Mathematik I

Vorlesung 7 - Komplexe Zahlen und endliche Körper

Prof. Dr. Sandra Eisenreich

13. November 2023

Hochschule Landshut

7.1 Komplexe Zahlen

Motivation komplexe Zahlen

Die reellen Zahlen sind der größte Zahlenraum, in dem wir uns bisher bewegt haben. Aber leider reicht dieser noch nicht.

Führen wir uns vor Augen, wie sich unser Zahlenraum immer mehr erweitert hat:

- $\mathbb{N}$: 4 Äpfel, drei Brötchen... Problem: wenn man einen Apfel schuldet, hat man plötzlich eine Zahl -1, die nicht in $\mathbb{N}$ enthalten ist.
- $\mathbb{Z}$: Erweiterung von $\mathbb{N}$ durch negative Zahlen. Problem: Wenn man einen Apfel halbiert, hat man plötzlich eine Zahl, die nicht mehr in $\mathbb{Z}$ liegt.
- $\mathbb{Q}$: So kommt man zu den Brüchen. Problem: Wenn man sich einen Kreis anschaut, kommt man auf die irrationale Zahl π, diese ist nicht in $\mathbb{Q}$.
- $\mathbb{R}$: Erweiterung von $\mathbb{Q}$ durch irrationale Zahlen reellen Zahlen. Problem: die Gleichung $x^2 = -1$ hat eine theoretische Lösung, wir nennen sie i, die aber nicht in den reellen Zahlen liegt. Es muss also nochmal eine größere Menge geben.
- $\mathbb{C}$: Erweiterung von $\mathbb{R}$ um i. Das sind die **komplexen Zahlen**.

Anwendungen in der Informatik: z.B. 3D-Game-Engines.

Ziel: Konstruiere eine Menge $\mathbb{C}$, die $\mathbb{R}$ enthält und eine Lösung der Gleichung $x^2 = -1$.

Definition

Wir definieren die Menge

$$\mathbb{C} := \{(x, y) \in \mathbb{R}^2 | x, y \in \mathbb{R}\} = \mathbb{R}^2$$

und fassen die reellen Zahlen $\mathbb{R}$ als die Teilmenge $\mathbb{R} = \{(x, 0) \in \mathbb{R}^2 | x \in \mathbb{R}\}$ auf.
Wir führen nun eine Addition und eine Multiplikation auf $\mathbb{C}$ ein:

- Addition: $(x, y) + (x', y') := (x + x', y + y')$
  (z.B. $(1, 2) + (-1, 3) = (0, 5)$)
- Multiplikation: $(x, y) \cdot (x', y') := (x \cdot x' - y \cdot y', x \cdot y' + y \cdot x')$
  (z.B. $(1, 2) \cdot (-1, 3) = (1 \cdot (-1) - 2 \cdot 3, 1 \cdot 3 + 2 \cdot (-1) = (-7, 1)$)

Satz

$(\mathbb{C}, +, \cdot)$ *ist ein Körper, der sogenannte Körper der* **komplexen Zahlen.**

Beweis.

- Neutrales Element der Addition =(0,0)
- Neutrales Element der Multiplikation = (1,0), da:

$$(x,y)\cdot(1,0) = (x\cdot 1 - y\cdot 0, x\cdot 0 + y\cdot 1) = (x,y)$$

- Assoziativität, Kommutativität, und Distributivgesetz rechnet man nach.
- Multiplikatives Inverses: Behauptung

$$(x,y)^{-1} = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$$

Rechnung:

$$\begin{aligned}(x,y)\cdot\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right) &= \left(\frac{x^2}{x^2+y^2} + \frac{y^2}{x^2+y^2}, \frac{-xy}{x^2+y^2} + \frac{xy}{x^2+y^2}\right)\\ &= (1,0)\\ &= \text{Einselement bezgl. Multiplikation}\end{aligned}$$

$\Rightarrow$ Beh.

■

Satz

Fasst man $\mathbb{R}$ als die Teilmenge $\{(x,0)|x \in \mathbb{R}\}$ von $\mathbb{C}$ auf, so ist $\mathbb{R}$ auf natürliche Weise eine Teilmenge von $\mathbb{C}$. Schreibt man $i = (0,1)$, so gilt: $(x,y) = x + i \cdot y$ und $i^2 = -1$.

