Übungen zu

Reste sind doch das Beste

Martin Kreuzer

Universität Passau

martin.kreuzer@uni-passau.de

Lehrerfortbildung

"TOP Secret - Geheimnisvolle Berechnungen"

Universität Passau, 15.12.2023

Inhaltsübersicht

1. **Grundlagen der Resterechnung**
2. **Der chinesische Restsatz**
3. **Der kleine Satz von Fermat**
4. **Der Satz von Euler**
5. **Fortgeschrittene Resterechnung**

§1. Grundlagen der Resterechnung

Lieber ein Spatz in der Hand
als eine Taube auf dem Dach.
A sparrow in the hand
will poop on your wrist.

Leonardo von Pisa (auch bekannt als **Fibonacci**) schrieb **1202** das

Liber Abaci

also das **Buch vom Abakus** oder das **Buch der Berechnungen**. Es enthält auf ca. 450 Seiten in 15 Kapiteln hunderte von Aufgaben, die die Basis der Mathematikausbildung im Mittelalter bildeten.

Erster Vogelkauf

Aufgabe 1. *Jemand kauft 30 Vögel für insgesamt 30 Denare, und zwar Rebhühner zu je 3 Denaren, Tauben zu je 2 Denaren und Spatzen zu einem Denar je zwei Stück. Wie viele Vögel jeder Sorte wurden erworben, wenn es jeweils mindestens einer war?*

Lösung 1. Sei r die Zahl der gekauften Rebhühner, t die der Tauben und s die der Spatzen. Dann gilt

$$r + s + t = 30 \qquad \text{und} \qquad 3\,r + 2\,t + \frac{1}{2}\,s = 30.$$

Wir multiplizieren die zweite Gleichung mit 2 und subtrahieren die erste. Es ergibt sich $5\,r + 3\,t = 30$.

Betrachten wir die Gleichung $5\,r + 3\,t = 30$ modulo 5, so erhalten wir $\bar{3} \cdot \bar{t} = \bar{0}$, und da man hier durch $\bar{3}$ teilen darf, ergibt sich $\bar{t} = 0$.

Dies zeigt, dass t von der Form $t = 5u$ ist mit $u \in \mathbb{Z}$.

Entsprechend können wir $5r + 3t = 30$ modulo 3 betrachten und erhalten $r = 3v$ mit $v \in \mathbb{Z}$.

Zusammengenommen ergibt sich $u + v = 2$, also $u = v = 1$, da ja von jeder Sorte mindestens ein Tier gekauft wurde.

Die Lösung der Aufgabe ist dann $r = 3v = 3$ und $t = 5u = 5$ und $s = 30 - r - t = 22$.

Es wurden also **3 Rebhühner** zu 9 Denaren, **5 Tauben** zu 10 Denaren und **22 Spatzen** zu 11 Denaren gekauft.

Zweiter Vogelkauf

Aufgabe 2: (Der zweite Vogelkauf)

Jemand kauft 12 Vögel zu insgesamt 12 Denaren, wobei er für jedes Rebhuhn 2 Denare, für je zwei Tauben 1 Denar und für je vier Spatzen 1 Denar zahlt. Wie viele Vögel jeder Sorte hat er gekauft, wenn es jeweils mindestens einer war?

Lösung 2: Sei r die Zahl der gekauften Rebhühner, t die der Tauben und s die der Spatzen. Dann gilt $2r+\frac{1}{2}t+\frac{1}{4}s = 12$ und $r+t+s = 12$. Hieraus erhalten wir $7r + t = 36$. Wegen $t \leq 12$ folgt $r \in \{4, 5\}$. Der Fall $r = 4$ ergibt $t = 8$ und $s = 0$, was aber $s > 0$ widerspricht. Also muss $r = 5$, $t = 1$ und $s = 6$ gelten.

Dritter Vogelkauf

Aufgabe 3: (Der dritte Vogelkauf)

Jemand kauft 30 Vögel zu insgesamt 30 Denaren. Er erwirbt Rebhühner zu je 3 Denaren, Tauben zu je 2 Denaren, Turteltauben zu 1 Denar für zwei Stück und Spatzen zu 1 Denar für 4 Stück. Da ihm Spatzen besonders gut schmecken, hat er möglichst viele davon gekauft. Wie viele waren es?

