - 7 \cdot 253 = 3 \cdot 598 - 7 \cdot (851 - 598) \\ &= 10 \cdot 598 - 7 \cdot 851 = 10 \cdot (1449 - 851) - 7 \cdot 851 = 10 \cdot 1449 - 17 \cdot 851. \end{aligned}$$

Aufgabe 1.4.5. Für den Euklidischen Algorithmus berechnen wir

$$1961 = 1591 + 370, \quad 1591 = 4 \cdot 370 + 111, \quad 370 = 3 \cdot 111 + 37$$

und 111 ist durch 37 teilbar, also haben wir $\text{ggT}(1961, 1591) = 37$.

In diesem Beispiel ging es wesentlich schneller (für uns jedenfalls!) mit dem Euklidischen Algorithmus als mit der Zerlegung aus Aufgabe 1.3.5.

Aufgabe 1.4.6. Es seien a und b teilerfremde ganze Zahlen.

Behauptung. Es gilt $\text{ggT}(a^2 - b^2, a + b) = |a + b|$ (sogar unabhängig von der Teilerfremdheitsvoraussetzung). Außerdem gilt $\text{ggT}(a^2 + b^2, a + b) = 1$, falls a oder b gerade ist und $\text{ggT}(a^2 + b^2, a + b) = 2$, falls a und b ungerade sind.

Beweis. Nach der binomischen Formel gilt $a^2 - b^2 = (a + b)(a - b)$, und das ist durch $a + b$ teilbar. Also ist $|a + b|$ der größte gemeinsame Teiler.

Nun betrachten wir die Zahl $d := \text{ggT}(a^2 + b^2, a + b)$. Wir stellen zuerst fest, dass die Voraussetzung $\text{ggT}(a, b) = 1$ impliziert, dass a und b nicht beide gerade sind. Wir können also der Einfachheit halber annehmen, dass b eine ungerade Zahl ist (sonst vertauschen wir einfach die Rollen von a und b .)

Nun ist $a + b$ ein Teiler von $a^2 - b^2$, wie wir gerade gesehen haben, und $a^2 + b^2 = (a^2 - b^2) + 2b^2$. Also ist nach Hilfssatz 1.3.1 d auch der größte gemeinsame Teiler von $2b^2$ und $a + b$.

Da a und b teilerfremd sind, sind auch b und $a + b$ teilerfremd (wieder wegen Hilfssatz 1.3.1). Mit Folgerung 1.3.5 ist auch b^2 teilerfremd zu $a + b$ und damit insbesondere zu d (denn d ist ein Teiler von $a + b$).

Jeder ungerade Teiler von $d = \text{ggT}(2b^2, a + b)$ ist ein ungerader Teiler von b^2 . Also folgt aus dem eben Gesagten, dass d keine nichttrivialen ungeraden Teiler hat. Da b ungerade ist, $2b^2$ also nicht von 4 geteilt wird, gilt also:

$$\begin{aligned} \text{ggT}(a^2 + b^2, a + b) &= 1, \text{ falls } a + b \text{ ungerade ist und} \\ \text{ggT}(a^2 + b^2, a + b) &= 2, \text{ falls } a + b \text{ gerade ist.} \end{aligned}$$

Der erste Fall tritt genau dann ein, wenn a gerade ist, und damit sind wir fertig. ■

Aufgabe 1.4.9. *Direkter Beweis des Lemmas von Bézout.* Ist $a = b = 0$, so folgt

$$\text{ggT}(a, b) = 0 = 0 \cdot a + 0 \cdot b,$$

also ist in diesem Fall nichts zu beweisen.

Andernfalls sei M die Menge aller natürlichen Zahlen, die sich als $ra + qb$ schreiben lassen mit $r, q \in \mathbb{Z}$. Diese Menge ist nicht leer, denn $|a| + |b|$ ist ein Element von M . Sei nun k das kleinste Element von M .

Wir behaupten, dass jedes Element $x \in M$ durch k teilbar ist. Dazu teilen wir x mit Rest durch k :

$$x = d \cdot k + c,$$

wobei $0 \leq c < k$ gilt. Nun gibt es nach Voraussetzung $s_1, t_1, s_2, t_2 \in \mathbb{Z}$ mit

$$k = s_1 \cdot a + t_1 \cdot b \quad \text{und} \quad x = s_2 \cdot a + t_2 \cdot b.$$

Also gilt

$$c = x - d \cdot k = (s_2 - d \cdot s_1)a + (t_2 - d \cdot t_1)b.$$

Andererseits ist $c < k$, und daher ist c kein Element von M . Also kann c keine natürliche Zahl sein; d.h. es gilt $c = 0$.

Insbesondere ist k ein gemeinsamer Teiler von a und b . Außerdem ist jeder Teiler von a und b auch ein Teiler von k (siehe die Lösung zu Aufgabe 1.3.13), also ist $k = \text{ggT}(a, b)$. ■

Aufgabe 1.4.10. Es seien $a, b \in \mathbb{Z}$. Nach dem Lemma von Bézout existieren ganze Zahlen s und t mit $\text{ggT}(a, b) = s \cdot a + t \cdot b$. Jeder gemeinsame Teiler von a und b ist auch ein Teiler von $s \cdot a + t \cdot b$.

Aufgabe 1.5.1. Durch Anwendung des Siebs des Eratosthenes erhalten wir die folgende Liste der Primzahlen, die kleiner sind als 400:

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, 211, 223, 227, 229, 233, 239, 241, 251, 257,
 263, 269, 271, 277, 281, 283, 293, 307, 311, 313,
 317, 331, 337, 347, 349, 353, 359, 367, 373, 379,
 383, 389, 397.

Aufgabe 1.6.3. Es sei $K \in \mathbb{N}$, und es sei P das Produkt aller Primzahlen $\leq K$. Dann sind $P + 2, P + 3, \dots, P + K$ alle zusammengesetzt, da jede der Zahlen $2, 3, \dots, K$ von einer Primzahl $\leq K$ geteilt wird, und daher mit P einen gemeinsamen Primfaktor hat.

Kapitel 2

Algorithmen

Aufgabe 2.3.4.

Behauptung (a). Es sei $f : \mathbb{N} \rightarrow \mathbb{R}$ eine Funktion und $\varepsilon > 0$ mit $f(n) > \varepsilon$ für alle $n \in \mathbb{N}$. Sei $C \in \mathbb{R}$ eine beliebige Konstante.

Dann gilt $f(n) + C = O(f(n))$.

Beweis. Es gilt für alle $n \in \mathbb{N}$:

$$|f(n) + C| \leq |f(n)| + |C| = |f(n)| \cdot \left(1 + \frac{C}{|f(n)|}\right) < |f(n)| \cdot \left(1 + \frac{C}{\varepsilon}\right).$$

Setzen wir also $K := 1 + \frac{C}{\varepsilon}$, so gilt $|f(n) + C| < K \cdot |f(n)|$ für alle n . Nach der Definition der O -Notation sind wir fertig. ■

Behauptung (b). Es seien $k, m \in \mathbb{N}_0$. Dann ist $x^k = O(x^m)$ genau dann, wenn $k \leq m$ ist.

Beweis. Ist $k \leq m$, so gilt $x^k \leq x^m$ für alle $x \in \mathbb{N}$, und daher ist $x^k = O(x^m)$.

Sei nun umgekehrt $k > m$ und C eine beliebige Konstante. Ist dann $x > C$, so gilt

$$x^k \geq x^{m+1} = x \cdot x^m > C \cdot x^m.$$

Damit haben wir gezeigt, dass nicht $x^k = O(x^m)$ gelten kann. ■

Behauptung (c). Ist P ein Polynom des Grades höchstens d , so gilt $P(n) = O(n^d)$.

Beweis. Es sei etwa $P = a_d X^d + \dots + a_1 X + a_0$ mit $a_0, \dots, a_d \in \mathbb{Z}$. Dann gilt für alle $n \in \mathbb{N}$:

$$P(n) = a_d n^d + \dots + a_1 n + a_0 \leq (a_d + \dots + a_1 + a_0) \cdot n^d. \quad \blacksquare$$

Behauptung (d). Für $a \leq 2$ ist $a^n = O(2^n)$. Für $a > 2$ gilt dies nicht.

Beweis. Die erste Behauptung ist klar, wegen $a^n \leq 2^n$.

Umgekehrt sei $a > 2$. Setzen wir $b := \frac{a}{2}$, so gilt also $b > 1$. Nun ist

$$a^n = (b \cdot 2)^n = b^n \cdot 2^n.$$

Wäre $a^n = O(2^n)$, so müsste $b^n \leq C$ gelten für ein geeignetes festes $C > 0$. Das ist aber nicht der Fall: Wegen $b > 1$ müsste sonst $n \leq \frac{\log b}{\log C}$ sein, was für genügend große n offensichtlich falsch ist. ■

Behauptung (e). Es sei $\varepsilon > 0$ eine reelle Zahl. Dann gilt $\log n = O(n^\varepsilon)$.

Beweis. Wir möchten zunächst auch auf der linken Seite einen Term n^ε einführen und schreiben dazu

$$\log n = \log((n^\varepsilon)^{\frac{1}{\varepsilon}}) = \frac{\log(n^\varepsilon)}{\varepsilon}.$$

Nun gilt $\log x < x$ für alle positiven reellen Zahlen x . Das folgt zum Beispiel aus Aufgabe 1.1.8 (a), wo wir $2^n \geq 2n$ für alle $n \in \mathbb{N}$ gezeigt hatten. Also ist $n \geq \log n + 1$ und daher

$$\log x \leq \log \lceil x \rceil \leq \lceil x \rceil - 1 < x.$$

Insgesamt gilt also

$$\log n = \frac{\log(n^\varepsilon)}{\varepsilon} < \frac{n^\varepsilon}{\varepsilon}$$

und damit $\log n = O(n^\varepsilon)$, wie behauptet. ■

Behauptung (f). Es sei $k \in \mathbb{N}$. Dann gilt $n^k = O(2^n)$.

Beweis. Wir behaupten zunächst, dass $(n+1)^k < 2n^k$ gilt für alle genügend großen $n \in \mathbb{N}$. Dazu erinnern wir uns daran, dass wir $(n+1)^k$ gemäß des binomischen Lehrsatzes schreiben können als $n^k + P(n)$, wobei

$$P(n) := \sum_{j=0}^{k-1} \binom{k}{j} n^j$$

ein Polynom des Grades $k-1$ in n ist. Nach Teil (c) gilt also $P(n) \leq K \cdot n^{k-1}$ für ein geeignetes $K > 0$. Ist nun $n > K$, so ist

$$(n+1)^k = n^k + P(n) \leq n^k + K \cdot n^{k-1} < n^k + n^k = 2n^k$$

wie behauptet.

Es sei jetzt $n_0 := \lceil K \rceil$ und $C := \frac{n_0^k}{2^{n_0}}$. Wir behaupten, dass

$$n^k \leq C \cdot 2^n$$

gilt für alle $n \geq n_0$. Für n_0 selbst folgt das sofort aus der Definition von C , das ist der Induktionsanfang. Ist die Behauptung nun für n richtig, so gilt für $n+1$:

$$(n+1)^k < 2n^k \leq 2 \cdot C \cdot 2^n = C \cdot 2^{n+1},$$

wie behauptet. ■

Aufgabe 2.3.5. Dass die schriftliche Division mit Rest effizient ist, begründen wir hier etwas informell. Dazu seien n und k natürliche Zahlen, gegeben der Einfachheit halber im Binärsystem. Wir wollen n mit Rest durch k teilen. Wir können natürlich annehmen, dass $n > k$ gilt; sonst geben wir n als Rest aus und sind fertig.

Es sei nun s die Stellenzahl von n und t die Stellenzahl von k . Wir wollen $n = q \cdot k + r$ schreiben. Die schriftliche Division findet diese Zahlen nach $s - t + 1$ Schritten, wobei im j -ten Schritt die j -te Stelle von q und ein Rest r_j wie folgt berechnet werden (mit $r_0 = n$ und $r_{s-t+1} = r$):

- Berechne $k'_j := 2^{s-t+1-j} \cdot k$ durch das Schreiben von $s - t + 1 - j$ Nullen hinter die Zahl k .
- Ist $k'_j \geq r_{j-1}$, so hat q an der j -ten Stelle eine 1; setze dann $r_j := r_{j-1} - k'_j$.
- Andernfalls hat q an der j -ten Stelle eine 0, und wir setzen $r_j := r_{j-1}$.

Wir führen also insgesamt höchstens $s - t + 1$ Vergleiche und Subtraktionen von bis zu s -stelligen Zahlen durch. Die Laufzeit ist damit polynomiell in s , wie behauptet.

