Thema: Wozu Rechnen mit Resten?

1. Teilbarkeitsfragen

Nach Definition ist b ein Teiler von a genau dann, wenn $a \equiv 0(\mod b)$.

Diese Sichtweise kann insbesondere dann nützlich sein, wenn keine Primfaktorzerlegungen zur Verfügung stehen. So ist zum Beispiel in Aufgabe 4.2 eine Primfaktorzerlegung von $10^n + 1$ für beliebige zweistellige Zahlen n nicht leicht herzustellen, während die Gleichung

$$10^n + 1 \equiv 0(\mod 101)$$

wegen der Periodizität von $10^n \mod 101$ im Exponenten n ($10^{n+4} \equiv 10^n(\mod 101)$) einfach gelöst werden kann.

Als weitere Anwendung dieser Sichtweise wollen wir Teilbarkeitsregeln betrachten und als Beispiel ein Kriterium für die Teilbarkeit durch 11 herleiten. Beginnen wir mit einem Zahlenbeispiel:

$$340927648 = 3 \cdot 10^8 + 4 \cdot 10^7 \cdot 0 \cdot 10^6 + 9 \cdot 10^5 + 2 \cdot 10^4 + 7 \cdot 10^3 + 6 \cdot 10^2 + 4 \cdot 10^1 + 8$$

Wegen $10 \equiv -1(\mod 11)$ gilt $10^n \equiv (-1)^n(\mod 11)$. Somit ist $10^n \equiv 1(\mod 11)$, falls n gerade und $10^n \equiv -1(\mod 11)$, falls n ungerade.

Wir folgern

$$340927648 \equiv 3 - 4 + 0 - 9 + 2 - 7 + 6 - 4 + 8 = 19 - 24 \equiv 6(\mod 11).$$

Die Zahl ist also nicht durch 11 teilbar. Allgemein gilt:

Eine Zahl ist durch 11 *genau dann teilbar, wenn ihre alternierende Quersumme durch* 11 *teilbar ist. Die alternierende Quersumme einer Zahl erhält man durch Addition der Ziffern der Dezimaldarstellung, wobei bei jeder zweiten Ziffer das Vorzeichen gewechselt wird.*

In ähnlicher Weise lassen sich die bekannten Teilbarkeitsregeln für $2, 3, 4, 5, 8$ und 9 herleiten.

2. Ganzzahlige Lösungen von Gleichungen

Sucht man nur ganzzahlige Lösungen einer Gleichung, so kann es hilfreich sein, die Gleichung modulo einer geeignet gewählten Zahl zu betrachten. Es gibt kein allgemeines Rezept, modulo welcher Zahl gerechnet werden soll und man sollte sich nicht scheuen zu experimentieren.

In Aufgabe 3.3 haben wir die Gleichung $13x - 5y = 122$ modulo 5 betrachtet, da auf diese Weise eine Gleichung in nur einer Variablen entstand, nämlich $3x \equiv 2(\mod 5)$. Dadurch haben wir herausgefunden, dass $x \equiv 4(\mod 5)$ gelten muss.

In Aufgabe 4.3 konnten wir sogar durch Rechnung modulo 4 nachweisen, dass die Gleichung $a^2 + b^2 = d^2$ keine ganzzahligen Lösungen besitzt, wenn zusätzlich gefordert wird, dass a und b beide ungerade sind.

3. Kryptographie
Betrachtet man für natürliche Zahlen a und b die Folge der Reste

$$a \mod b, \quad a^2 \mod b, \quad a^3 \mod b, \quad a^4 \mod b, \quad \ldots \quad ,$$

so stellt man stets fest, dass sich ein periodisches Muster einstellt. Zum Beispiel erhalten wir für $a = 10, b = 7$ die Folge der Reste

$$3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, 1, 3, \ldots$$

Ein anderes Beispiel zeigt, dass sich das periodische Muster auch erst später einstellen kann (gemischt periodischer Fall). Für $a = 2, b = 24$ ergibt sich

$$2, 4, 8, 16, 8, 16, 8, 16, \ldots$$

Der Beweis der Periodizität ist einfach und ganz analog zu dem Beweis, dass die Dezimaldarstellung einer Bruchzahl immer periodisch oder gemischt periodisch ist. Beide Beweise beruhen darauf, dass es nur endlich viele Reste gibt und somit irgendwann irgendein Rest ein zweites Mal in der Folge von Resten auftauchen muss. Von diesem Punkt an wiederholen sich die Reste periodisch. Die eben diskutierte Periodizität der Reste hat im Computerzeitalter eine große Bedeutung erlangt. Sie ist die Grundlage des RSA-Verfahrens der public key Verschlüsselung.

Was man sich merken sollte!

1. **Beim Rechnen mit Resten dürfen bei Addition, Multiplikation und Subtraktion (nicht bei Division!) die Zahlen durch andere Zahlen, die den gleichen Rest besitzen, ersetzt werden. Auf diese Weise kann man sehr effizient rechnen.**

2. **Das Rechnen mit Resten kann nützlich sein, um**

   - **Teilbarkeitsfragen zu klären, wenn keine Primfaktorenzerlegungen zur Verfügung stehen,**
   - **Informationen über ganzzahlige Lösungen von Gleichungen zu erhalten.**