Lösung 3: Neben den üblichen Bezeichnungen r, s, t sei u die Zahl der gekauften Turteltauben. Dann gilt

$$r + s + t + u = 30 \qquad \text{sowie} \qquad 12r + s + 8t + 2u = 120$$

woraus wir sofort $s = 2\tilde{s}$ mit $\tilde{s} \in \{1, 2, \ldots, 13\}$ sehen.

Nun lösen wir die beiden Gleichungen nach $\tilde{s}$ und u auf und erhalten

$$\tilde{s} \;=\; 5r + 3t - 30 \;\in\; \{1, \ldots, 13\}$$
$$u \;=\; 90 - 11r - 7t \;\in\; \{1, \ldots, 26\}$$

In jedem der Fälle $r \in \{1, \ldots, 7\}$ ist t maximal zu wählen, d.h. wir müssen $90 - 11r = 7t + u$ **mit Rest durch 7 teilen**, um t und u zu berechnen.

Der maximale Wert $\tilde{s} = 9$, also $s = 18$, ergibt sich für $r = 6$, $t = 3$, $u = 3$ oder für $r = 3$, $t = 8$, $u = 1$.

Das Problem des Geisteswissenschaftlers

Aufgabe 4: **Ich wenigstens kenne keine vollbefriedigende Erklärung dafür, warum jede ungerade Zahl (von 3 ab), mit sich selbst multipliziert, stets ein Vielfaches von 8 mit 1 als Rest ergibt.**

(Erich Bischoff, Erforscher der Kabbalah, 1920)

Lösung 4: Schreibe $a = 2n + 1$. Dann gilt $a^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1$. Da $n(n+1)$ gerade ist, schreiben wir $n(n+1) = 2m$. Dann hat die Zahl $a^2 = 8m + 1$ den Rest 1 modulo 8.

Aufgabe 5: Sei $n \in \mathbb{N}_+$ weder durch 2 noch durch 5 teilbar. Zeige, dass es ein Vielfaches von n gibt von der Form $111\cdots11$, d.h. im Zehnersystem sind alle Ziffern 1.

Lösung 5: Betrachte die Zahlen 1, 11, 111, ... modulo n.

Nach dem **Schubfachprinzip** müssen zwei davon denselben Rest modulo n haben.

Die Differenz dieser beiden Zahlen ist dann von der Form

$$111\cdots1100\cdots00 \;=\; (111\cdots11)\cdot 10^k$$

und durch n teilbar.

Wegen $\mathrm{ggT}(n, 10) = 1$ kann man die Faktoren 10 aus dieser Zahl streichen und die verbleibende Zahl $111\cdots11$ ist immer noch durch n teilbar.

§2. Der chinesische Restsatz

Erfahrung ist ein Kamm,
den uns die Natur gibt,
wenn wir bereits eine Glatze haben.
(Chinesisches Sprichwort)

Der indische Mathematiker und Astronom **Brahmagupta** (598-665) schrieb ca. 628 ein Werk **Brahma-sphuta-siddhanta** (Der Anfang des Universums), in dem erstmals die korrekte Verwendung der Null und Rechnungen mit negativen Zahlen erklärt wurden.

Aufgabe 6: (Kap. 8 *Algebra*, §1) Welche Zahl liefert geteilt durch 6 den Rest 5, geteilt durch 5 den Rest 4, geteilt durch 4 den Rest 3 und geteilt durch 3 den Rest 2?

Lösung 6: Wir sollen folgende simultane Kongruenzen lösen:

$$x \equiv 5 \,(\mathrm{mod}\ 6), \quad x \equiv 4 \,(\mathrm{mod}\ 5), \quad x \equiv 3 \,(\mathrm{mod}\ 4), \quad x \equiv 2 \,(\mathrm{mod}\ 3)$$

Die erste Kongruenz ist dabei äquivalent zur vierten und zu $x \equiv 1 \,(\mathrm{mod}\ 2)$, wobei letztere Bedingung schon aus der dritten Kongruenz folgt. Wir können die erste Kongruenz also weglassen, weil sie aus den anderen folgt.

Für die zweite und dritte Kongruenz berechnen wir $a, b \in \mathbb{Z}$ mit $a \cdot 5 + b \cdot 4 = 1$. Offensichtlich funktioniert $a = 1$, $b = -1$. Eine Lösung ist also $x = 4 \cdot (-4) + 3 \cdot 5 = -1$.