Bemerkung. Wir könnten mit Hilfe des Prinzips „Teile und Herrsche“ auch einen noch einfacheren, wenn auch weniger effizienten Algorithmus formulieren: Wir suchen nach der größten Zahl m mit $k \cdot m \leq n$. Da $m \leq n$ gelten muss, kommen wir dafür mit höchstens $\lceil \log m \rceil$ Multiplikationen aus.

Nun zum Euklidischen Algorithmus. Wenden wir diesen auf zwei Zahlen m und n mit $m > n$ an, so teilen wir zunächst m mit Rest durch n :

$$m = q_1 \cdot n + r_2, \quad q_1 \geq 1, \quad r_2 < n.$$

Wir behaupten, dass dabei $r_2 < \frac{m}{2}$ gelten muss. Ist $n \leq \frac{m}{2}$, so ist das klar wegen $r_2 < n$. Andernfalls ist $q_1 = 1$ und ebenfalls

$$r_2 = m - n < m - \frac{m}{2} = \frac{m}{2}.$$

Damit sehen wir, dass für die im Euklidischen Algorithmus auftauchenden Zahlen r_j stets $r_{j+2} < \frac{r_j}{2}$ gilt, und insbesondere ist

$$r_{2k} < \frac{m}{2^k}.$$

Es folgt, dass höchstens $2 \cdot \lceil \log m \rceil - 1$ Divisionen mit Rest durchgeführt werden müssen, bevor wir den Rest 0 erhalten und der Algorithmus anhält. Damit ist die Anzahl dieser Divisionen also von der Größenordnung $O(\log m)$, wie behauptet, und der Algorithmus ist effizient.

Aufgabe 2.3.6. Wir möchten die Potenz n^k mit dem Prinzip „Teile und Herrsche“ berechnen. Die Idee ist folgende: Ist k gerade, etwa $k = 2m$, so teilen wir die Potenz auf als

$$n^k = n^m \cdot n^m.$$

Wir müssen dann die Potenz n^m nur *einmal* berechnen, und bekommen dann die Potenz n^k daraus durch Quadrierung.

Ist k ungerade, etwa $k = 2m + 1$, so ist die Idee dieselbe: Wir schreiben

$$n^k = n \cdot n^m \cdot n^m$$

und müssen wieder nur einmal die Potenz n^m berechnen, können sie aber gleich an zwei Stellen in dieser Formel verwenden.

Jetzt können wir unseren fertigen Algorithmus formulieren. Er ist *rekursiv*: Der Algorithmus ruft sich selbst bei seiner Ausführung wieder auf, dabei aber jedesmal zur Berechnung einer kleineren Potenz. Die Leserin überlege sich selbst, wie das Verfahren auch ohne Rekursion formuliert werden könnte.

ALGORITHMUS POTENZ

Eingabe: Zahlen $n \in \mathbb{Z}$ und $k \in \mathbb{N}_0$.

1. Ist $k = 0$, gib 1 aus.
2. Ist $k = 1$, gib n aus.
3. Ist $k \geq 2$, schreibe $k = 2m$ oder $k = 2m + 1$ und verwende den Algorithmus POTENZ, um $a = n^m$ zu berechnen.
 - (a) Ist k gerade, so ist das Ergebnis gegeben durch a^2 .
 - (b) Ist k ungerade, so ist das Ergebnis gegeben durch $k \cdot a^2$.

Schritt **3.** wird genau $\lfloor \log k \rfloor$ -mal ausgeführt, und jedesmal werden höchstens zwei Multiplikationen durchgeführt. Also wird insgesamt höchstens $2\lfloor \log k \rfloor$ -mal multipliziert.

Aufgabe 2.3.7. Seien $k, n \in \mathbb{N}$. Um die Zahl $m_0 := \lfloor \sqrt[k]{n} \rfloor$ effizient zu ermitteln, verwenden wir wieder das Verfahren „Teile und Herrsche“. Es gilt $m_0 \leq n$, also müssen wir höchstens $\lfloor \log n \rfloor$ -mal überprüfen, ob eine Potenz m^k größer ist als n oder nicht.

Nach der vorigen Aufgabe ist das effizient möglich. (Wir weisen darauf hin, dass wir bei der Potenzbildung abbrechen können, wenn wir bei einer Zahl ankommen, die größer ist als n ; dementsprechend rechnen wir stets nur mit Zahlen der Stellenzahl höchstens $2\lfloor \log n \rfloor + 2$.) Insgesamt ist dieser Algorithmus also effizient.

Für praktische Zwecke können wir den Algorithmus verbessern, indem wir bessere Schranken für m_0 angeben. Dazu erinnern wir uns daran, dass die Anzahl t der Stellen von n in Binärdarstellung (in der wir uns n hier gegeben vorstellen) genau $\lfloor \log n \rfloor + 1$ ist. Nach Definition von m_0 gilt $m_0^k \leq n$ und $(m_0 + 1)^k > n$. Daraus folgt

$$\log m_0 \leq \left\lceil \frac{t}{k} \right\rceil \quad \text{und} \quad \log(m_0 + 1) > \left\lfloor \frac{t-1}{k} \right\rfloor,$$

also ist

$$2^{\lfloor \frac{t-1}{k} \rfloor} - 1 \leq m_0 \leq 2^{\lceil \frac{t}{k} \rceil},$$

und wir können uns bei der Anwendung des Prinzips „Teile und Herrsche“ auf die Suche nach einem solchen m_0 beschränken.

Wollen wir nun eine natürliche Zahl n daraufhin testen, ob es natürliche Zahlen m und $k > 1$ gibt mit $n = m^k$, so können wir für $k = 2, 3, 4, \dots$ jeweils die Zahl $m_k := \lfloor \sqrt[k]{n} \rfloor$ berechnen, bis zum ersten Mal entweder $m_k^k = n$ oder $m_k^k > n$ gilt. Im ersten Fall lautet die Antwort „ja“, im zweiten Fall lautet sie „nein“.

Da wir offensichtlich höchstens $\log n$ Zahlen k ausprobieren müssen, ist dieser Algorithmus effizient.

Aufgabe 2.5.4.

Behauptung. Es sei P ein ganzzahliges Polynom in n Variablen, welches nicht konstant gleich 0 ist, und es sei d der höchste Exponent, mit dem eine der Variablen in P auftritt. Sei ferner $M > 0$.

Dann gibt es höchstens $n \cdot d \cdot M^{n-1}$ ganzzahlige Nullstellen von P , deren Koordinaten alle zwischen 1 und M liegen.

Beweis. Wir beweisen die Behauptung durch Induktion über n . Für $n = 0$ kommen in P gar keine Variablen vor, d.h. P ist ein konstantes Polynom. P ist aber nicht konstant gleich 0, hat also gar keine Nullstellen. Das ist der Induktionsanfang.

Jetzt sei die Behauptung für n richtig; wir müssen sie für $n + 1$ beweisen. Es sei also P ein Polynom in $n + 1$ Variablen, das nicht konstant gleich 0 ist. Dann gibt es Zahlen $y_1, \dots, y_n, y_{n+1}$ mit $P(y_1, \dots, y_n, y_{n+1}) \neq 0$. Wir betrachten jetzt eine ganzzahlige Nullstelle $(x_1, x_2, \dots, x_n, x_{n+1})$ von P mit $x_j \in \{1, \dots, M\}$ für alle $j \in \{1, \dots, n + 1\}$. Wir unterscheiden zwei Fälle:

- (a) Ist $P(y_1, y_2, \dots, y_n, x_{n+1}) \neq 0$, so ist $(x_1, \dots, x_n)$ eine Nullstelle eines nichtkonstanten Polynoms in n Variablen $X_1, \dots, X_n$, nämlich

$$Q(X_1, \dots, X_n) := P(X_1, \dots, X_n, x_{n+1}).$$

Nach Induktionsvoraussetzung hat dieses Polynom höchstens $n \cdot d \cdot M^{n-1}$ Nullstellen. Da wir bis zu M mögliche Werte für x_{n+1} haben, gibt es insgesamt höchstens $n \cdot d \cdot M^n$ Nullstellen dieser Art.

(b) Ist andererseits $P(y_1, \dots, y_n, x_{n+1}) = 0$, so ist x_{n+1} eine Nullstelle des Polynoms

$$R(X) := P(y_1, \dots, y_n, X)$$

in einer Variablen X . Nach Folgerung 3.4.5 gibt es höchstens d solche Werte x_{n+1} . Für $x_1, \dots, x_n$ haben wir insgesamt M^n Möglichkeiten, also gibt es höchstens $d \cdot M^n$ Nullstellen dieser Art.

Insgesamt gibt es also höchstens

$$n \cdot d \cdot M^n + d \cdot M^n = (n+1) \cdot d \cdot M^n$$

Nullstellen dieser Form, und damit ist der Induktionsschluss vollendet. ■

Aufgabe 2.5.5. Wir betrachten eine Münze, die bei jedem Wurf mit Wahrscheinlichkeit p „Kopf“ und mit Wahrscheinlichkeit $q = 1 - p$ „Zahl“ zeigt.

Behauptung (a). Die Wahrscheinlichkeit, dass nach n Würfeln keinmal „Kopf“ gefallen ist, beträgt genau q^n .

Beweis. Das folgt sofort aus den üblichen Regeln der Wahrscheinlichkeitslehre: Die Wahrscheinlichkeit, dass n voneinander unabhängige Ereignisse eintreten, ist das Produkt über deren Wahrscheinlichkeiten. ■

Insbesondere ist im Fall $q = 1/2$ diese Wahrscheinlichkeit genau $1/2^n$. Möchten wir, dass

$$\frac{1}{2^n} < 0,000001$$

gilt, so müssen wir

$$n = \left\lceil \log \frac{1}{0,000001} \right\rceil = \lceil \log 10^6 \rceil = 20$$

wählen. Nach 20 Münzwürfen erhalten wir also mit mehr als 99,9999-prozentiger Wahrscheinlichkeit mindestens einmal „Kopf“.

Behauptung (c). Die durchschnittliche Anzahl der Würfe, bis wir das erste Mal „Kopf“ erhalten, ist genau

$$\frac{1}{p}.$$

Beweis. Die Wahrscheinlichkeit, dass wir nach n Würfeln das erste Mal „Kopf“ erhalten (d.h. wir werfen erst $(n-1)$ -mal „Zahl“ und dann einmal „Kopf“) beträgt $p \cdot q^{n-1}$. Der Erwartungswert ist also nach Definition die (unendliche) Summe

$$\sum_{j=1}^{\infty} j \cdot p \cdot q^{j-1} = p \cdot \sum_{j=0}^{\infty} (j+1) \cdot q^j.$$

Diese Summe können wir nach Aufgabe 1.1.8 berechnen. Denn es gilt

$$\sum_{j=0}^{k-1} (j+1) \cdot q^j = \frac{kq^{k+1} - (k+1)q^k + 1}{(1-q)^2}.$$

Im Grenzwert für $k \rightarrow \infty$ geht wegen $q < 1$ der Zähler der rechten Seite gegen 1; daher ist

$$p \cdot \sum_{j=0}^{\infty} (j+1) \cdot q^j = \frac{p}{(1-q)^2} = \frac{p}{p^2} = p,$$

wie behauptet. ■

Im Algorithmus POLY-NULLE beträgt die Wahrscheinlichkeit, eine Nicht-Nullstelle zu finden, mindestens $1/2$. Also werden im Durchschnitt höchstens zwei Wiederholungen benötigt, um ein Polynom als nicht konstant gleich Null zu erkennen.

Kapitel 3

Zahlentheoretische Grundlagen

Aufgabe 3.1.6.

Addition und Multiplikation modulo 3:

+	0	1	2	·	0	1	2
0	0	1	2	0	0	0	0
1	1	2	0	1	0	1	2
2	2	0	1	2	0	2	1

Addition und Multiplikation modulo 7:

+	0	1	2	3	4	5	6	·	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6	0	0	0	0	0	0	0	0
1	1	2	3	4	5	6	0	1	0	1	2	3	4	5	6
2	2	3	4	5	6	0	1	2	0	2	4	6	1	3	5
3	3	4	5	6	0	1	2	3	0	3	6	2	5	1	4
4	4	5	6	0	1	2	3	4	0	4	1	5	2	6	3
5	5	6	0	1	2	3	4	5	0	5	3	1	6	4	2
6	6	0	1	2	3	4	5	6	0	6	5	4	3	2	1

Aufgabe 3.1.7. $9! = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ ist durch 2 und durch 5 teilbar, also durch 10.

$10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ ist *nicht* durch 11 teilbar, denn mit Hilfssatz 1.4.1 wäre ansonsten einer der Faktoren $1, 2, \dots, 10$ durch 11 teilbar. Das ist aber nicht der Fall.

