Beschleunigung durch Abstraktion, Leonardo-Sommerschule 2013

1. Sätze über die letzte Ziffer oder den Rest beim Teilen durch 10

Satz. Die letzte Ziffer einer natürlichen Zahl a ist der eindeutige Rest $0 \leq r \leq 9$ bei Division mit Rest durch 10, d. h. $a = 10 \cdot q + r$ mit einer natürlichen Zahl q (dem Ganzzahlquotienten).

Satz. Für jede ganze Zahl m haben a und $a + 10 \cdot m$ dieselbe letzte Ziffer.

Satz. Die letzte Ziffer der Summe natürlicher Zahlen ist die letzte Ziffer der Summe der letzten Ziffern. Genauer: Seien a, b natürliche Zahlen mit letzter Ziffer r bzw. s, d.h.

$$a = 10 \cdot q + r \text{ und } b = 10 \cdot t + s,$$

wobei $0 \leq r \leq 9$ und $0 \leq s \leq 9$. Die letzte Ziffer von $a + b$ ist dann die von $r + s$.
Beweis. $a + b = 10 \cdot (q + t) + (r + s)$. Daher haben $a + b$ und $r + s$ dieselbe letzte Ziffer.

Satz. Die letzte Ziffer des Produktes natürlicher Zahlen ist die letzte Ziffer des Produkts der letzten Ziffern. Genauer: Die letzte Ziffer von $a \cdot b$ ist die letzte Ziffer von $r \cdot s$.
Beweis. $a \cdot b = (10 \cdot q + r) \cdot (10 \cdot t + s) = 10 \cdot (10 \cdot q \cdot t + q \cdot s + r \cdot t) + r \cdot s$. Daher haben $a \cdot b$ und $r \cdot s$ dieselbe letzte Ziffer.

Potenzieren ist nur mehrfaches Hintereinanderausführen von Multiplikationen. Also:
Satz. Die letzte Ziffer von a^m ist die letzte Ziffer von r^m für jede natürliche Zahl m.

Die Tabelle auf der Rückseite zeigt folgenden Satz.

Somit können wir eine Anleitung für die ‘Rechenmagie’ geben:

Die letzte Ziffer der Potenzen von a. Was erkennt man?

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	
0	0	0	0	0	0	0	0	0	
1	1	1	1	1	1	1	1	1	
2	4	8	6	2	4	8	6	2	
3	9								
4									
5									
6									
7									
8									
9	1	9	1	9	1	9	1	9	

1. Abstraktion

Definition. Haben a und b denselben Rest bei Division durch n, so schreiben wir

$$a \equiv b \mod n.$$

Es gelten dieselben Regeln wir für das Rechnen mit $n = 10$:
Satz. Falls $a \equiv r \mod n$ und $b \equiv s \mod n$, dann gelten:

$$a + b \equiv r + s \mod n,$$

$$a \cdot b \equiv r \cdot s \mod n,$$

$$a^m \equiv r^m \mod n.$$

Beweis. Man ersetze 10 durch n in den früheren Beweisen.

Satz (Kleiner Satz von Fermat). Sei p eine Primzahl. Weiter sei m eine natürliche Zahl mit der Eigenschaft $m \equiv 1 \mod p - 1$. Dann gilt für jede natürliche Zahl a

$$a^m \equiv a \mod p.$$

Beweis. Dieser Satz wird in den Algebra-Vorlesungen im Rahmen der Gruppentheorie bewiesen.

1. Anwendung: Ganz viele neue Rechentricks

Finde neue Rechentricks!
Weiß man zum Beispiel, dass

$$21^5 \equiv 1 \mod 100$$

gilt, so kann man ganz einfach die letzten zwei Ziffern von a^n berechnen, wenn die letzten beiden Ziffern von a gleich 21 sind. Als allereinfachste Anwendung sind die letzten beiden Ziffern von a^n gleich 01, wenn n durch 5 teilbar ist (d.h. wenn die letzte Ziffer von n gleich 0 oder 5 ist).

Die abstrakte Erkenntnis der zugrunde liegenden Regeln *beschleunigt* das Finden ähnlicher Regeln also enorm.

2. Anwendung: Verschlüsselung im Internet – ein Kryptographie-Verfahren

Problem: Alice will eine geheime Nachricht an Bob schicken. Alice und Bob wollen nicht, dass jemand anderes die Nachricht kennt, auch wenn der/die andere die gesamte Kommunikation zwischen Alice und Bob abhört. Der Einfachheit halber nehmen wir an, dass die Nachricht eine positive natürliche Zahl N ist. Für den Computer sind Buchstaben und Sätze ohnehin nur Zahlen.