Jetzt sehen wir, dass $x = -1$ zufällig auch die dritte Kongruenz löst. Insgesamt folgt $\mathbb{L} = -1 + 3 \cdot 4 \cdot 5\,\mathbb{Z} = -1 + 60\,\mathbb{Z} = \mathbf{59} + 60\,\mathbb{Z}$.

Die Eieraufgabe

Aufgabe 7: (Aus einem byzantinischen Rechenbuch, 15. Jhd.)
Eine Frau geht mit einem Korb Eier auf den Markt. Beginnt man den Korb zu leeren, indem man immer zwei Eier nimmt, so bleibt ein Ei übrig. Nimmt man aber immer drei Eier, so bleiben zwei Eier übrig. Entsprechend ergibt sich bei vier Eiern ein Rest von drei, bei fünf Eiern ein Rest von vier und bei sechs Eiern ein Rest von fünf. Erst wenn man sieben Eier auf einmal aus dem Korb nimmt, ist er am Ende leer. Wie viele Eier befinden sich mindestens im Korb?

Lösung 7: Die simultanen Kongruenzen $x \equiv 1 \,(\mathrm{mod}\ 2)$, $\ldots$, $x \equiv 5 \,(\mathrm{mod}\ 6)$ haben wir soeben gelöst und $\mathbb{L} = 59 + 60\,\mathbb{Z}$ erhalten. Die kleineste durch 7 teilbare positive Zahl in $\mathbb{L}$ ist **119**.

Noch eine Eieraufgabe

Aufgabe 8: Eine Frau bringt einen Korb Eier auf den Markt und ein Pferd zertritt die Eier. Der Besitzer des Pferdes will den Schaden ersetzen. Die Frau sagt:

"Die genaue Zahl der Eier weiß ich nicht. Aber egal ob ich sie zu 2, 3, 4, 5 oder 6 abgezählt habe, immer ist eines übrig geblieben. Erst das Abzählen zu je 7 Stück ist aufgegangen."

Wie viele Eier waren mindestens im Korb?

Lösung 8: Diesmal ist $x-1$ durch 2, 3, 4, 5 und 6 teilbar, also durch $\mathrm{kgV}(2,3,4,5,6) = 60$. Somit ist x von der Form $x = 1 + 60\,\mathbb{Z}$. Zusammen mit $7 \mid x$ ergibt sich $x = \mathbf{301}$.

§3. Der kleine Satz von Fermat

Wer braucht hier Paartherapie?

Du oder ich?

(Sommerhaus der Stars)

Der erste erhaltene Beweis des kleinen Satzes von Fermat stammt von **Gottfried Wilhelm Leibniz** (1646-1716) aus dem Jahre 1683 (unveröffentlicht). Auch er wurde später von Euler unabhängig entdeckt und publiziert.

Satz (Freshman's Dream)

Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$. Dann gilt

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

Beweis: Nach dem binomischen Lehrsatz gilt

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{p-1} a\, b^{p-1} + b^p$$

Die Binomialkoeffizienten sind dabei wegen $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1\cdot 2\cdots i}$ für $i = 1, \ldots, p-1$ durch p teilbar, weil sich der Faktor p nicht wegkürzt. Betrachten wir die Gleichung nun modulo p, so folgt der Satz. □

Beweis des kleinen Satzes von Fermat: Zeige $a^p \equiv a \pmod{p}$ für $a \geq 1$ mit vollständiger Induktion nach a. Der Satz folgt dann für alle $a \in \mathbb{Z}$ mit $p \nmid a$, weil $a^p \pmod{p}$ nur von $a \pmod{p}$ abhängt.

Induktionsanfang: Für $a = 1$ gilt $1^p \equiv 1 \pmod{p}$.

Induktionsschritt: Nach der Induktionsvoraussetzung gilt $(a-1)^p \equiv a - 1 \pmod{p}$. Dann folgt

$$a^p \equiv ((a-1)+1)^p \equiv (a-1)^p + 1^p \equiv (a-1) + 1 \equiv a \pmod{p}.$$

Mersenne-Primzahlen

Im Jahr 1644 veröffentliche der Mönch **Marin Mersenne** eine Liste von Zahlen der Form $2^n - 1$, von denen er behautete, dass sie Primzahlen seien.

Aufgabe 9: (a) Beweise, dass für jede Primzahl der Form $2^n - 1$ der Exponent n eine Primzahl sein muss.