Rechnen wir noch einige Beispiele, so legt das die Vermutung nahe, dass $n!$ durch $n + 1$ teilbar ist, falls $n + 1$ keine Primzahl ist. Andererseits ist $3! = 3 \cdot 2 \cdot 1 = 6$ nicht durch 4 teilbar. Das nächste kleine Beispiel ist $5! = 5 \cdot 4 \cdot 3 \cdot 2 = 120$ – diese Zahl ist durch 6 teilbar. Möglicherweise stimmt unsere Vermutung also für alle Zahlen ab 5! Versuchen wir, das zu beweisen:

Sei $n \in \mathbb{N}$ so, dass $n \geq 5$ und $n + 1$ nicht prim ist, und schreibe $n + 1 = p_1 \cdots p_k$, wobei $p_1, \dots, p_k$ Primzahlen sind. Nach Definition ist $n! = n \cdot (n - 1) \cdots 2 \cdot 1$, und alle

Primzahlen, die $n + 1$ teilen, sind kleiner n und kommen deshalb als Faktor im Produkt $n!$ vor.

Betrachten wir zuerst den Fall, dass $p_1, p_2, \dots, p_n$ paarweise verschieden sind. Da $n!$ von jeder der Zahlen $p_1, \dots, p_n$ geteilt wird und diese paarweise nicht nur verschieden, sondern teilerfremd sind, wird $n!$ von ihrem Produkt geteilt. Also ist $n! \equiv 0$ modulo $n + 1$.

Nehmen wir jetzt an, dass etwa $p_1 = p_2$ ist. Wegen $n \geq 5$ ist $n + 1 \geq 6$ und daher $2p_1 \leq n$. Das bedeutet aber, dass sowohl p_1 als auch $2p_1$ als Faktoren im Produkt $n!$ auftauchen. Deshalb ist $n!$ durch $p_1^2 = p_1 p_2$ teilbar. So können wir für alle Primzahlen argumentieren, die mehrfach in einer Primfaktorzerlegung von $n + 1$ vorkommen. Zusammen mit dem vorherigen Argument, angewandt auf die paarweise teilerfremden Primzahlpotenzen in einer Primfaktorzerlegung von $n + 1$, folgt die Behauptung.

Aufgabe 3.1.8.

Behauptung. Seien a, b ganze Zahlen, m, n natürliche Zahlen mit $m \mid n$, und es gelte $a \equiv b \pmod{n}$. Dann ist $a \equiv b \pmod{m}$. Die Umkehrung ist falsch.

Beweis. $a \equiv b \pmod{n}$ bedeutet, dass $a - b$ durch n teilbar ist. Aber m teilt n , also ist $a - b$ auch durch m teilbar und damit ist $a \equiv b \pmod{m}$ wie behauptet.

Um zu zeigen, dass die Umkehrung nicht wahr ist, geben wir ein Gegenbeispiel an: $2 \mid 4$ und $8 \equiv 10 \pmod{2}$, aber 8 ist nicht kongruent zu 10 modulo 4. ■

Aufgabe 3.1.9. Sei $n \in \mathbb{N}$.

Behauptung. Genau dann ist $\sum_{i=0}^{n-1} i \equiv 0$ modulo n , wenn n ungerade ist. Genau dann ist $\sum_{i=0}^{n-1} i^2 \equiv 0$ modulo n , falls $n \equiv \pm 1 \pmod{6}$.

Beweis. Wir verwenden die Formeln aus Aufgabe 1.1.8. Das liefert $\sum_{i=0}^{n-1} i = \frac{(n-1)n}{2}$.

Falls n ungerade ist, dann ist $n - 1$ durch 2 teilbar und daher $\frac{(n-1)n}{2}$ eine ganze Zahl, die durch n teilbar ist. Falls n gerade ist, dann sei 2^k die größte Potenz der Zahl 2, die n teilt. Nun ist $n - 1$ nicht durch 2 teilbar, also ist $\frac{(n-1)n}{2}$ zwar eine ganze Zahl, aber nicht durch 2^k teilbar, denn sonst wäre n durch 2^{k+1} teilbar. Insbesondere ist n kein Teiler von $\frac{(n-1)n}{2}$ und damit die erste Behauptung bewiesen.

Für die zweite Behauptung wenden wir die entsprechende Formel an und erhalten

$$\sum_{k=1}^{n-1} k^2 = \frac{(n-1)n(2(n-1)+1)}{6} = \frac{(n-1)n(2n-1)}{6}.$$

Kongruenzen modulo 6 liefern

n	0	1	2	3	4	5
$n-1$	-1	0	1	2	3	4
$2n-1$	-1	1	3	5	1	3

Genau dann ist $\frac{(n-1)n(2n-1)}{6}$ durch n teilbar, wenn $(n-1)(2n-1)$ durch 6 teilbar ist. Aus der Tabelle lesen wir ab, dass die einzigen Möglichkeiten sind, dass $(n-1)$ kongruent zu 0 ist oder dass $(n-1)$ kongruent zu 4 ist und $(2n-1)$ zu 3. Das ist genau dann der Fall, wenn n kongruent zu 1 oder -1 ($\equiv 5$) ist modulo 6 und gleichbedeutend damit, dass n teilerfremd zu 6 ist. ■

Aufgabe 3.1.10. Für die erste Aussage sei $x \in \mathbb{Z}$ mit $x^2 \equiv 1 \pmod{n}$. Das heißt, dass n ein Teiler ist von $x^2 - 1 = (x+1)(x-1)$. Da n prim ist, muss einer der beiden Faktoren von n geteilt werden, nach Hilfssatz 1.4.1. Das bedeutet aber genau $x \equiv 1 \pmod{n}$ oder $x \equiv -1 \pmod{n}$.

Für den Satz von Wilson haben wir zwei Richtungen zu beweisen. Zuerst setzen wir voraus, dass $(n-1)! + 1$ durch n teilbar ist und zeigen, dass dann n prim ist.

Angenommen, n besitzt einen echten Primteiler p , also $1 < p < n$. Nach Voraussetzung ist dann p ein Teiler von $(n-1)! + 1$. Andererseits sehen wir, dass p im Produkt $(n-1)! = (n-1)(n-2) \cdots 2 \cdot 1$ vorkommen muss, d. h. $p \mid (n-1)!$. Das ist aber ein Widerspruch, denn p ist prim, insbesondere $p \neq 1$ und daher kann p nicht zwei aufeinanderfolgende Zahlen teilen.

Ist umgekehrt n eine Primzahl, so betrachten wir wieder das Produkt $(n-1)!$. Da alle Faktoren echt kleiner als n sind, sind sie zu n teilerfremd. Satz 3.1.3 liefert zu jeder der Zahlen $1, 2, \dots, n-1$ ein Inverses modulo n . Die Anzahl derjenigen Zahlen darunter, die von ihrem Inversen verschieden sind, muss gerade sein, denn sie treten ja paarweise auf. Die anderen Zahlen sind zu sich selbst invers modulo n , ihr Quadrat ist also kongruent zu 1 modulo n . Da n prim ist, liefert die Aussage, die wir ganz zu Anfang bewiesen haben, dass es nur zwei Möglichkeiten dafür gibt - nämlich die Zahlen 1 und $n-1$.

Schreiben wir nun das Produkt $(n-1)!$ aus, so erhalten wir modulo n jeweils Paare zueinander inverser Zahlen und dann noch die Faktoren 1 und $n-1$. Es ist also

$$(n-1)! \equiv n-1 \equiv -1 \pmod{n}.$$

Aber dann ist $(n-1)! + 1 \equiv -1 + 1 = 0$ modulo n wie behauptet.

Aufgabe 3.1.10.

Behauptung. Sei $n \geq 2$ und seien a und b ganze Zahlen. Setze $d := \text{ggT}(a, n)$. Die Gleichung

$$a \cdot x \equiv b \pmod{n}; \tag{3.1}$$

besitzt Lösungen genau dann, wenn d ein Teiler ist von b . Es gibt genau dann eine modulo n eindeutige Lösung, falls a und n teilerfremd sind, falls also $d = 1$ ist.

Beweis. Beginnen wir mit der Annahme $d|b$ und sei $e \in \mathbb{N}$ mit $ed = b$. Mit dem Lemma von Bézout (1.3.3) existieren $k, l \in \mathbb{Z}$ derart, dass $d = ka + ln$ ist. Also folgt

$$b = de = kae + lne,$$

d.h. $b \equiv kae \pmod{n}$. Setzen wir dann $x := ke$, so ist x eine Lösung der Gleichung $a \cdot x \equiv b \pmod{n}$.

Sei umgekehrt x eine Lösung. Dann ist n ein Teiler von $b - xa$, sei also $k \in \mathbb{N}$ mit $kn = b - xa$. Dann ist $b = kn + xa$. Da d ein Teiler ist von a und von n , ist $kn + xa$ durch d teilbar und damit auch b .

Nehmen wir nun an, dass $d = 1$ ist, und seien x, y Lösungen zu $a \cdot x \equiv b \pmod{n}$. Dann ist $xa \equiv b \equiv ya \pmod{n}$. Da a und n teilerfremd sind, dürfen wir die Kürzungsregel anwenden und durch a teilen (3.1.4). Das liefert $x \equiv y \pmod{n}$, d.h. die Lösungen x und y sind modulo n gleich.

Umgekehrt sei x die einzige Lösung modulo n und sei $y := x + \frac{n}{d}$. Dann ist $ya = xa + \frac{an}{d}$, und $\frac{an}{d}$ ist durch n teilbar, da $\frac{a}{d}$ eine ganze Zahl ist. Das bedeutet $ya \equiv xa \pmod{n}$ und damit ist auch y eine Lösung der Gleichung. Die Eindeutigkeit von x liefert $x \equiv y \pmod{n}$, also ist $x - y = \frac{n}{d}$ durch n teilbar. Daraus folgt $d = 1$ wie behauptet. ■

Aufgabe 3.1.11. Die Zahlen 4 und 3 sind Nullteiler modulo 6, denn sie sind beide nicht kongruent zu 0 modulo 6, aber das Produkt $3 \cdot 4 = 12$ ist durch 6 teilbar.

Ebenso sind 2 und 5 Nullteiler modulo 10, denn sie sind beide nicht kongruent zu 0 modulo 10, aber $2 \cdot 5 = 10$ ist durch 10 teilbar.

Sei jetzt p eine Primzahl und seien x, y ganze Zahlen mit der Eigenschaft $xy \equiv 0 \pmod{p}$. Dann ist p ein Teiler von xy , mit Hilfssatz 1.4.1 also auch ein Teiler von x oder von y . Das heißt: Modulo einer Primzahl gibt es keine Nullteiler. Das ist bereits der Beweis für eine Hälfte des folgenden Satzes:

Behauptung. Sei $n \geq 2$. Es gibt Nullteiler modulo n genau dann, wenn n zusammengesetzt ist.

Beweis. Wir haben oben gezeigt, dass es keine Nullteiler gibt, falls n prim ist. Falls es also umgekehrt Nullteiler gibt modulo n , dann muss n zusammengesetzt sein. Nehmen wir nun an, dass n zusammengesetzt ist. Dann gibt es $x, y \in \mathbb{N}$ so, dass $n = xy$ ist, mit $1 < x \leq y < n$. Weder x noch y ist kongruent zu 0 modulo n , aber $xy = n$ ist durch n teilbar. Also sind x und y Nullteiler modulo n . ■

Aufgabe 3.1.12. Es sei $n \geq 2$, $a \geq 0$ und $k \in \mathbb{N}$. Der Einfachheit halber können wir annehmen, dass $a < n$ gilt (sonst teilen wir a ganz zu Anfang einmal mit Rest durch n , was mit der schriftlichen Division effizient geht).

Um den Rest von a^k zu berechnen, verfahren wir wie in Aufgabe 2.3.6, reduzieren aber alle auftretenden Zahlen modulo n . Wir müssen dann höchstens $2\lceil \log k \rceil$ Multipli-

kationen von Zahlen durchführen, die kleiner als n sind; insgesamt ist dieser Algorithmus also effizient.

Jetzt geht es um die Berechnung des Inversen von a modulo n . In Aufgabe 2.3.5 haben wir gesehen, dass der Euklidische Algorithmus effizient ist und dass bei seiner Anwendung auf n und a höchstens $2\lceil \log n \rceil - 1$ Divisionen mit Rest durchgeführt werden. Das „Rückwärtseinsetzen“ in die auftretenden Gleichungen erfordert dann auch noch einmal höchstens $\log n$ Schritte. Wir können dabei alle auftretenden Zahlen modulo n reduzieren. Also führen wir nur Rechenoperationen mit Zahlen aus, die kleinere Stellenzahl als n haben, und die Anzahl dieser Rechenoperationen ist polynomiell in $\log n$ beschränkt. Insgesamt ist der Algorithmus daher effizient.

Bemerkung. Die Zahlen s und t mit $s \cdot n + t \cdot a = 1$, die wir mit dem Euklidischen Algorithmus berechnen, werden in Wahrheit für keine Wahl von n und a größer als n werden. Daher ist es nicht nötig, in jedem Schritt modulo n zu reduzieren, aber wir beweisen diese Tatsache hier nicht.