Unser Kryptographie-Verfahren (ähnliche werden im Internet angewandt!!) funktioniert so:

• A und B einigen sich auf eine große Primzahl p, z.B. 17976931348623159077293051907890247336179769789423065727343008115773267580550096313270847732240753602112011387987139335765878976881441662249284743063947412437776789342486548527630221960124609411945308295208500576883815068234246288147391311054082723716335051068458629823994724593847971630483535632962422413785 9

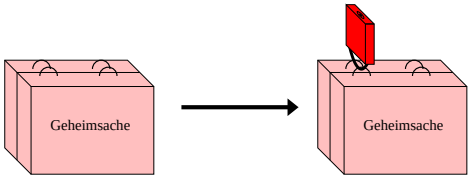
Jeder darf diese Primzahl kennen; sie ist kein Geheimnis.

Der Einfachheit nehmen wir an, dass $0 < N < p$ gilt (ansonsten führen wir das Verfahren mehrfach durch).

• Alice wählt geheim eine natürliche Zahl $0 \leq a < p-1$ und berechnet c, so dass $ac \equiv 1 \mod p-1$ gilt.

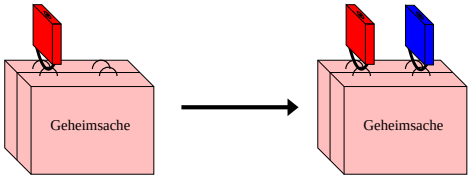
• Bob wählt geheim eine natürliche Zahl $0 \leq b < p-1$ und berechnet d, so dass $bd \equiv 1 \mod p-1$ gilt.

• Alice: Abschließen mit rotem Schloss



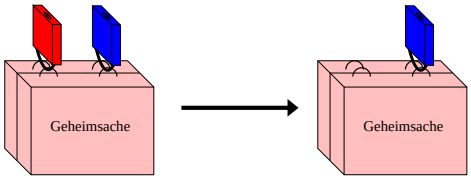
Berechne A, so dass $N^a \equiv A \mod p$.
Schicke A an Bob.

• Bob: Abschließen mit blauem Schloss



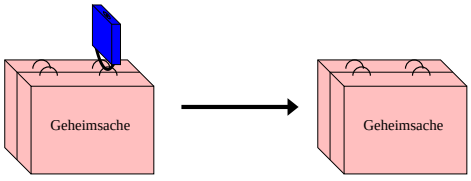
Berechne B, so dass $A^b \equiv B \mod p$.
Schicke B an Alice.

• Alice: Entfernen des roten Schlosses



Berechne C, so dass $B^c \equiv C \mod p$.
Schicke C an Bob.
Merke nach unseren Regeln:
$C \equiv B^c \equiv A^{bc} \equiv N^{abc} \equiv (N^b)^{ac} \equiv N^b \mod p$.

• Bob: Entfernen des blauen Schlosses



Berechne D, so dass $C^d \equiv D \mod p$.
Merke nach unseren Regeln:
$D \equiv C^d \equiv (N^b)^d \equiv N^{bd} \equiv N \mod p$.
Das Verfahren funktioniert! Denn dies ist die ursprüngliche Nachricht.

• Merke: N wurde nie selbst verschickt!

Nach heutigem Kenntnisstand ist es praktisch unmöglich, aus der Kenntnis von A, B und C auf die Nachricht N zu schließen.

2. Abstraktion: Gruppen, Ringe und Körper

Die Menge der Reste bei Division durch n bildet einen sogenannten **Ring**, das ist grob gesprochen eine Menge zusammen mit einer Addition und einer Multiplikation, so dass das Assoziativ-, das Kommutativ- und das Distributivgesetz gelten. Ist n eine Primzahl, so hat man sogar einen sogenannten **Körper**.

