Schüler-Propädeutikum Mathematik 2020
Vortrag 2: Modulorechnung

Andreas Lochmann

8. Oktober 2020

1 Division mit Rest

Mit $\mathbb{Z}$ bezeichnen wir die Menge aller ganzen Zahlen, also

$$\mathbb{Z} \;=\; \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

und mit $\mathbb{N}$ die Menge der natürlichen Zahlen; darunter wollen wir die positiven ganzen Zahlen verstehen, also $\mathbb{N} = \{1, 2, 3, \ldots\}$ ohne die Null.

1.1 Satz (Division mit Rest) *Es seien $n, m \in \mathbb{Z}$ mit $m > 0$. Dann gibt es genau eine Kombination $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ mit*

$$n = xm + y \;\; \textit{und} \;\; 0 \leq y < m\,, \;\; \textit{also} \;\; \frac{n}{m} = x + \frac{y}{m}\,.$$

y heißt Rest der Division von n durch m, und wir bezeichnen ihn mit $n \,\%\, m$.

Beweis Wir betrachten $f(x) = xm - n$ für verschiedene $x \in \mathbb{R}$. Wegen $m > 0$ ist $f(|n|) = |n| \cdot m - n > 0$ und $f(-|n|) = -|n|m - n < 0$. Außerdem ist f streng monoton wachsend, d.h. es gibt genau ein $x \in \mathbb{Z}$ mit $f(x-1) < 0$ und $f(x) \geq 0$. Wir setzen $y = f(x)$, dann ist also $y \in \mathbb{Z}$, $y \geq 0$ und $n = xm + y$, sowie $f(x-1) = (x-1)m - n = y - m < 0$, also $y < m$. Wenn es ein weiteres Paar $(x, y) \in \mathbb{Z}^2$ mit $n = xm + y$ gäbe, müsste es eine weitere Nullstelle von f geben, aber f ist, wie gesagt, streng monoton wachsend und kann daher nur eine Nullstelle besitzen. □

Der Beweis benutzt im Grunde etwas Analysis linearer Funktionen ohne das wirklich zu benötigen, aber es macht den Beweis etwas klarer. Für einen elementareren Beweis siehe Bundschuh, 2.2.

Man kann den Rest einer Division $a \,\%\, b$ durch schriftliche Division von Hand bestimmen; man kann ihn aber mit Hilfe eines normalen Vierspezies-Taschenrechners berechnen, z.B. wie folgt:

1. Dividiere a durch b.
2. Notiere den Ganzteil des Ergebnisses.
3. Ziehe den Ganzteil vom Ergebnis ab.
4. Multipliziere mit b, das Ergebnis ist der Rest der Division.

Beginnt man mit $a, b \in \mathbb{Z}$, so muss bei diesem Verfahren am Ende eine ganze Zahl übrig bleiben. Aufgrund numerischer Rundungsfehler kann es sein, dass der Taschenrechner ein geringfügig zu großes oder zu kleines Ergebnis ausspuckt; man muss dann zur nächsten ganzen Zahl runden.

1.2 Beispiel

$$\begin{aligned} 5397 : 19 &= 284,0526\ldots \\ \ldots - 284 &= \quad 0,0526\ldots \\ \ldots \cdot 19 &= \quad 0,999\ldots, \end{aligned}$$

also ist $5397 = 19 \cdot 284 + 1$ und $5397\%19 = 1$.

1.3 Satz *Es sei $n \in \mathbb{N}$. Von n aufeinander folgenden ganzen Zahlen ist stets genau eine durch n teilbar.*

Beweis Es sei a die größte der n Zahlen. Es sei $a = nx + y$ mit $x, y \in \mathbb{Z}$, $0 \leq y < n$. Dann ist $a - y$ durch n teilbar und wegen $0 \leq y < n$ eine der n Zahlen. Eindeutigkeit folgt aus der Eindeutigkeit der Division mit Rest. □

2 Kongruenzen

2.1 Definition Für ganze Zahlen $a, b \in \mathbb{Z}$ sagen wir: a **teilt** b (in Zeichen: $a \mid b$), wenn es ein $x \in \mathbb{Z}$ gibt mit $a \cdot x = b$. In dem Fall nennen wir a einen **Teiler** von b und b ein **Vielfaches** von a.