(b) Betrachte nun $2047 = 2^{11} - 1$. Zeige, dass 2047 eine Pseudoprimzahl zur Basis 2 ist.

(c) Zeige mittels iteriertem Quadrieren, dass $3^{88} \equiv 1 \pmod{2047}$ gilt. (Taschenrechner!)

(d) Zeige, dass 2047 keine Pseudoprimzahl zur Basis 3 ist. (Taschenrechner!)

Dass $2047 = 23 \cdot 89$ keine Primzahl ist, wusste Mersenne natürlich. Er behauptete aber auch, dass $2^{67} - 1$ eine Primzahl sei. Dies konnte **Edouard Lucas** 1876 mit einem Primzahltest widerlegen.

1903 gab **Frank Nelson Cole** einen Vortrag, in dem er vor großem Publikum das Produkt $193\,707\,721 \cdot 761\,838\,257\,287$ berechnete und $2^{67} - 1$ erhielt.

Lösung 9: (a) Gilt $n = k \cdot \ell$, so folgt

$$2^n - 1 = (2^k - 1)\left((2^k)^{\ell-1} + (2^k)^{\ell-2} + \cdots + 1\right).$$

(b) Es gilt $2^{11} \equiv 1 \pmod{2^{11} - 1}$. Wegen $11 \mid 2046$ zeigt dies $2^{2046} \equiv 1 \pmod{2047}$.

(c) Wegen $88 = 64+16+8$ berechnen wir $3^4 \equiv 81 \pmod{2047}$, $3^8 \equiv 420 \pmod{2047}$, $3^{16} \equiv 358 \pmod{2047}$, $3^{32} \equiv 1250 \pmod{2047}$, $3^{64} \equiv 639 \pmod{2047}$ und schließlich $639 \cdot 358 \cdot 420 \equiv 1 \pmod{2047}$.

(d) Wegen $2046 \equiv 22 \pmod{88}$ gilt $3^{2046} \equiv 3^{22} \pmod{2047}$.

Mit $22 = 16 + 4 + 2$ und den Werten aus (c) erhalten wir $3^{22} \equiv 358 \cdot 81 \cdot 9 \equiv 1013 \pmod{2047}$, also nicht den Rest 1.

Aufgabe 10: (a) Implementiere das iterierte Quadrieren in einem CAS oder Spreadsheet.

(b) Weise nach, dass $2^{67} - 1$ keine Pseudoprimzahl zur Basis 3 ist.

Lösung 10: (b) $3^{2^{67}} \equiv 122\,453\,792\,873\,589\,376\,894 \pmod{2^{67} - 1}$ und dies ist nicht die Restklasse von 9.

§4. Der Satz von Euler

„Was ist die Hälfte von 637 Kilogramm?“

„637 Pfund!“

Aufgabe 11: Seien $a, b \in \mathbb{N}_+$ teilerfremde Zahlen. Zeige, dass es $m, n \in \mathbb{N}_+$ gibt mit $a^m + b^n \equiv 1 \pmod{ab}$.

Lösung 11: Nach dem chinesischen Restsatz können wir die Äquivalenz separat modulo a und modulo b lösen.

Modulo a muss gelten $b^n \equiv 1 \pmod{a}$. Wir können also $n = \varphi(a)$ wählen.

Modulo b erhalten wir $a^m \equiv 1 \pmod{b}$ und können $m = \varphi(b)$ wählen.

Aufgabe 12: Bestimme die letzten beiden Ziffern von $2^{3^{2023}}$.

Lösung 12: Gesucht ist die Restklasse modulo 100. Wir wissen bereits $\varphi(100) = 40$. Man kann den Exponenten also immer um 40 vermindern, ohne die Restklasse zu ändern.

Somit brauchen wir zuerst $3^{2023} \pmod{40}$. Wegen $\varphi(40) = 16$ und wegen $2023 \equiv 7 \pmod{16}$ erhalten wir $3^{2023} \equiv 3^7 \equiv 3 \cdot 729 \equiv 27 \pmod{40}$.

Also gilt $2^{3^{2023}} \equiv 2^{27} \equiv 1024^2 \cdot 128 \equiv 24^2 \cdot 28 \equiv \mathbf{28} \pmod{100}$.