Aufgabe 3.1.14. Eine Möglichkeit, eine Zahl x mit den gewünschten Eigenschaften zu finden, ist die folgende:

Es soll $x \equiv 1 \pmod{5}$ sein, also können wir schreiben $x = 5k + 1$ mit einem geeigneten $k \in \mathbb{Z}$. Für die Kongruenz modulo 13 betrachten wir die verschiedenen Möglichkeiten für k modulo 13:

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$5k + 1$	1	6	11	3	8	0	5	10	2	7	12	4	9

Wir lesen ab, dass wir für $k = 3$ eine zu 3 (modulo 13) kongruente Zahl erhalten und berechnen $x = 5k + 1 = 16$. Diese Zahl ist kongruent zu 1 modulo 5, zu 3 modulo 13 und (aber das ist Glück!) zu 2 modulo 7 wie gewünscht. Eine andere Möglichkeit, eine solche Zahl x zu finden, besteht darin, die Argumente für den Beweis des Chinesischen Restsatzes nachzuzahlen.

Aufgabe 3.1.15. Das ist nicht besonders originell, aber es gibt auch immer dann eine Lösung, wenn a_1 und a_2 modulo n_1 und n_2 kongruent sind! (Nämlich a_1 oder a_2 selbst.)

Aufgabe 3.1.16. Es sei $n = n_1 \cdot n_2$ wie im Chinesischen Restsatz. Für eine ganze Zahl x sei $r_1(x)$ der Rest von x beim Teilen durch n_1 , und $r_2(x)$ der Rest beim Teilen durch n_2 . Sind x und x' modulo n verschiedene ganze Zahlen, so sind sie auch modulo n_1 und modulo n_2 verschieden, also erhalten wir unterschiedliche Paare $(r_1(x), r_2(x))$ und $(r_1(x'), r_2(x'))$. Da es genau n verschiedene Paare (r_1, r_2) gibt mit $0 \leq r_1 < n_1$ und $0 \leq r_2 < n_2$, gibt es auch genau n verschieden Paare $(r_1(x), r_2(x))$ von „Resten“ ganzer Zahlen x modulo n_1 und n_2 . Insbesondere finden wir zu (r_1, r_2) mit $0 \leq r_1 < n_1$ und $0 \leq r_2 < n_2$ eine ganze Zahl x so, dass $(r_1, r_2) = (r_1(x), r_2(x))$ ist.

Seien a_1, a_2 ganze Zahlen. Dann gibt es $r_1, r_2 \in \mathbb{Z}$ so, dass $0 \leq r_1 < n_1$ und $0 \leq r_2 < n_2$ ist und $a_1 \equiv r_1 \pmod{n_1}$, $a_2 \equiv r_2 \pmod{n_2}$. Wir finden also ein $x \in \mathbb{Z}$ so,

dass $(r_1, r_2) = (r_1(x), r_2(x))$ ist und daher $x \equiv r_1(x) = r_1 \equiv a_1 \pmod{n_1}$ und genauso $x \equiv r_2(x) = r_2 \equiv a_2 \pmod{n_2}$ wie gewünscht.

Aufgabe 3.1.17. Angenommen, es seien $x, y \in \mathbb{Z}$ so, dass $x^2 = 5y - 2$ gilt. Wir bezeichnen diese Gleichung mit $(*)$. Betrachten wir das modulo 5, so sehen wir, dass die rechte Seite zu -2 kongruent ist. Wegen $(*)$ muss auch die linke Seite kongruent zu -2 sein. Wir müssen also die Frage beantworten, wozu ein Quadrat modulo 5 kongruent sein kann! Quadrieren wir $-2, -1, 0, 1, 2$ (ein vollständiges Restesystem modulo 5), so erhalten wir modulo 5 die Zahlen $4(\equiv -1), 1, 0, 1$ und $4(\equiv -1)$, aber *niemals* -2 .

Das widerspricht der Wahl von x und y , und daraus schließen wir, dass es keine ganzzahlige Lösung der Gleichung $(*)$ gibt.

Aufgabe 3.1.18. Seien $x, y \in \mathbb{Z}$ so, dass die Gleichung $x^2 + 2 = y^3$, bezeichnet mit $(\bullet)$, erfüllt ist. Dann muss die Gleichung insbesondere modulo 4 richtig sein. Wir müssen also entscheiden, wozu Quadrate und dritte Potenzen kongruent sind modulo 4. Am übersichtlichsten geht das in Tabellen – die Einträge sind modulo 4 zu lesen.

x	-1	0	1	2
x^2	1	0	1	0
$x^2 + 2$	-1	2	-1	2

y	-1	0	1	2
y^3	-1	0	1	0

Damit $(\bullet)$ überhaupt erfüllt sein kann, müssen wir eine Übereinstimmung in den untersten Zeilen in beiden Tabellen finden. Der einzige Eintrag, der in beiden Zeilen vorkommt, ist die Zahl -1 . Er erscheint, wenn y^3 zu -1 kongruent ist modulo 4, wenn also auch y selbst zu -1 kongruent ist. In der Tabelle für x sehen wir, dass aus $x^2 + 2 \equiv -1 \pmod{4}$ schon $x^2 \equiv 1 \pmod{4}$ folgt. Daher ist x selbst zu 1 oder -1 kongruent. Stets folgt, dass sowohl x als auch y ungerade sind.

Aufgabe 3.1.19. Hier ist eine mögliche Version:

Behauptung. Seien $n_1, \dots, n_t$ ganze, paarweise teilerfremde Zahlen, $t \geq 2$, und seien $a_1, \dots, a_t \in \mathbb{Z}$. Dann gibt es eine ganze Zahl $b \in \mathbb{Z}$ derart, dass $b \equiv a_i$ ist modulo n_i für alle $i \in \{1, \dots, t\}$.

Hinweis für den Beweis. Argumentiere mit vollständiger Induktion über t . Beweise zuerst folgendes Hilfsresultat:

Seien $n_1, \dots, n_t$ ganze, paarweise teilerfremde Zahlen, $t \geq 1$, und sei $x \in \mathbb{Z}$. Dann gibt es ein gemeinsames Vielfaches y von $n_1, \dots, n_{t-1}$, so dass $x - y$ durch n_t teilbar ist.

Für den Induktionsschritt von $t - 1$ zu t nimm an, dass es bereits eine ganze Zahl b' gibt so, dass $b' \equiv a_i$ ist modulo n_i für alle $i \in \{1, \dots, t - 1\}$. Wende dann das Hilfsresultat oben auf $a_t - b'$ an. Die Idee dabei ist, beim Übergang zu a_t und n_t nicht die Lösung b' , die wir bereits haben, zu „verlieren“.

Aufgabe 3.1.21. Seien a und n teilerfremd. Zuerst zeigen wir, dass verschiedene Elemente von aR paarweise inkongruent sind modulo n . Seien also $x, y \in R$ mit $ax \equiv ay \pmod{n}$. Dann ist $a(x - y) = ax - ay$ durch n teilbar. Da nach Voraussetzung a und n teilerfremd sind, muss $x - y$ durch n teilbar sein, und es folgt $x \equiv y \pmod{n}$. Nach Definition eines VRS ist $x = y$, also $ax = ay$.

Das beweist einerseits, dass verschiedene Elemente von aR paarweise nicht-kongruent sind modulo n . Mit der Kürzungsregel sind aber auch alle Elemente ax mit $x \in R$ paarweise verschieden, d. h. aR hat genau so viele Elemente wie R . Daraus folgt schon, dass auch aR ein VRS ist.

Sei nun umgekehrt aR ein VRS modulo n . Sei $x \in aR$ so, dass $x \equiv 1$ ist modulo n und sei $r \in R$ mit $x = ar$. Es ist $x - 1$ durch n teilbar, sei also weiter $k \in \mathbb{Z}$ so, dass $x - 1 = kn$ gilt. Dann folgt insgesamt

$$ar + (-k)n = x - kn = 1,$$

und deshalb sind a und n teilerfremd mit Folgerung 1.3.4.

Für den zweiten Teil der Aufgabe müssen wir nur sehen, dass bei Multiplikation mit a aus zu n teilerfremden Zahlen wieder zu n teilerfremde Zahlen werden. Aber das haben wir sofort dank Folgerung 1.3.5, und die andere Richtung funktioniert genau wie oben.

Aufgabe 3.2.7. $5^2 = 25 \equiv 1 \pmod{12}$, also ist 2 die Ordnung von 5 modulo 12.

$7^2 = 49 \equiv 4 \pmod{15}$, $7^3 \equiv 4 \cdot 7 = 28 \equiv -2 \pmod{15}$ und $7^4 \equiv 4^2 = 16 \equiv 1 \pmod{15}$, also ist 4 die Ordnung von 7 modulo 15.

$13^2 \equiv (-2)^2 = 4 \pmod{15}$, $13^3 \equiv (-2)^3 = -8 \pmod{15}$ und $13^4 \equiv (-2)^4 = 16 \equiv 1 \pmod{15}$, also ist 4 auch die Ordnung von 13 modulo 15.

Wir stellen fest, dass $13 \cdot 7 = 91 \equiv 1 \pmod{15}$ ist, also sind 7 und 13 zueinander invers modulo 15. Sie haben die gleiche Ordnung modulo 15, und das ist ein Beispiel für ein allgemeines Resultat - siehe nächste Aufgabe!

Aufgabe 3.2.8.

Behauptung. Sei $x \in \mathbb{Z}$ teilerfremd zu $n \in \mathbb{N}$ und sei $x' \in \mathbb{Z}$ mit $xx' \equiv 1 \pmod{n}$. Dann ist $\text{ord}_n(x) = \text{ord}_n(x')$.

Beweis. Sei $d := \text{ord}_n(x)$ und $d' := \text{ord}_n(x')$. Wir haben $xx' \equiv 1 \pmod{n}$, also auch $x^d x'^d = (xx')^d \equiv 1 \pmod{n}$. Aber nach Definition der Ordnung ist $x^d \equiv 1 \pmod{n}$ und daher $x'^d \equiv 1 \pmod{n}$. Daraus folgt mit Hilfssatz 3.2.1, dass d' ein Teiler von d ist.

Mit dem gleichen Argument, angewandt auf $(xx')^{d'}$, sehen wir, dass umgekehrt d ein Teiler von d' ist. Also ist $d = d'$ wie behauptet. ■

Aufgabe 3.2.9. Seien $a, n \in \mathbb{Z}$, $n \geq 2$ und a teilerfremd zu n . Setze $k := \text{ord}_n(a)$.

Behauptung. (a) Sind $b_1, b_2 \in \mathbb{N}_0$ mit $b_1 \equiv b_2 \pmod{k}$, so ist $a^{b_1} \equiv a^{b_2} \pmod{n}$.

- (b) Sei $A := \{a^j \bmod n : j \geq 0\}$ die Menge der Reste modulo n aller Potenzen von a . Dann ist

$$A = \{1, a \bmod n, a^2 \bmod n, \dots, a^{k-1} \bmod n\}.$$

- (c) $\#A = k$.

Beweis. Um (a) zu beweisen, seien $b_1, b_2 \in \mathbb{N}_0$ mit $b_1 \equiv b_2 \pmod{k}$. Wir können annehmen, dass $b_1 \leq b_2$ ist. Nach Voraussetzung ist $b_2 - b_1$ durch k teilbar, also $b_2 - b_1 = k \cdot s$ mit $s \in \mathbb{N}_0$. Nun ist

$$a^{b_1} = a^{ks+b_2} = (a^k)^s \cdot a^{b_2} \equiv 1^s \cdot a^{b_2} = a^{b_2} \pmod{n}$$

wie behauptet.

Daraus folgt schon, dass die in (b) definierte Menge A höchstens k verschiedene Elemente hat und dass ihre Elemente genau die in (b) angegebenen sind. Um (c) zu beweisen, müssen wir nur noch sehen, dass alle Potenzen $1, a, a^2, \dots, a^{k-1}$ modulo n verschieden sind. Das folgt aus Hilfssatz 3.2.1. ■

Aufgabe 3.2.10. Da $m^2 + 1$ durch p teilbar ist, ist p kein Teiler von m . Also sind p und m teilerfremd.

Nach Voraussetzung ist $m^2 \equiv -1 \pmod{p}$, also $m^4 \equiv 1 \pmod{p}$, und 4 ist dann schon die Ordnung von m modulo p . Mit dem kleinen Satz von Fermat (Satz 3.2.2) ist $m^{p-1} \equiv 1 \pmod{p}$, also 4 ein Teiler von $p - 1$ wie behauptet.

Aufgabe 3.2.11. Sei $a \in \mathbb{N}$. Dann ist nach dem kleinen Satz von Fermat schon $a^p \equiv a \pmod{p}$, also $a^p - a$ ein Vielfaches von p .