2.2 Beispiel Die Teiler von 21 sind: $1, 3, 7, 21, -1, -3, -7$ und -21.

2.3 Definition Es seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ beliebig. Wir sagen a und b sind zueinander *kongruent* modulo m, in Zeichen $a \equiv b \pmod{m}$ oder einfach $a \equiv b\ (m)$, wenn $m \mid a - b$ (also m ein Teiler von $a - b$ ist). Die Zahl m in einer Kongruenz wird *Modul* genannt.

Eine Zahl ist genau dann durch m teilbar, wenn sie kongruent Null modulo m ist, denn $a \equiv 0\ (m)$ gilt genau dann, wenn $m \mid a - 0$.

2.4 Lemma *Es seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ beliebig. Es gilt $a \equiv b\ (m)$ genau dann, wenn $a \,\%\, m = b \,\%\, m$ gilt.*

Beweis "⇒": Es sei $m \mid a - b$. Aufgrund der Division mit Rest gibt es Zahlen $k, l \in \mathbb{Z}$ mit $a = km + (a \,\%\, m)$ und $b = lm + (b \,\%\, m)$, also $a - b = (k - l)m + (a \,\%\, m) - (b \,\%\, m)$. Nach Voraussetzung ist $m \mid a - b$, also gibt es $n \in \mathbb{Z}$ mit $a - b = nm$, also

$$(n - k + l)m \;=\; (a \,\%\, m) - (b \,\%\, m)\,.$$

Außerdem wissen wir, dass $0 \leq a \,\%\, m < m$ und $0 \leq b \,\%\, m < m$ gelten, also $-m < (a \,\%\, m) - (b \,\%\, m) < m$. Nun muss aber $(a \,\%\, m) - (b \,\%\, m)$ durch m teilbar sein; das geht nur für $(a \,\%\, m) - (b \,\%\, m) = 0$.

"⇐": Es sei $a \,\%\, m = b \,\%\, m$. Dann gibt es Zahlen $k, l \in \mathbb{Z}$ mit $a = km + (a \,\%\, m)$ und $b = lm + (b \,\%\, m) = lm + (a \,\%\, m)$, also $a - b = (k - l)m$. Folglich ist $m \mid a - b$. □

2.5 Folgerung *Seien $a, b, c \in \mathbb{Z}$ und $m \in \mathbb{N}$.*
a) Stets ist $a \equiv a\ (m)$.
b) Ist $a \equiv b\ (m)$, so ist auch $b \equiv a\ (m)$.
c) Ist $a \equiv b\ (m)$ und $b \equiv c\ (m)$, so ist $a \equiv c\ (m)$.

In dieser Hinsicht verhält sich $\equiv$ also wie ein Gleichheitszeichen. Es *ist* zwar kein Gleichheitszeichen (denn beispielsweise ist ja $2 \equiv 7\ (5)$, obwohl $2 \neq 7$ ist), aber es zeigt ein ähnliches Verhalten und ähnliche Rechenregeln. So etwas nennt man auch eine **Äquivalenzrelation**.

2.6 Lemma *Es seien $m \in \mathbb{N}$ und $a, b, a', b' \in \mathbb{Z}$ beliebig. mit $a \equiv a'\ (m)$ und $b \equiv b'\ (m)$. Dann gelten auch $a + b \equiv a' + b'\ (m)$ und $ab \equiv a'b'\ (m)$.*

Beweis Es seien $k, l \in \mathbb{Z}$ mit $a = a' + km$ und $b = b' + lm$. Dann ist $a+b = a'+b'+(k+l)m$, also $a+b \equiv a'+b'\ (m)$, und $ab = a'b'+a'lm+b'km+lkm^2 = a'b' + m(a'l + b'k + lkm)$, also $ab \equiv a'b'\ (m)$. □