§5. Fortgeschrittene Resterechnung

Das Ergebnis habe ich schon.
Jetzt brauche ich nur noch den Weg,
der zu ihm führt.
(Carl Friedrich Gauß)

Aufgabe 13: Besitzt die Gleichung $x^2 + 9xy + y^2 = 600$ eine Lösung mit ganzzahligen x, y?

Lösung 13: Modulo 3 ergibt sich $x^2 + y^2 \equiv 0 \pmod 3$. Die Quadrate modulo 3 sind $\bar{0}$ und $\bar{1}$. Der einzige Weg, die Summe 0 zu erhalten, ist $3 \mid x$ und $3 \mid y$. Dann ist $x^2 + 9xy + y^2$ durch 9 teilbar, die Zahl 600 aber nicht. Also gibt es keine ganzzahligen Lösungen.

Aufgabe 14: Finde alle $x, y, n \in \mathbb{N}$ mit $x^2 + y^2 = 2^n + 3$.

Lösung 14: Falls $n \geq 2$, so folgt $x^2 + y^2 \equiv 3 \pmod 4$. Die Quadrate modulo 4 sind $\bar{0}$ und $\bar{1}$. Also gibt es in diesem Fall keine Lösungen.

Im Fall $n = 1$ gilt $x^2 + y^2 = 5$, also $(x, y) \in \{(1, 2), (2, 1)\}$.

Im Fall $n = 0$ gilt $x^2 + y^2 = 4$, also $(x, y) \in \{(0, 2), (2, 0)\}$.

Cowboys, Kühe und eine Mundharmonika

Aufgabe 15. *Zwei Cowboys treiben gemeinsame ihre x Kühe in die Stadt und verkaufen sie zu je x Dollar. Für den Erlös kaufen sie ungerade viele Schafe zu je 12 Dollar, wobei der Rest gerade noch für ein Lamm reicht. Demjenigen, der beim Teilen das Lamm erhält, schenkt der andere zum Ausgleich seine Mundharmonika.*

Was kostet die Mundharmonika?

Lösung 15. Sei $s = 2t + 1$ die Zahl der Schafe und ℓ der Preis des Lamms. Der Erlös ist dann $x^2 = 12s + \ell = 24t + 12 + \ell$.

Insbesondere ist $\ell \in \{1, 2, \ldots, 11\}$ eine ganze Zahl und es ergibt sich $12 + \ell \in \{13, 14, \ldots, 23\}$.

Nun betrachten wir $\bar{x}^2 \equiv \overline{12} + \bar{\ell} \pmod{24}$ und berechnen

$n \pmod{24}$	0	1	2	3	4	5	6	7	8	9	10	11
$n^2 \pmod{24}$	0	1	4	9	16	1	12	1	16	9	4	1

Hieraus folgt $12 + \ell = 16$, also $\ell = 4$.

Ist m der Preis der Mundharmonika, so gilt $12 - m = \ell + m = 4 + m$, woraus wir $m = 4$ erhalten.

Die Mundharmonika kostet also 4 Dollar.

Ein irrationaler Kreis

Aufgabe 16. Zeige, dass es auf dem Kreis mit Radius $\sqrt{3}$ um den Ursprung $(0,0)$ keine rationalen Punkte (a,b) mit $a,b \in \mathbb{Q}$ gibt.

Lösung 16. Angenommen, $(a,b) \in \mathbb{Q}^2$ wäre ein solcher Punkt. Schreibe $a = \frac{x}{z}$ und $b = \frac{y}{z}$ mit $x,y,z \in \mathbb{Z}$, wobei $z \neq 0$ gelte. Die Kreisgleichung liefert dann $x^2 + y^2 = 3z^2$, wobei wir annehmen können, dass x,y,z keinen gemeinsamen Teiler ≥ 2 haben.

Betrachten wir diese Gleichung modulo 3, so erhalten wir $\bar{x}^2 + \bar{y}^2 = \bar{0}$, was nach obigem Beispiel nur für $\bar{x} = \bar{y} = \bar{0}$ geht.

Also ist $x^2 + y^2 = 3\,z^2$ durch 9 teilbar, und folglich ist z durch 3 teilbar, im Widerspruch zu $\mathrm{ggT}(x,y,z) = 1$.

ENDE

Bisher konnte noch nicht bewiesen werden,
dass irgendetwas in der Mathematik schwierig ist.
(Norbert a'Campo)

Vielen Dank für Ihre Aufmerksamkeit!