Nun gibt es zwei Fälle: a ist gerade oder ungerade. Falls a gerade ist, dann ist auch a^p gerade und daher die Differenz $a^p - a$ durch 2 teilbar. Falls a ungerade ist, dann ist auch a^p ungerade und wieder die Differenz $a^p - a$ durch 2 teilbar. In beiden Fällen wird also $a^p - a$ von p und von 2 geteilt. Aber p ist ungerade nach Voraussetzung, d.h. p und 2 sind teilerfremd und daher ist $a^p - a$ nun auch durch $2p$ teilbar.

Aufgabe 3.2.12. Sei p prim.

Behauptung. Es gilt $(a + b)^p \equiv a^p + b^p \pmod{p}$ für alle $a, b \in \mathbb{Z}$.

Wir stellen zwei Beweise vor:

Beweis, Version (1). Wir wenden den kleinen Satz von Fermat sowohl auf $a + b$ als auch auf a und b an und erhalten:

$$(a + b)^p \equiv a + b \equiv a^p + b^p \pmod{p} \quad \blacksquare$$

Beweis, Version (2). Nach dem binomischen Lehrsatz ist

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^{p-i} b^i.$$

Für die Binomialkoeffizienten $\binom{p}{i}$ mit $0 < i < p$ können wir Hilfssatz 3.2.3 anwenden und erhalten, dass dann stets $\binom{p}{i} \equiv 0$ ist modulo p . Die Summe oben vereinfacht sich modulo p also zu

$$(a + b)^p \equiv \binom{p}{0} a^p b^0 + \binom{p}{p} a^0 b^p = a^p + b^p \pmod{p}$$

wie gewünscht. ■

Aufgabe 3.2.13.

Behauptung. (a) Sind $n, m \in \mathbb{N}$ teilerfremd, so ist $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.

(b) Ist p prim und $k \in \mathbb{N}$, so ist $\varphi(p^k) = (p - 1) \cdot p^{k-1}$.

Beweis von (a). Wir verwenden den Chinesischen Restsatz (Satz 3.1.5). Er besagt: Sind $a_1, a_2 \in \mathbb{N}_0$ mit $a_1 < n$ und $a_2 < m$, so gibt es genau eine Zahl x zwischen 0 und $nm - 1$ mit $x \equiv a_1 \pmod{n}$ und $x \equiv a_2 \pmod{m}$.

Ist x teilerfremd zu nm , so ist x auch teilerfremd zu n und zu m , d.h. $a_1 \in \text{Tf}(n)$ und $a_2 \in \text{Tf}(m)$. Ist umgekehrt a_1 teilerfremd zu n und a_2 teilerfremd zu m , so ist x teilerfremd sowohl zu n als auch zu m und damit auch (nach Hilfssatz 1.3.5) zu nm .

Es gibt daher genau $\varphi(n) \cdot \varphi(m)$ Möglichkeiten, die Zahlen a_1 und a_2 so zu wählen, dass x zu nm teilerfremd ist, und damit ist die Behauptung bewiesen. ■

Beweis von (b). Die *nicht* zu p^k teilerfremden Zahlen in $\{0, 1, \dots, p^k - 1\}$ sind genau die Vielfachen von p in dieser Menge, also

$$0, p, 2p, \dots, p^2, 2p^2, \dots, (p - 1)p^{k-1}.$$

Deren Anzahl ist p^{k-1} , und alle übrigen Zahlen von 0 bis $p^k - 1$ sind teilerfremd zu p^k . Daher ist $\varphi(p^k) = p^k - p^{k-1} = (p - 1) \cdot p^{k-1}$. ■

Wir verwenden jetzt die gerade bewiesenen Regeln, um $\varphi(10)$, $\varphi(50)$ und $\varphi(180)$ auszurechnen:

$$\begin{aligned} \varphi(10) &= \varphi(2 \cdot 5) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4; \\ \varphi(50) &= \varphi(2 \cdot 5^2) = \varphi(2)\varphi(5^2) = 1 \cdot 4 \cdot 5^1 = 20; \\ \varphi(180) &= \varphi(2^2)\varphi(3^2)\varphi(5) = (1 \cdot 2) \cdot (2 \cdot 3) \cdot 4 = 2 \cdot 6 \cdot 4 = 48. \end{aligned}$$

Behauptung. Ist $n \in \mathbb{N}$, $n > 2$, so ist $\varphi(n)$ gerade.

Beweis. Wir nehmen zunächst an, dass n einen ungeraden Primteiler p besitzt. Dann können wir n schreiben als $n = p^k \cdot m$ mit $k, m \in \mathbb{N}$ und $p \nmid m$. Jetzt gilt

$$\varphi(n) = \varphi(p^k \cdot m) = \varphi(p^k) \cdot \varphi(m) = (p-1) \cdot p^{k-1} \cdot \varphi(m).$$

Da p ungerade ist, ist $p-1$ gerade. Also ist auch $\varphi(n)$ eine gerade Zahl.

Hat n keinen ungeraden Primteiler, so gilt $n = 2^k$ für ein $k \geq 2$, denn nach Voraussetzung ist ja $n > 2$. Also folgt

$$\varphi(n) = \varphi(2^k) = (2-1) \cdot 2^{k-1} = 2^{k-1}.$$

Wegen $k \geq 2$ ist das auch eine gerade Zahl, wie behauptet. ■

Aufgabe 3.2.14. Wir folgen dem Hinweis in der Aufgabe und setzen darum, für jeden Teiler k von n :

$$T(n, k) := \{x \in \{1, \dots, n\} : \text{ggT}(x, n) = k\}.$$

Seien nun k_1, k_2 verschiedene Teiler von n und angenommen, es gebe ein Element $x \in T(n, k_1) \cap T(n, k_2)$. Dann ist $k_1 = \text{ggT}(x, n) = k_2$, aber $k_1 \neq k_2$, ein Widerspruch. Daher sind $T(n, k_1)$ und $T(n, k_2)$ disjunkt. Jede Zahl $m \in \{1, \dots, n\}$ besitzt einen größten gemeinsamen Teiler k_m mit n , d.h. $\text{ggT}(m, n) = k_m$, also liegt m in der Menge $T(n, k_m)$. Es folgt, dass $\{1, \dots, n\}$ die disjunkte Vereinigung der Mengen $T(n, k)$ ist, wobei k über alle Teiler von n läuft (inklusive 1). Insbesondere ist

$$n = \#\{1, \dots, n\} = \# \bigcup_{k|n} T(n, k) = \sum_{k|n} \#T(n, k).$$

Sei k ein Teiler von n und sei $x \in T(n, k)$. Nach Aufgabe 1.3.7 (a) ist dann $\text{ggT}(\frac{x}{k}, \frac{n}{k}) = 1$, d.h. $\frac{x}{k}$ und $\frac{n}{k}$ sind teilerfremd. Es gibt $\varphi(\frac{n}{k})$ Möglichkeiten für solche Zahlen $\frac{x}{k}$, also folgt $\#T(n, k) = \varphi(\frac{n}{k})$. Die Aussage oben wird dann zu

$$n = \sum_{k|n} \#T(n, k) = \sum_{k|n} \varphi\left(\frac{n}{k}\right).$$

Schließlich verwenden wir die Bemerkung, dass $\sum_{k|n} \varphi(k) = \sum_{k|n} \varphi(\frac{n}{k})$ gilt, und erhalten

$$n = \sum_{k|n} \#T(n, k) = \sum_{k|n} \varphi(k).$$

Aufgabe 3.2.15. Sei $m \in \mathbb{Z}$. Mit Aufgabe 3.2.10, angewandt für $p = 5$, folgt dann $m^5 \equiv m \pmod{2 \cdot 5}$, also ist $m^5 - m$ durch 10 teilbar.

Aufgabe 3.2.16.

Behauptung. 42 teilt $m^7 - m$ für alle natürlichen Zahlen m .

Beweis. Sei $m \in \mathbb{Z}$. Mit Aufgabe 3.2.10, angewandt für $p = 7$, erhalten wir, dass $m^7 - m$ durch 14 teilbar ist. Da 3 teilerfremd zu 2 und 7 ist und $42 = 2 \cdot 3 \cdot 7$, genügt es nun, zu zeigen, dass auch 3 ein Teiler von $m^7 - m$ ist.

1. *Fall:* m ist selbst durch 3 teilbar. Dann folgt die Behauptung sofort.
2. *Fall:* $m \equiv 1 \pmod{3}$. Dann ist auch $m^7 \equiv 1 \pmod{3}$, also $m^7 - m \equiv 0 \pmod{3}$.
3. *Fall:* $m \equiv 2 \pmod{3}$. Dann ist $m^7 \equiv 2^7 = 2 \cdot 4^3 \equiv 2 \cdot 1 = 2 \pmod{3}$, also wieder $m^7 - m \equiv 0 \pmod{3}$. ■

Nun zur allgemeineren Aussage:

Behauptung. Seien $r, s \geq 2$ teilerfremde natürliche Zahlen und sei $n := r \cdot s$. Ist a eine zu n teilerfremde ganze Zahl, so gilt

$$a^{\text{kgV}(\varphi(r), \varphi(s))} \equiv 1 \pmod{n}.$$

Beweis. Sei $k := \text{kgV}(\varphi(r), \varphi(s))$. Es sind a und r, s jeweils teilerfremd, also haben wir, mit dem Satz von Fermat-Euler, dass $a^{\varphi(r)} \equiv 1$ ist modulo r und $a^{\varphi(s)} \equiv 1$ modulo s . Damit folgt $a^k \equiv 1$ modulo r und s . Der Chinesische Restsatz liefert nun, dass auch $a^k \equiv 1$ ist modulo n , wie gewünscht. ■

Aufgabe 3.2.17. Da A nicht-leer ist und alle Elemente teilerfremd zu $n = 15$ sind, müssen wir nur alle möglichen Produkte von Elementen aus $A = \{1, 4, 11, 14\}$ überprüfen. Dabei ignorieren wir Multiplikation mit 1, und im Folgenden sind stets Kongruenzen modulo 15 gemeint.

$4^2 = 16 \equiv 1$, $11^2 = 121 \equiv 1$ und $14^2 = 2^2 \cdot 7^2 = 4 \cdot 49 \equiv 4 \cdot 4 = 16 \equiv 1$, also sind alle Potenzen von 4, 11 und 14 modulo 15 in A enthalten.

Weiter sind $4 \cdot 11 = 44 \equiv 14$, $4 \cdot 14 = 4 \cdot 7 \cdot 2 = 28 \cdot 2 \equiv (-2) \cdot 2 = -4 \equiv 11$, $11 \cdot 14 = 11 \cdot 2 \cdot 7 = 11 \cdot 14 \equiv 11 \cdot (-1) \equiv 4$,

also sind alle Produkte von Elementen aus A modulo 15 wieder in A enthalten. Damit erfüllt A die Voraussetzungen des Satzes von Lagrange.

Aufgabe 3.2.18. Sei $n \in \mathbb{N}$ mit $n = p^k$, wobei p prim und $k \geq 2$ ist.

Behauptung. Es gibt eine Zahl $a \in \text{Tf}(n)$ mit $\text{ord}_n(a) = p$. Das gleiche gilt für jede Zahl n , die von p^2 geteilt wird.

Beweis. Wir folgen dem Hinweis und setzen $a := p^{k-1} + 1$. Da die Teiler von n genau die (höchstens gleich großen) Potenzen von p und deren Produkte mit -1 sind, sind a und n teilerfremd. Berechnen wir a^p , so erhalten wir

$$a^p = (p^{k-1} + 1)^p = p^{p(k-1)} + \binom{p}{1} p^{(p-1)(k-1)} + \dots + \binom{p}{p-1} p^{k-1} + 1.$$

Der erste Term auf der rechten Seite ist durch $n = p^k$ teilbar. Die Binomialkoeffizienten in den mittleren Termen sind nach Hilfssatz 3.2.3 durch p teilbar, also sind alle mittleren Terme durch $p^{k-1} \cdot p = p^k = n$ teilbar. Damit bleibt genau 1 übrig, d.h. $a^p \equiv 1$ modulo n wie gewünscht. Wir überlassen es der Leserin, sich zu überlegen, warum nicht schon für eine kleinere Potenz die Zahl 1 erreicht wird.

Sei jetzt p^2 ein Teiler von n , aber n nicht notwendigerweise eine p -Potenz. Wir können schreiben $n = p^k \cdot m$, wobei $2 \leq k \in \mathbb{N}$ ist und $m \in \mathbb{N}$ teilerfremd zu p . Mit dem ersten Teil gibt es eine zu p^k teilerfremde Zahl $a \in \mathbb{N}$ mit $\text{ord}_{p^k}(a) = p$.

...