Sofern es also die Addition und Multiplikation betrifft, können Zahlen in einer Rechnung gegen kongruente Zahlen ersetzt werden. Beispielsweise ist

$$7 \cdot 5 \;=\; 35 \;\equiv\; 3\ (4)$$

, und da $7 \equiv 3$ ist, ist auch

$$3 \cdot 5 \;=\; 15 \;\equiv\; 3\ (4)\,.$$

2.7 Beispiel Wir wollen wissen, was der Rest von $123 \cdot 458$ bei Division durch 7 ist. Dazu berechnen wir zunächst $123 = 70 + 53 = 70 + 49 + 4$, also $123 \,\%\, 7 = 4$, sowie $458 = 420 + 38 = 420 + 35 + 3$, also $456 \,\%\, 7 = 3$. Damit ist $123 \equiv 4\ (7)$ und $456 \equiv 3\ (7)$, also $123 \cdot 456 \equiv 12\ (7)$. Es reicht daher aus, den Rest von 12 bei Division durch 7 zu berechnen, und das ist 5, also $(123 \cdot 458) \,\%\, 7 = 5$.

Vorsicht bei der Division! Es ist im allgemeinen nicht möglich, aus einer Kongruenz zu kürzen. Beispielsweise ist $2 \cdot 8 \equiv 2 \cdot 3\ (10)$, aber $8 \not\equiv 3\ (10)$. Auch in einem Nenner modulo zu rechnen ist gefährlich, solange Nenner und Modul nicht teilerfremd sind:

$$2 \;=\; \frac{4}{2} \;\not\equiv\; \frac{4}{-4} \;=\; -1 \pmod 6 .$$

Auch **Wurzelziehen** ist im allgemeinen nicht möglich. Es gilt zwar $16 \equiv 25\ (9)$, aber $4 \not\equiv 5\ (9)$.

Potenzieren mit einer festen, natürlich-zahligen Potenz ist letztlich nur mehrfache Multiplikation und daher kann die Basis einer Potenz gegen eine kongruente Zahl ersetzt werden, Beispiel:

$$7^3 \;=\; 343 \;\equiv\; 3\,(4)\,, \text{ ebenso ist } 3^3 \;=\; 27 \;\equiv\; 3\,(4)\,.$$

Frage: Kann auch der Exponent in einer Potenz gegen eine kongruente Zahl ersetzt werden? Prüfen Sie ein paar Beispiele.

2.8 Beispiel Für $x \in \mathbb{Z}$ ist x^2+2 nie durch 5 teilbar. Stellt man eine Liste von $(x^2+2)\,\%\,5$ auf, so stellt man fest, dass nur die Reste 1,2 und 3 möglich sind, folglich ist $5 \nmid x^2+2$.

Knobelaufgabe: Es sei p eine Primzahl mit $p \equiv 2 \pmod 7$. Zeigen Sie: $\frac{p+12}{7}$ ist ganzzahlig und nicht durch 3 teilbar.

Knobelaufgabe: Es sei n eine ungerade Zahl. Zeigen Sie, dass dann $2n+5$ keine Quadratzahl sein kann.

3 Der kleine Fermat und der Satz von Wilson

Hier ist ein Beispiel für eine Multiplikationstabelle modulo 5:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Relevant sind dabei nur die Reste 1, 2, 3 und 4, da Multiplikation mit 0 immer 0 ergibt, auch wenn man Modulo rechnet. Interessanterweise taucht in jeder Zeile jede Zahl genau einmal auf.

Aufgabe: Schreiben Sie die Multiplikationstabellen modulo 6, modulo 7 und modulo 8 auf, und vergleichen Sie: Wann taucht in einer Zeile jede Zahl genau einmal auf?