Beweis. Es gilt

$$(x,0) + (x',0) = (x + x', 0)$$
$$(x,0) \cdot (x',0) = (x \cdot x' - 0 \cdot 0, x \cdot 0 + 0 \cdot x') = (x \cdot x', 0)$$

Somit entsprechen die Ergebnisse der Addition bzw. Multiplikation auf $\{(x,0)|x \in \mathbb{R}\}$ genau den Ergebnissen der Operationen auf den reellen Zahlen, d.h.

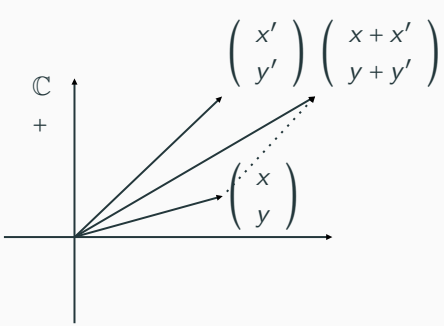
$$\psi : \mathbb{R} \to \mathbb{C}, x \mapsto (x,0)$$

ist ein Ringhomomorphismus.

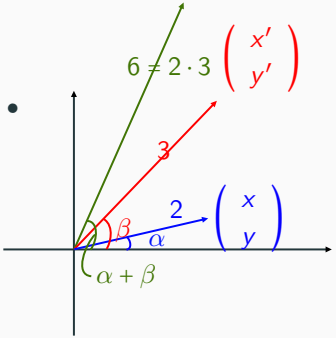
Außerdem ist $i^2 = (0,1) \cdot (0,1) = (0^2 - 1^2, 0 \cdot 1 + 1 \cdot 0) = (-1,0) = -(1,0)$ ■

Geometrie der Addition und Multiplikation

Addition von komplexen Zahlen:

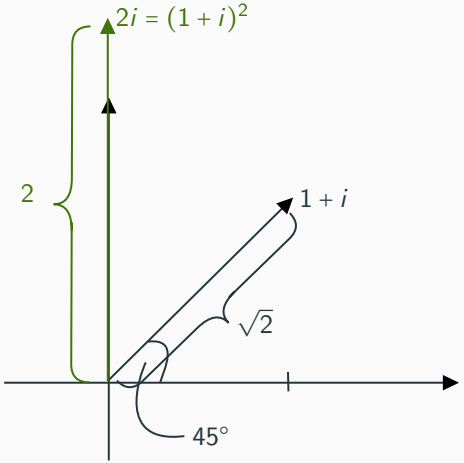


Multiplikation von kompl. Zahlen:



Merke: Beim Multiplizieren werden Längen multipliziert und Winkel zur x-Achse addiert.

Beispiel:



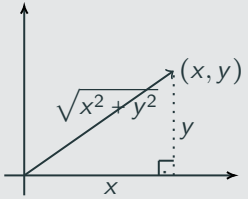
$$\begin{aligned}(1+i)^2 &= 1 + i^2 + 2i \\ &= 0 + 2i\end{aligned}$$

Rechnen mit komplexen Zahlen

Definition

Sei $z = x + iy \in \mathbb{C}$ eine komplexe Zahl. Dann definieren wir

$Re(z) := x$	(**Realteil** von z)
$Im(z) := y$	(**Imaginärteil** von z)
$\overline{z} := x - iy$	(**konjugiert Komplexe** zu z)
$\lvert z\rvert := \sqrt{x^2 + y^2}$	(**Betrag** von z)



Satz

Für $z = x + iy$ gilt:

$$\begin{aligned} z \cdot \overline{z} &= |z|^2 \\ z + \overline{z} &= 2 \cdot Re(z) \\ z - \overline{z} &= 2i \cdot Im(z) \end{aligned}$$

Beweis.

$$\begin{aligned} z \cdot \overline{z} &= (x + iy)(x - iy) = x^2 - i^2 \cdot y^2 + ixy - ixy = x^2 + y^2 = |z|^2 \\ z + \overline{z} &= x + iy + x - iy = 2x = 2 \cdot Re(z) \\ z - \overline{z} &= x + iy - (x - iy) = 2iy = 2i \cdot Im(z) \end{aligned}$$