Aufgabe 3.2.19. fehlt noch

Aufgabe 3.2.20. Sei $k := \varphi(n)$, und sei $T = \{b_1, b_2, \dots, b_k\}$ ein vollständiges System teilerfremder Reste modulo n wie in der Aufgabe vorgegeben. Mit Aufgabe 3.1.21 ist aT ebenfalls ein VSTR modulo n . Wir beweisen die einzelnen Behauptungen in der Aufgabe einzeln.

Behauptung. $b_1 \cdot b_2 \cdots b_k \equiv (a \cdot b_1) \cdot (a \cdot b_2) \cdots (a \cdot b_k) \pmod{n}$.

Beweis. Nach Definition eines VSTR ist jedes Element von T zu genau einem Element von aT kongruent modulo n . Für jedes $i \in \{1, \dots, k\}$ sei $i' \in \{1, \dots, n\}$ so gewählt, dass $b_i \equiv a \cdot b_{i'}$ ist modulo n . Dann ist

$$\prod_{i=1}^k b_i \equiv \prod_{i=1}^k a \cdot b_{i'},$$

und wegen unserer Anfangsbemerkung ist die rechte Seite genau das Produkt $(a \cdot b_1) \cdot (a \cdot b_2) \cdots (a \cdot b_k)$. Also sind wir fertig. ■

Behauptung. $b_1 \cdot b_2 \cdots b_k \equiv a^k \cdot (b_1 \cdot b_2 \cdots b_k) \pmod{n}$.

Beweis. Das folgt aus der letzten Aussage, denn es handelt sich um Produkte ganzer Zahlen, und da dürfen wir die Reihenfolge beliebig vertauschen. Auf der rechten Seite steht k -mal der Faktor a , also ist

$$b_1 \cdot b_2 \cdots b_k \equiv (a \cdot b_1) \cdot (a \cdot b_2) \cdots (a \cdot b_k) \equiv a^k \cdot (b_1 \cdot b_2 \cdots b_k) \pmod{n}.$$

Behauptung. $1 \equiv a^k \pmod{n}$.

Beweis. In der vorherigen Aussage sehen wir auf beiden Seiten das Produkt $b_1 \cdot b_2 \cdots b_k$. Wir sind also fertig, falls wir modulo n diese Zahl „wegkürzen“ dürfen. Unsere Kürzungsregel 3.1.4 erlaubt das, denn jede der Zahlen $b_1, \dots, b_k$ ist zu n teilerfremd, und mit Folgerung 1.3.5 ist deshalb auch ihr Produkt teilerfremd zu n . ■

Aufgabe 3.3.2. Wir müssen für alle $n = 9, 21, 25, 27, 31, 33, 35$ testen, ob $2^{n-1} \equiv 1$ ist modulo n . Dementsprechend gibt der Fermat-Test für die Basis 2 diese Zahlen als prim aus, oder, wenn die Kongruenz nicht erfüllt ist, als zusammengesetzt.

$$2^{9-1} = 2^8 = 8^2 \cdot 4 \equiv (-1)^2 \cdot 4 = 4 \text{ modulo } 9,$$

$$2^{21-1} = 2^{20} = 16^5 \equiv 5^5 \cdot 25^2 \cdot 5 \equiv (-5) \cdot 5 = -25 \equiv -4 \text{ modulo } 21,$$

$$2^{25-1} = 2^{24} = 32^4 \cdot 16 \equiv 7^4 \cdot 16 = 49^2 \cdot 16 \equiv (-1)^2 \cdot 16 \equiv -9 \text{ modulo } 25,$$

$$2^{27-1} = 2^{26} = 32^5 \cdot 2 \equiv 5^5 \cdot 2 = 25^2 \cdot 10 \equiv (-2)^2 \cdot 10 = -40 \equiv 13 \text{ modulo } 27,$$

$$2^{33-1} = 2^{32} = 32^6 \cdot 4 \equiv (-1)^6 \cdot 4 = 4 \text{ modulo } 33 \text{ und}$$

$$2^{35-1} = 2^{34} = 32^6 \cdot 16 \equiv (-3)^6 \cdot 16 = (-27)^2 \cdot 16 \equiv 8^2 \cdot 16 = 32^2 \equiv (-3)^2 = 9 \text{ modulo } 35.$$

Es werden also alle diese Zahlen als zusammengesetzt erkannt.

Aufgabe 3.4.11. (a) $(X^4 - 1) : (X^2 - 1) = X^2 + 1$,

(b) $(X^5 + X^4 + X^3 + X^2 + X + 1) : (X^2 + X + 1) = X^3 + 1$ und

(c) $(2X^2 - X) : (X - \frac{1}{2}) = 2X$.

(d) $2X^2 + 3X + 5 = 3X \cdot (\frac{2}{3}X + 1) + 5$.

Aufgabe 3.4.12. Falls P und Q gleich sind, dann ist auch $P(x) = Q(x)$ für alle $x \in \mathbb{Z}$. Gilt umgekehrt $P(x) = Q(x)$ für alle $x \in \mathbb{Z}$, so hat das Polynom $P - Q$ unendlich viele Nullstellen und ist daher nach Folgerung 3.4.5 das Nullpolynom.

Aufgabe 3.4.13. (a) $X^2 - 1 = (X + 1)(X - 1)$, also ist $X^2 - 1$ nicht irreduzibel (weder über $\mathbb{Q}$ noch über $\mathbb{Z}$).

(b) $X^2 + 1$ ist irreduzibel über $\mathbb{Q}$: Angenommen, nicht. Dann müssen die echten Teiler beide vom Grad 1 sein, und durch geeignetes Multiplizieren können wir annehmen, dass beide Teiler normierte rationale Polynome sind. Wir finden also $a, b \in \mathbb{Q}$ so, dass $X^2 + 1 = (X + a)(X + b)$ ist. Ausmultiplizieren liefert

$$X^2 = X^2 + aX + bX + ab = X^2 + (a + b)X + ab.$$

Vergleichen wir die Koeffizienten, so erhalten wir $a + b = 0$ und $ab = 1$. Aber $a + b = 0$ bedeutet $a = -b$, und mit Einsetzen folgt $1 = ab = -b^2$. Das ist unmöglich, denn es gibt keine rationale Zahl, deren Quadrat -1 ist. (Wer sich mit den *komplexen Zahlen* auskennt, wird aber sehen, dass man durchaus Teiler von $X^2 + 1$ mit komplexen Koeffizienten hinschreiben könnte!)

(c) $3X^4 + 2X^2 - 6X + 1$ ist nicht irreduzibel, denn

$$3X^4 + 2X^2 - 6X + 1 = (X - 1)(3X^3 + 3X^2 + 5X - 1).$$

(d) $X^4 + 1$ ist irreduzibel über $\mathbb{Z}$:

Angenommen nicht, und zuerst betrachten wir den Fall, dass $X^4 + 1$ Produkt zweier Polynome vom Grad 2 ist. Seien also $a, b, c, d, e, f \in \mathbb{Z}$ so, dass $X^4 + 1 = (aX^2 + bX + c)(dX^2 + eX + f)$ ist. Ausmultiplizieren liefert dann

$$X^4 + 1 = adX^4 + bdX^3 + cdX^2 + aeX^3 + beX^2 + ceX + afX^2 + bfX + cf = adX^4 + (bd + ae)X^3 + (cd + be + af)X^2 + (ce + bf)X + cf.$$

Ein Koeffizientenvergleich zeigt $ad = 1$, $bd + ae = 0$, $cd + be + af = 0$, $ce + bf = 0$ und $cf = 1$.

1. *Fall:* $a = d = 1$. Dann ist $b + e = 0$, also $b = -e$. Es folgt $0 = cd + be + af = c - b^2 + f$. Aber das impliziert, dass $c = f = 1$ oder $c = f = -1$ sein muss, in jedem Fall sind also c und f gleich. Das liefert $0 = 2c - b^2$, also $b^2 = 2c = \pm 2$, ein Widerspruch. (Die ganzen Zahlen enthalten keine Quadratwurzeln von 2 und -2 .)

2. *Fall:* Das funktioniert genauso, hier ist $a = d = -1$ und wieder $b = -e$. Genau wie oben folgt ein Widerspruch.

Jetzt fehlt noch der Fall, dass $X^4 + 1$ Produkt zweier Polynome ist, von denen eines Grad 1 und das andere Grad 3 hat. Nehmen wir also an, das sei der Fall und wählen $a, b, c, d, e, f \in \mathbb{Z}$ so, dass $X^4 + 1 = (aX^3 + bX^2 + cX + d)(eX + f)$ ist. Diesmal erhalten wir $X^4 + 1 = aeX^4 + afX^3 + beX^3 + bfX^2 + ceX^2 + cfX + deX + df = aeX^4 + (af + be)X^3 + (bf + ce)X^2 + (cf + de)X + df$, also $ae = df = 1$ und $af + be = 0 = bf + ce = cf + de$.

Wieder wissen wir, dass $a = e = \pm 1$ ist und behandeln diesmal beide Fälle gleichzeitig. Es folgt nämlich stets $f = -b$, also ist $0 = bf + ce = -b^2 + ce$. Andererseits haben wir auch $d = f = \pm 1$, also $c = -e$. Damit folgern wir $0 = bf + ce = -b^2 - c^2$. Aber Quadrate sind nicht-negativ, also ist das unmöglich.

Anmerkung. Auch über den rationalen Zahlen zerfällt dieses Polynom nicht. In $\mathbb{R}$ kann man es aber als $X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ schreiben.

Aufgabe 3.4.14. Sei $P = aX^2 + bX + c$ ein ganzzahliges Polynom. Setzen wir zuerst voraus, dass P irreduzibel ist über $\mathbb{Q}$ und zeigen, dass es dann keine rationale Nullstelle gibt. Angenommen, e sei eine rationale Nullstelle. Mit Satz 3.4.4 ist dann $(X - e)$ ein Teiler von P über $\mathbb{Q}$, also P sicherlich nicht irreduzibel über $\mathbb{Q}$.

Setzen wir umgekehrt voraus, dass P keine rationalen Nullstellen besitzt und zeigen, dass P dann irreduzibel ist über $\mathbb{Q}$. Andernfalls gibt es rationale Polynome Q_1, Q_2 vom Grad 1, so dass $P = Q_1 Q_2$ ist. Sei etwa $Q_1 = d_1x + d_2$ mit $d_i \in \mathbb{Q}$. Dann ist $d := \frac{d_2}{d_1}$ eine Nullstelle von Q_1 und daher auch von P , entgegen unserer Voraussetzung.

Aufgabe 3.4.15.

Behauptung. Ist P ein rationales Polynom mit $\text{grad } P \geq 1$, so gibt es ein über $\mathbb{Q}$ irreduzibles ganzzahliges Polynom H , welches P teilt.

Beweis. Wir argumentieren ähnlich zu dem Beweis, dass jede natürliche Zahl $n \geq 2$ einen Primfaktor besitzt. Es sei dazu $k \geq 1$ minimal mit der Eigenschaft, dass es ein rationales Polynom H' des Grades k gibt, welches P über $\mathbb{Q}$ teilt. Die Koeffizienten von H' sind allesamt rationale Zahlen; es sei d das kleinste gemeinsame Vielfache der Nenner dieser Koeffizienten. Dann ist $H := d \cdot H'$ ein ganzzahliges Polynom vom Grad k , und wegen $H' = \frac{1}{d} \cdot H$ ist auch H ein Teiler von P über $\mathbb{Q}$.

Wir behaupten, dass H irreduzibel über $\mathbb{Q}$ ist. Ein nicht-trivialer Teiler T von H über $\mathbb{Q}$ wäre nämlich auch ein Teiler von P mit $1 \leq \deg T < k$, und das würde der Wahl von k widersprechen. ■

Aufgabe 3.4.16. Polynomdivision ergibt

$$Y^2 - 2 \equiv (Y - (X - 3)) \cdot (Y + (X - 3)) \pmod{X^2 - 6X + 7}.$$

Also ist $3 - X$ eine zweite polynomiale Nullstelle von $Y^2 - 2$, was man durch Einsetzen nachprüfen kann:

$$(3 - X)^2 - 2 = 9 - 6X + X^2 - 2 = X^2 - 6X + 7 \equiv 0 \pmod{X^2 - 6X + 7}.$$

Alternativ kann man diese Nullstelle auch finden, indem man bemerkt, dass $X - 3$ und $3 - X$ beim Einsetzen in $Y^2 - 2$ das gleiche Ergebnis haben.

(Natürlich ist auch jedes zu $X - 3$ oder $3 - X$ modulo $X^2 - 6X + 7$ kongruente Polynom eine polynomiale Nullstelle – wir betrachten diese aber als „dieselben“ Nullstellen.

Aufgabe 3.4.17. Setze $Q := Y^2 - 1$ und $H := X^2 - 1$. Dann hat Q modulo H die polynomialen Nullstellen $1, -1, X$ und $-X$, und diese Polynome sind alle modulo H verschieden.