3.1 Lemma *Sei $m > 1$ eine natürliche Zahl und $a \in \{1, \ldots, m-1\}$. Wenn man die Zahlen $1, \ldots, m-1$ nacheinander mit a multipliziert und $\%m$ rechnet, taucht jede dieser Zahlen genau einmal als Ergebnis auf,* **falls** *a und m teilerfremd sind. Wenn sie nicht teilerfremd sind, fehlt mindestens die 1.*

Beweis **Fall 1:** a und m sind teilerfremd. Angenommen, eine Zahl würde bei der Multiplikation mit a zweimal als Ergebnis erscheinen. Dann müsste es also $x, y \in \{1, \ldots, m-1\}$ geben mit $ax \equiv ay \ (m)$. Gemäß den Rechenregeln für Modulo folgt daraus $a(x-y) \equiv 0 \ (m)$, also $m \mid a(x-y)$. Da a und m teilerfremd sind, muss m ein Teiler von $x-y$ sein. Da x und y aber kleiner als $m-1$ sind, ist $-m < x-y < m$ und die einzige Zahl in diesem Bereich, die durch m teilbar ist, ist 0, also $x-y = 0$ und folglich $x = y$. Es kann also nicht sein, dass eine Zahl in einer Zeile doppelt auftritt, und folglich taucht jede Zahl genau einmal auf.

Fall 2: a und m sind nicht teilerfremd. Sei g der größte gemeinsame Teiler von a und m. Angenommen, es gibt ein $x \in \{1, \ldots, m-1\}$ mit $ax \equiv 1 \ (m)$. Dann gibt es nach Definition der Kongruenz ein $y \in \mathbb{Z}$ mit $ax = 1 + ym$. Nun ist $g \mid a$, das heißt die linke Seite wird von g geteilt. Andererseits ist $g \mid m$, d.h. ym ist durch g teilbar, und $ym+1$ folglich nicht durch g teilbar – Widerspruch. □

3.2 Lemma *Sind $a, b, c \in \mathbb{Z}$ und $m \in \mathbb{N}$, $m > 1$, so dass m und a teilerfremd sind. Wenn $a \cdot b \equiv a \cdot c \ (m)$ gilt, so ist auch $b \equiv c \ (m)$, d.h. man darf eine Zahl kürzen, wenn sie zum Modul teilerfremd ist.*

Knobelaufgabe: Wie kann man dieses Lemma beweisen?

3.3 Satz (Kleiner Fermatscher Satz) *Wenn p eine Primzahl und $a \in \mathbb{N}$ ist, so ist $a^p \equiv a \ (p)$. Wenn p darüber hinaus kein Teiler von a ist, gilt sogar $a^{p-1} \equiv 1 \ (p)$.*

Beweis Ist p ein Teiler von a, so ist $a \equiv 0 \ (p)$ und $a^p \equiv 0 \ (p)$, also $a^p \equiv a \ (p)$ – die Behauptung ist in diesem Fall also trivial. Betrachten wir daher den Fall $p \nmid a$.

Sei dafür $t = (p-1)!$, also $t = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$. Nun betrachten wir

$$s \ := \ (a \cdot 1) \cdot (a \cdot 2) \cdot \cdots \cdot (a \cdot (p-1)) \, .$$

Offenbar können wir s auch als $a^{p-1} \cdot t$ schreiben. Wenn wir aber modulo p rechnen, gehen wir bei $a \cdot 1$, $a \cdot 2$ etc. wiederum alle Elemente von 1 bis $p-1$ durch (denn diese Zahlen sind allesamt teilerfremd zu p) und folglich ist $s \equiv t \ (p)$. Damit folgt $a^{p-1} \cdot t \equiv t \ (p)$, und da t und p teilerfremd sind, dürfen wir t kürzen und finden $a^{p-1} \equiv 1 \ (p)$. Durch Multiplikation mit a auf beiden Seiten folgt auch $a^p \equiv a \ (p)$. □