Beispiele von Ringen sind

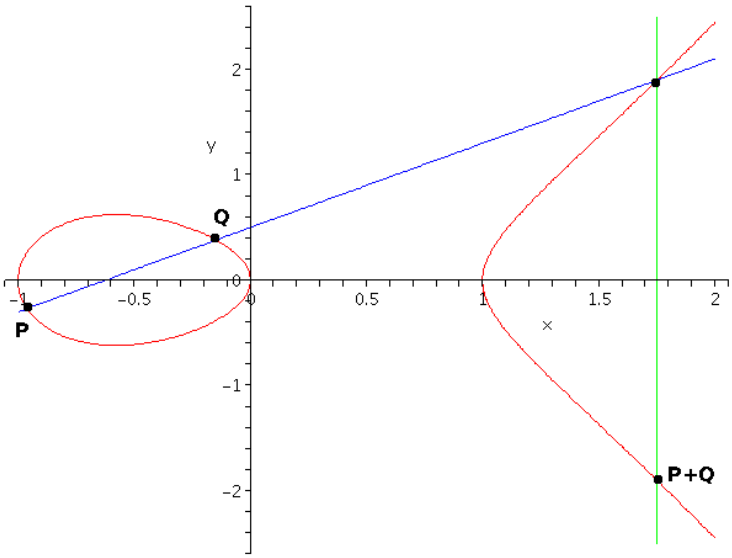
- die ganzen Zahlen,
- die rationalen Zahlen (Bruchzahlen),
- die reellen Zahlen.

Die letzteren beiden sind auch Körper.

Eine einfachere Struktur ist diejenige einer **Gruppe**, das ist eine Menge zusammen mit einer Multiplikation, so dass das Assoziativgesetz gilt und jedes Element ein Inverses hat.

Beispiele von Gruppen sind

- die positiven reellen Zahlen,
- die Reste ungleich null bei Division durch eine Primzahl,
- Symmetrien von Figuren (z.B. Polygonen) oder in der Chemie von Kristallen,
- in der Geometrie bestimmte Kurven, sogenannte elliptische Kurven.



Diese Objekte (und viele andere mehr!) werden in Mathematik-Vorlesungen an der Uni studiert. Sätze werden in möglichst großer Allgemeinheit bewiesen (im Beispiel der Reste bei Division würde der allgemeine Fall n behandelt), so dass sie auf möglichst viele Beispiele und in möglichst vielen Gebieten angewandt werden können.

Das Erkennen gemeinsamer zu Grunde liegender Strukturen und deren abstrakte Behandlung ist ein Grundprinzip der Mathematik.

Es beschleunigt den Erkenntnisgewinn!

Einige Resultate und einige Anwendungen der Mathematik

- Elliptische Kurven werden unter Verwendung der Division mit Rest durch eine große Primzahl seit einigen Jahren in der Kryptographie eingesetzt. Zum Beispiel enthält der Chip des deutschen Reisepasses und des deutschen Personalausweises die Rechengesetze einer elliptischen Kurve!

- Elliptische Kurven geben auch Erkenntnisse über Symmetrien von algebraischen Zahlen. Dies wird entscheidend benutzt im Beweis des sogenannten Großen Satzes von Fermat, der vor 20 Jahren nach über 350 Jahren Suche endlich bewiesen worden ist!

  Er besagt, dass es keine positiven ganzen Zahlen a, b, c und $n \geq 3$ gibt, so dass

$$a^n + b^n = c^n.$$

  Für $n = 2$ hat man aber die sogenannten Pythagoräischen Tripel (nach dem Satz von Pythagoras), z. B. $3^2 + 4^2 = 5^2$.

- Der große Satz von Fermat kann nur mit Hilfe von Mathematik bewiesen werden, die über das hinaus geht, was an der Uni im Bachelor und Master gelehrt wird.

  Symmetrien von Zahlen werden aber in den Algebra-Vorlesungen im Rahmen der sogenannten Galois-Theorie studiert.

Evariste Galois 1811 – 1832 (in einem Duell gestorben)

  Jeder kennt die Formel zur Lösung quadratischer Gleichungen $x^2+bx+c = 0$, nämlich

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

  Es gibt auch noch solche Formeln zum Lösen von Gleichungen dritten und vierten Grades, d. h. $x^3 + bx^2 + cx + d = 0$ bzw. $x^4 + bx^3 + cx^2 + dx + e = 0$.

  In der Algebra-Vorlesung wird mit Hilfe der Symmetrien von Zahlen bewiesen, dass es keine solche Lösungsformeln mit Wurzelausdrücken gibt für Gleichungen fünften oder höheren Grades!

  Es wird ebenfalls bewiesen, dass die Quadratur des Kreises unmöglich ist.

(Handout von Gabor Wiese, 5. Juli 2013)