Aufgabe 3.5.7. Es sei $n \geq 2$. Wir möchten ein Polynom P zu finden mit $P \not\equiv 0 \pmod{n}$, aber $P(x) \equiv 0 \pmod{n}$ für alle $x \in \mathbb{Z}$. Das ist ganz einfach, denn wir müssen P nur so wählen, dass z.B. jede der Zahlen von 0 bis $n - 1$ eine Nullstelle von P (in $\mathbb{Z}$) ist. Also können wir etwa

$$P := X \cdot (X - 1) \cdot (X - 2) \cdots (X - (n - 1))$$

verwenden. Ist n eine Primzahl, so hat nach dem Satz von Fermat auch

$$P := X^n - X$$

die geforderte Eigenschaft.

Aufgabe 3.5.8. Durch Polynomdivision erhalten wir:

$$\begin{aligned}
 X^4 + X^2 - 2 &= (X^2 - X + 1) \cdot (X^2 + X + 1) - 3 \\
 &\equiv 0 \pmod{3, X^2 + X + 1}; \\
 2X^5 + 3X^3 + X^2 + 1 &= (2X^3 + X + 1) \cdot (X^2 + 1) - X \\
 &\equiv 5X \pmod{6}; \\
 2X^5 + 4X^2 + X + 5 &= (2X^2 - 4X - 2) \cdot (X^3 + 2X^2 + 5X + 6) + 16X^2 + 35X + 17 \\
 &\equiv 2X^2 + 3 \pmod{7, X^3 + 2X^2 + 5X + 6}.
 \end{aligned}$$

Aufgabe 3.5.9. Es sei $n \geq 2$ eine natürliche Zahl. Außerdem seien P und Q Polynome, wobei der Leitkoeffizient von P zu n teilerfremd ist und alle auftretenden Koeffizienten (der Einfachheit halber) zwischen 0 und $n-1$ liegen. Wir betrachten das Teilen mit Rest von Q durch P modulo n ; d.h. wir suchen Polynome T und R mit

$$Q \equiv T \cdot P + R \pmod{n}.$$

Das Verfahren funktioniert ja wie folgt:

1. Ist $\text{grad } Q < \text{grad } P$, so ist $T = 0$ und $R = Q$, und wir sind fertig.
2. Sonst setzen wir $k := \text{grad } Q - \text{grad } P$ und teilen den Leitkoeffizienten von Q modulo n durch den Leitkoeffizienten von P . Wir nennen das Ergebnis a ; das Polynom T wird dann Grad k haben und Leitkoeffizienten a .
3. Um die weiteren Koeffizienten von T und den Rest R zu bestimmen, berechnen wir das Polynom $Q - a \cdot P \cdot X^k$ und reduzieren alle Koeffizienten modulo n . Wir ersetzen Q durch das so erhaltene Polynom Q' und machen bei Schritt 1 weiter.

Wir wissen, dass die Division modulo n effizient durchführbar ist, und Schritt 3 erfordert für jeden der Koeffizienten von Q höchstens eine Multiplikation und eine Subtraktion modulo n . Das Polynom Q' hat modulo n kleineren Grad als Q , also werden die Schritte 2 und 3 höchstens $(\text{grad } Q - \text{grad } P)$ -mal ausgeführt. Insgesamt ist das Verfahren polynomiell in $\log n$, $\text{grad } P$ und $\text{grad } Q$.

Insbesondere können Summen und Produkte modulo n und H effizient berechnet werden. Denn Summen und Produkte von ganzzahligen Polynomen können effizient berechnet werden: Für die Summe müssen nur die Koeffizienten addiert werden; das Produkt zweier Polynome P und Q erfordert (mit dem „offensichtlichen“ Algorithmus) bis zu $\text{grad } P \cdot \text{grad } Q$ Multiplikationen von Koeffizienten und höchstens $\text{grad } P \cdot \text{grad } Q$ Additionen der resultierenden Zahlen. Danach müssen wir dann noch jeweils eine Division mit Rest durch H modulo n durchführen, die ja wie oben besprochen effizient ist.

Zu guter Letzt können wir Potenzen modulo n und H wie in Aufgabe 2.3.6 berechnen. Dabei ist es wichtig, wie in Aufgabe 3.1.12 in jedem Schritt die auftretenden Polynome

durch den Rest beim Teilen durch H modulo n zu ersetzen. (Damit wird verhindert, dass die Koeffizienten und die Grade dieser Polynome zu groß werden.)

Aufgabe 3.5.11. Es sei $n \geq 2$, $a \in \mathbb{Z}$ und P ein Polynom.

Behauptung. (a) a ist eine Nullstelle von P modulo n genau dann, wenn $(X - a)$ ein Teiler von P modulo n ist.

(b) Ist $P \not\equiv 0 \pmod{n}$, so hat P eine Darstellung

$$P \equiv (X - a_1) \cdots (X - a_m) \cdot Q \pmod{n}. \quad (3.2)$$

Hierbei ist $m \geq 0$, jede der Zahlen $a_1, \dots, a_m$ liegt zwischen 0 und $n - 1$ und Q ist ein Polynom, welches keine Nullstellen modulo n besitzt.

(c) Ist n prim, so sind die Zahlen $a_1, \dots, a_m$ bis auf die Reihenfolge eindeutig bestimmt. Das heißt, ist

$$P \equiv (X - b_1) \cdots (X - b_k) \cdot R \pmod{n}$$

eine weitere solche Darstellung, so ist $m = k$ und die b_j stimmen bis auf die Reihenfolge mit den a_j überein.

(d) Ist n prim und $P \not\equiv 0 \pmod{n}$, so hat P modulo n höchstens $\text{grad}_n(P)$ Nullstellen.

Beweisskizze. Teil (a) geht genauso wie Satz 3.4.4. Ist $(X - a)$ ein Teiler von P modulo n , so ist klar, dass dann a eine Nullstelle von P modulo n sein muss. Ist umgekehrt a eine Nullstelle von P modulo n , so teilen wir P mit Rest durch $(X - a)$. Der Rest (ein konstantes Polynom) muss dann wegen $P(a) \equiv 0 \pmod{n}$ zu 0 kongruent sein.

Teil (b) folgt aus Teil (a) durch Induktion nach dem Grad von P . Hat P selbst keine Nullstellen modulo n , so setzen wir $m := 0$ und $Q := P$. Andernfalls sei a eine Nullstelle von P modulo n ; dann können wir nach (a) durch $X - a$ teilen und erhalten $P \equiv (X - a) \cdot P' \pmod{n}$, wobei $\text{grad } P' = \text{grad } P - 1$ gilt. Die Behauptung folgt dann aus der Induktionsvoraussetzung.

Teil (c) können wir so ähnlich beweisen wie die Eindeutigkeit der Primfaktorzerlegung von natürlichen Zahlen (Satz 1.4.2). Wir argumentieren dazu per Induktion über die Zahl m aus der Darstellung von P gemäß (3.2). Ist $m = 0$, so ist also $P \equiv Q \pmod{n}$, und P besitzt keine Nullstellen modulo n . Dann hat P offensichtlich keine andere solche Darstellung. Andernfalls gibt es eine Nullstelle a von P modulo n mit $0 \leq a < n$. Sind

$$P \equiv (X - a_1) \cdots (X - a_m) \cdot Q \quad \text{und} \quad P \equiv (X - b_1) \cdots (X - b_k) \cdot R \pmod{n}$$

zwei Darstellungen wie oben, so muss wegen der Nullteilerfreiheit modulo p (Aufgabe 3.1.11) eine der Zahlen a_j zu a kongruent sein und ebenso eine der Zahlen b_j . Wir können die Darstellungen also so umordnen, dass $a_1 \equiv a \equiv b_1 \pmod{n}$ gilt. Wenn wir jetzt die Induktionsvoraussetzung auf

$$P' := (X - a_2) \cdots (X - a_m) \cdot Q \equiv (X - b_2) \cdots (X - b_k) \cdot Q$$

anwenden, sind wir fertig.

Teil (d) folgt ebenso aus Teil (b) und der Nullteilerfreiheit, denn die Nullstellen von P modulo n sind genau die zu $a_1, \dots, a_m$ kongruenten ganzen Zahlen und es gilt $m \leq \deg P$. (Alternativ können wir wie in Folgerung 3.4.5 (d) mit Hilfe von (a) und einer Induktion beweisen.) ■

Aufgabe 3.5.12. Das Polynom $P = X^2 + 1$ ist nicht irreduzibel modulo 2 (obwohl es irreduzibel über $\mathbb{Z}$ und $\mathbb{Q}$ ist). In der Tat besitzt es ja modulo 2 eine Nullstelle, denn

$$P(1) = 1^2 + 1 = 2 \equiv 0 \pmod{2}.$$

Also können wir P durch den Linearfaktor $X - 1$ teilen:

$$X^2 + 1 \equiv X^2 - 2X + 1 = (X - 1)^2 \pmod{2}.$$

Für $Q = 5X^2 + X + 1$ gehen wir ähnlich vor. Zunächst überlegen wir uns, dass Q keine rationalen, und sogar keine reellen Nullstellen besitzt, denn es gilt $Q(x) > 0$ für alle $x \in \mathbb{R}$.

(Das sieht man leicht mit den üblichen, aus der Schule bekannten Formeln. Alternativ können wir auch einfach darauf hinweisen, dass auf jeden Fall $Q(x) > 0$ gilt, wenn $x > -1$ ist, denn dann ist $5x^2 + x + 1 \geq x + 1 > 0$. Andererseits gilt für $x \leq -1$ auf jeden Fall $5x^2 + x > x^2 + x \geq 0$.)

Deshalb ist Q irreduzibel über $\mathbb{Q}$, denn jeder nichttriviale Teiler von Q müsste Grad 1 haben und damit eine Nullstelle besitzen.

Modulo 7 aber gibt es wieder Nullstellen, z.B. gilt ja

$$5 \cdot 1^2 + 1 + 1 = 7 \equiv 0 \pmod{7}.$$

Wir können jetzt wieder Polynomdivision vornehmen, und sehen

$$5X^2 + X + 1 \equiv (5X + 6) \cdot (X - 1) \pmod{7}.$$

(Wenn wir das Polynom vollständig in Linearfaktoren zerlegen wollen wie in der vorhergehenden Aufgabe, können wir noch $5X + 6 \equiv 5(X + 4) \pmod{7}$ schreiben, und damit $Q \equiv 5(X + 4)(X - 1) \pmod{7}$.)

Aufgabe 3.5.13. Ist n eine natürliche Zahl, so ist das Polynom $X^2 + n$ über $\mathbb{Q}$ irreduzibel, weil es den Grad 2 hat und keine Nullstellen besitzt.

Modulo n gilt aber $X^2 + n \equiv X^2 = X \cdot X$.

Bemerkung. Wir hatten im Text Irreduzibilität eines Polynoms nur modulo einer Primzahl definiert, aber die Aussage ist – mit der entsprechenden Definition – für alle natürlichen Zahlen richtig.

Aufgabe 3.5.14. Es sei p eine Primzahl und P ein Polynom mit $P \not\equiv 0 \pmod{p}$.

Behauptung. (a) Ist $\text{grad}_p(P) > 0$, so gibt es ein normiertes und modulo p irreduzibles Polynom H , welches modulo p ein Teiler von P ist.

(b) Es gibt $m \geq 0$, $a \in \mathbb{Z}$ und irreduzible normierte Polynome $H_1, \dots, H_m$ mit

$$P \equiv a \cdot H_1 \cdots H_m \pmod{p}.$$

Beweisskizze. Der Beweis von Teil (a) ist vollkommen analog zu Aufgabe 3.4.15.

Teil (b) folgt aus Teil (a) durch Induktion über den Grad von P ; wir überlassen der Leserin die Details. ■

Aufgabe 3.5.15. Am Anfang des Beweises von Satz 3.5.6 hatten wir folgende Aussage formuliert: *Ist H ein modulo p irreduzibles Polynom, welches ein Produkt $B \cdot C$ modulo p teilt, so teilt H auch eines der Polynome B und C modulo p .*

Mit ihrer Hilfe können wir nun die Eindeutigkeit der Zerlegung in irreduzible Faktoren (modulo p und bis auf die Reihenfolge) ganz genauso per Induktion beweisen, wie wir das im Fundamentalsatz der Arithmetik (Satz 1.4.2) für die Eindeutigkeit der Primfaktorzerlegung einer natürlichen Zahl getan hatten. Eine detaillierte Ausarbeitung dieses Beweises überlassen wir der Leserin.

Kapitel 4

Primzahlen und Kryptographie

Aufgabe 4.4.5. Es sei $n \geq 1$ und $v(n)$ das kleinste gemeinsame Vielfache von $1, 2, 3, \dots, n$.

Behauptung (a). Es gilt $v(n) \geq 2^{\pi(n)}$.

Beweis. Die Behauptung ist für $n = 1$ richtig, denn es gilt $v(1) = 1$ und $\pi(1) = 0$.