Aufgabe: Prüfen Sie den Satz, indem Sie folgende Äquivalenzen prüfen:

$$2^6 \stackrel{?}{\equiv} 2 \quad (6) \qquad 2^7 \stackrel{?}{\equiv} 2 \quad (7) \qquad 2^8 \stackrel{?}{\equiv} 2 \quad (8)$$
$$3^6 \stackrel{?}{\equiv} 3 \quad (6) \qquad 3^7 \stackrel{?}{\equiv} 3 \quad (7) \qquad 3^8 \stackrel{?}{\equiv} 3 \quad (8)$$
$$4^6 \stackrel{?}{\equiv} 4 \quad (6) \qquad 4^7 \stackrel{?}{\equiv} 4 \quad (7) \qquad 4^8 \stackrel{?}{\equiv} 4 \quad (8)$$

Das sieht erstmal nach einem vielversprechenden Verfahren aus, um Primzahlen zu testen, jedoch gibt es einige Zahlen n, die keine Primzahlen sind und trotzdem $a^{n-1} \equiv 1\ (n)$ (und dann natürlich auch $a^n \equiv a\ (n)$) erfüllen. Solche Zahlen heißen **Carmichael-Zahlen**, die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$. Seit 1994 weiß man, dass es unendlich viele Carmichael-Zahlen gibt, sie scheinen aber relativ selten. Jedoch kennen wir bis heute nicht die genaue Asymptotik der Carmichael-Zähl-Funktion, so dass es auch sein könnte, dass es im Bereich sehr, sehr großer Zahlen letztlich mehr Carmichael-Zahlen als Primzahlen gibt – wir wissen es nicht.

Wenn man den kleinen Fermatschen Satz als Primzahltest nutzen will, müsste man darüber hinaus sehr viele Potenzen berechnen – jede einzelne Potenz kann zwar relativ schnell von Computern berechnet werden, jedoch müssten wir zum Testen einer 100-stelligen Primzahl etwa 10^{100} solche Potenzen berechnen; das liegt außerhalb der Fähigkeiten selbst moderner Computer.

3.4 Satz (Satz von Wilson) *Sei p eine natürliche Zahl. Dann ist p genau dann eine Primzahl, wenn*

$$(p-1)! \ \equiv \ -1 \ \ (mod\ p)$$

gilt. (Alternativ kann man auch $(p-1)! \equiv p-1$ schreiben, denn $-1 \equiv p-1$ modulo p.)

Beweis Angenommen, p ist keine Primzahl. Dann werden die Primteiler von p allesamt in den Zahlen 1 bis $p-1$ auftauchen, das Produkt $(p-1)!$ enthält also p als Teiler und damit ist es Null modulo p, und nicht -1.

Nehmen wir jetzt an, p ist eine Primzahl. In jeder Zeile der Multiplikationstabelle modulo p steht genau eine Eins. Wenn wir die entsprechenden Paare von Zahlen zusammenfassen, erscheint im Produkt $(p-1)!$ modulo p für jedes dieser Paare eine 1. Die einzige Ausnahme sind solche Zahlen x, die modulo p ihr eigenes Inverses sind, also Zahlen x mit $x \cdot x \equiv 1\ (p)$. Da diese ihre eigenen Partner sind, tauchen Sie im Produkt $(p-1)!$ nur einmal auf. Aber aus $x^2 \equiv 1$ folgt $x^2 - 1 \equiv 0$, also $p \mid (x-1)(x+1)$. Da p eine Primzahl ist, ist dies nur möglich, wenn $p \mid x-1$ oder $p \mid x+1$ ist, unter den Zahlen $x \in \{1, \ldots, p-1\}$ trifft dies nur auf $x = 1$ und $x = p-1$ zu. Also ist

$$(p-1)! \ \equiv \ 1 \cdot (p-1) \ \equiv \ -1 \ \ (p)\,.$$

□

Der Satz von Wilson ist im Prinzip ein geeigneter Primzahltest: Man multipliziere alle Zahlen von 1 bis $p-1$ miteinander, rechne modulo p und prüfe, ob das Ergebnis -1 ist. Wenn ja, handelt es sich in jedem Fall um eine Primzahl, wenn nein, ist es definitiv keine Primzahl.