Sei nun $n \geq 2$ und setze $k := \pi(n)$. Nach Definition sind dann unter den Zahlen $1, 2, 3, \dots, n$ genau k Primzahlen; nennen wir sie $p_1, \dots, p_k$. Es gilt also

$$\text{kgV}(p_1, \dots, p_k) \mid v(n).$$

Nun ist aber $\text{kgV}(p_1, \dots, p_k) = \prod_{j=1}^k p_j$ (siehe Aufgabe 1.3.7). Also wird $v(n)$ von diesem Produkt geteilt; insbesondere gilt (wegen $p_j \geq 2$):

$$v(n) \geq \prod_{j=1}^k p_j \geq 2^k. \quad \blacksquare$$

Bemerkung. Wir hätten den Fall $n = 1$ eigentlich nicht gesondert behandeln müssen, auch hier ist der Beweis richtig. Denn es gilt dann $k = 0$, und sowohl $v(1)$ als auch das (leere) Produkt über die Primzahlen ≤ 1 sind gleich 1.

Behauptung (b). Es gilt $v(n) \geq \sqrt{n}^{\pi(n)}$.

Beweis. Wieder ist nur der Fall $n \geq 2$ zu behandeln. Es seien dazu wie oben $k = \pi(n)$ und $p_1, \dots, p_k$ die Primzahlen $\leq n$. Sei

$$v(n) = p_1^{e_1} \cdots p_k^{e_k}$$

die Primfaktorzerlegung von $v(n)$. Wie im Beweis von Hilfssatz 4.4.2 erwähnt, ist dabei e_j die größte natürliche Zahl mit $p_j^{e_j} \leq n$. Insbesondere gilt $p_j^{e_j} \geq \sqrt{n}$, denn sonst wäre $p_j^{e_j+1} < n$. Also gilt, wie behauptet:

$$v(n) = \prod_{j=1}^k p_j^{e_j} \geq \sqrt{n}^k. \quad \blacksquare$$

Aufgabe 4.5.7. Festzustellen, ob n gerade ist, erfordert nur eine Division mit Rest durch 2, und die ist sicher effizient möglich. (Wenn n , wie üblich, im Binärsystem gegeben ist, ist das sogar noch einfacher – wir müssen nur schauen, ob die letzte Stelle eine 0 ist.) Dass echte Potenzen effizient erkannt werden können, ist Aufgabe 2.3.7.

Die Zahl $n - 1$ als $d \cdot 2^l$ zu schreiben, erfordert höchstens $\lfloor \log n \rfloor + 1$ Divisionen mit Rest. (Im Binärsystem ist es wieder noch einfacher, wie die Leserin sich selbst überlegen kann.)

Zum Test der Teilerfremdheit von a und n verwenden wir den Euklidischen Algorithmus; dieser ist effizient (Aufgabe 2.3.5). Berechnung der Potenz $a^d \bmod n$ ist ebenfalls effizient möglich (Aufgabe 3.1.12).

Dasselbe gilt für die Potenzen b, b^2, b^4 , etc. Wir müssen hier höchstens $l - 1$ Zahlen berechnen, und es gilt ja $l \leq \log n$. Also ist der Algorithmus insgesamt effizient.

Kapitel 5

Der Ausgangspunkt: Fermat für Polynome

Aufgabe 5.1.4. Es sei $n \geq 2$ eine natürliche Zahl und p ein Primteiler von n . Ferner sei j der größte Exponent derart, dass p^j ein Teiler von n ist.

Behauptung (a). Es gilt $\binom{n}{p} \not\equiv 0 \pmod{p^j}$.

Beweis. Es ist

$$p! \binom{n}{p} = \frac{n!}{(n-p)!} = (n-p+1) \cdot (n-p+2) \cdots n.$$

Da $(n-p+1)$ bis $n-1$ nicht von p geteilt werden, wird die rechte Seite dieser Gleichung von p^j geteilt, aber nicht von p^{j+1} . Also wird auch die linke Seite der Gleichung nicht von p^{j+1} geteilt, und daher wird $\binom{n}{p}$ nicht von p^j geteilt, wie behauptet. ■

Behauptung (b). Es gilt $\binom{n}{p^j} \not\equiv 0 \pmod{p}$.

Beweis. Die Idee ist ähnlich wie oben, aber wir müssen etwas genauer zählen. Es gilt wieder

$$(p^j)! \binom{n}{p^j} = (n-p^j+1) \cdot (n-p^j+2) \cdots n.$$

Wir müssen nun zeigen, dass die höchste Potenz von p , die die rechte Seite der Gleichung teilt, auch $(p^j)!$ teilt. Dazu bezeichnen wir mit $e_p(m) \in \mathbb{N}_0$ den Exponenten, mit dem p in der Primfaktorzerlegung von $m \in \mathbb{N}$ auftaucht. D.h. $p^{e_p(m)}$ teilt m , aber $p^{e_p(m)+1}$ tut das nicht.

Ist jetzt $k \in \mathbb{N}$ mit $k \leq p^j$, so gilt

$$e_p(k) = e_p(n - p^j + k).$$

(Überlege selbst, warum!) Also ist

$$e_p((p^j)!) = \sum_{k=1}^{p^j} e_p(k) = \sum_{k=1}^{p^j} e_p(n - p^j + k) = e_p((n - p^j + 1) \cdots n).$$

Mit Hilfssatz 1.4.1 muss

$$e_p\left(\binom{n}{p^j}\right) = 0$$

sein, wie behauptet. ■

Aufgabe 5.1.6. Hier geht es darum, einen effizienten Algorithmus für die Prüfung der Kongruenz

$$(P(X))^n \equiv P(X^n) \pmod{n, Q}$$

anzugeben.

Dabei ist $n \geq 2$, Q und P sind ganzzahlige Polynome, deren Koeffizienten zwischen 0 und $n - 1$ liegen, und der Grad $d := \text{grad } P$ ist kleiner als $r := \text{grad } Q$. Außerdem soll der Leitkoeffizient von Q zu n teilerfremd sein.

Dass die Potenz $((P(X))^n \pmod{n, Q})$ effizient berechnet werden kann, haben wir bereits in Aufgabe 3.5.9 gesehen. Das heißt, wir können effizient das (eindeutig bestimmte) modulo n und Q zu $(P(X))^n$ kongruente Polynom berechnen, dessen Grad kleiner als r ist und dessen Koeffizienten zwischen 0 und $n - 1$ liegen.

Schreibe nun

$$P(X) = a_d X^d + \cdots + a_1 X + a_0.$$

Dann ist

$$P(X^n) = a_d X^{nd} + \cdots + a_1 X^n + a_0.$$

Wieder aufgrund von Aufgabe 3.5.9 können wir die Potenzen X^{nd} , $X^{n(d-1)}$, $\dots$, X^n modulo n und Q effizient berechnen. Zur Berechnung von $P(X^n)$ müssen wir jetzt nur noch $d + 1$ Polynome von kleinerem Grad als r addieren und dann modulo n und Q reduzieren, was effizient möglich ist.

Zu guter Letzt müssen die höchstens r Koeffizienten der beiden Ergebnisse verglichen werden, und wir sind fertig.

Aufgabe 5.2.1.

Behauptung. Es sei p eine Primzahl und P ein (ganzzahliges) Polynom. Dann gilt für alle $m \in \mathbb{N}_0$:

$$(P(X))^{p^m} \equiv P(X^{p^m}) \pmod{p}.$$

Beweis. Die Idee ist ganz einfach: Potenzieren mit p^m ist dasselbe, wie m -mal mit p zu potenzieren. Das heißt, wir müssen nur m -mal Satz 5.1.1 anwenden und sind fertig.

Formal beweisen wir die Behauptung durch Induktion nach m . Für $m = 0$ ist die Behauptung trivial, denn es gilt

$$(P(X))^{p^0} = P(X) = P(X^{p^0}).$$

Es sei die Behauptung nun für $m \geq 0$ richtig, und wir müssen sie für $m+1$ verifizieren. Es gilt nach Induktionsvoraussetzung:

$$(P(X))^{p^{m+1}} = \left((P(X))^{p^m} \right)^p \equiv (P(X^{p^m}))^p \pmod{p}.$$

Mit Satz 5.1.1 ist außerdem

$$(P(X^{p^m}))^p \equiv P((X^p)^{p^m}) = P(X^{p^{m+1}}) \pmod{p},$$

wie behauptet. ■

Aufgabe 5.2.2. Sei n eine zusammengesetzte Zahl, die zwei verschiedene Primteiler p und q besitzt. Sei außerdem a zu n teilerfremd.

Behauptung. Es gilt

$$(X + a)^n \not\equiv X^n + a \pmod{p}.$$

Beweis. Der Beweis ist wie in Satz 5.1.3, aber jetzt unter Verwendung von Aufgabe 5.1.4 (b).

Es sei j die größte Zahl mit $p^j \mid n$; dann gilt nach Voraussetzung $p^j < n$. Der p^j -te Koeffizient von $(X + a)^n$ ist

$$\binom{n}{p^j} a^{p^j},$$

und dieser ist nach Aufgabe 5.1.4 (b) modulo p nicht zu Null kongruent. ■

Kapitel 6

Der Satz von Agrawal, Kayal und Saxena

Aufgabe 6.3.6. Setze $m := \lceil 2\sqrt{t} \log n \rceil$. Dann gilt (wie im Beweis von Folgerung 6.3.5) $t \geq m$. Außerdem gilt nach Voraussetzung $\ell \geq m$. Nun ist

$$A \geq \binom{t + \ell - 1}{t - 1} \geq \binom{m - 1 + \ell}{m - 1} > \binom{2(m - 1)}{m - 1}$$

wegen Aufgabe 1.1.12. (Die Leserin überlege sich selbst, warum im letzten Schritt eine *echte* Ungleichung gilt.)

Insgesamt gilt also wie im Beweis der Folgerung:

$$A \geq 2^{m-1} = \frac{n^{2\sqrt{t}}}{2},$$

und die Behauptung folgt wie dort.

Aufgabe 6.4.3. Es sei $n \geq 2$ und H ein Polynom, dessen Leitkoeffizient zu n teilerfremd ist.

Behauptung. Es sei $r \geq 1$ mit $X^r \equiv 1 \pmod{n, H}$, und es sei k die kleinste natürliche Zahl mit $X^k \equiv 1 \pmod{n, H}$. Dann gilt $k \mid r$.

Beweis. Das geht haargenau so wie in Hilfssatz 3.2.1. Wir teilen r mit Rest durch k :

$$r = t \cdot k + r_0,$$

wobei $0 \leq r_0 < k$ gilt. Dann ist

$$1 \equiv X^r = X^{t \cdot k + r_0} = (X^k)^t \cdot X^{r_0} \equiv X^{r_0} \pmod{n, H}.$$

Wegen $r_0 < k$ und nach Wahl von k muss also $r_0 = 0$ gelten. Also gilt $r = t \cdot k$ und damit $k \mid r$ wie behauptet. ■

Aufgabe 6.4.4. Es sei r eine Primzahl und K_r das r -te Kreisteilungspolynom.

Behauptung (a). Für das Polynom $K' := K_r(X + 1)$ gilt

$$K' \equiv X^{r-1} \pmod{r}.$$

Beweis. Es ist $X \cdot K' = (X + 1)^r - 1$. Wegen Satz 5.1.1 gilt also

$$X \cdot K' \equiv X^r + 1 - 1 = X^r \pmod{r}.$$

Das bedeutet nichts anderes, als dass der Koeffizient von X^{r-1} in K' kongruent ist zu 1 modulo r und dass alle anderen Koeffizienten durch r teilbar sind. Damit ist die Behauptung bewiesen. ■

Behauptung (b). Das Polynom K' ist irreduzibel über $\mathbb{Q}$.

Beweis. Das folgt sofort aus dem Eisensteinschen Irreduzibilitätskriterium, denn mit Teil (a) ist der Leitkoeffizient von K' nicht durch r teilbar, und alle anderen Koeffizienten sind durch r teilbar. Außerdem ist der konstante Koeffizient von K' gleich r , denn

$$K' = (X + 1)^{r-1} + \cdots + (X + 1)^2 + (X + 1) + 1,$$

und der konstante Koeffizient jedes der r Summanden ist gleich 1. ■

Behauptung (c). K_r ist irreduzibel über $\mathbb{Q}$.

Beweis. Hätte K_r einen nichttrivialen Teiler T über $\mathbb{Q}$, so wäre $T(X+1)$ ein nichttrivialer Teiler von K' über $\mathbb{Q}$, und daher folgt diese Behauptung aus Teil (b). ■

Primzahltests für Einsteiger
Zahlentheorie – Algorithmik – Kryptographie
Waldecker, R.; Rempe-Gillen, L.
2016, XX, 211 S., Softcover
ISBN: 978-3-658-11216-5