■

Brüche von komplexen Zahlen

Die Gleichung $z \cdot \overline{z} = |z|^2$ kann man dazu verwenden, um einen Bruch $\frac{z}{z'} = \frac{x+iy}{x'+iy'}$ wieder in eine komplexe Zahl der Form $a + bi$ umzuformen:

Rechenregel

Um $\frac{z}{z'}$ in die Form $a + bi$ zu bringen, gehe wie folgt vor:

- erweitere den Bruch mit z':

$$\frac{z}{z'} = \frac{z \cdot \overline{z'}}{z' \cdot \overline{z'}} = \frac{z \cdot \overline{z'}}{|z'|^2}$$

  Dadurch wird der Nenner eine reelle Zahl.

- multipliziere den Zähler aus:

$$\frac{z \cdot \overline{z'}}{|z'|^2} = \frac{(x+iy)(x'-iy')}{x'^2+y'^2} = \frac{xx'+yy'}{x'^2+y'^2} + i \cdot \frac{x'y-xy'}{x'^2+y'^2}$$

Beispiele

- $(3+2i)(-1+i) = -3+3i-2i+2i^2 = -3+i-2 = -5+i$
- $(-i)(-2+3i) = 2i-3i^2 = 3+2i$
- $(5-i)(5+i) = 25+i^2 = 26$
- $(1+2i)(1-2i) = 1-(2i)^2 = 1-4(-1) = 5$
- $\dfrac{3+2i}{5-3i} = \dfrac{(3+2i)(5+3i)}{(5-3i)(5+3i)} = \dfrac{9+19i}{5^2+3^2} = \dfrac{9}{34}+\dfrac{19}{34}i$
- $\dfrac{1-i}{5-i} = \dfrac{(1-i)(5+i)}{(5-i)(5+i)} = \dfrac{5+i-5i-i^2}{26} = \dfrac{6-4i}{26} = \dfrac{3-2i}{13}$
- $\dfrac{2+2i}{1-i} = \dfrac{(2+2i)(1+i)}{(1-i)(1+i)} = \dfrac{2+2i+2i+2i^2}{2} = \dfrac{2+4i+2(-1)}{2} = \dfrac{4i}{2} = 2i$

Geometrie der komplexen Zahlen

Sei $z = x + iy$ eine komplexe Zahl. Man kann sie auf zwei Arten beschreiben:

- über die Koordinaten x und y, also $x + iy$.
- über den Winkel α, den der Vektor mit der x-Achse einschließt, zusammen mit der Länge $|z|$ des Vektors.

Wie kommt man von einer Beschreibung zur anderen? Mit Schulgeometrie.

Satz

Sei $z = x + iy$ eine komplexe Zahl.

- *Der Winkel α ist $\alpha = \arctan\left(\frac{y}{x}\right)$*
- *Die Länge von z ist $|z|$.*

Umgekehrt: Hat man den Winkel α und die Länge $|z|$ einer komplexen Zahl gegeben, so erhält man die Koordinaten als

$$x = |z| \cdot \cos(\alpha), \quad y = |z| \cdot \sin(\alpha), \text{ also}$$
$$z = |z| \cdot \cos(\alpha) + i \cdot |z| \sin(\alpha)$$

Fundamentalsatz der Algebra

Satz (Fundamentalsatz der Algebra)

Jedes Polynom $p \in \mathbb{C}[x]$ von Grad n besitzt genaue n komplexe Nullstellen $z_1, \ldots, z_n$ (mehrfache Nullstellen treten entsprechend der Multiplizität häufig auf), und es gilt

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n = a_n (x - z_1) \ldots (x - z_n)$$

(d.h. p zerfällt in Linearfaktoren). Wir sagen auch, dass $\mathbb{C}$ **algebraisch abgeschlossen** *ist, da jede Polynomgleichung in $\mathbb{C}$ lösbar ist.*

Beispiel für Linearfaktorzerlegung:

$$2 \cdot x^4 - 8x^3 + 14x^2 - 24x + 24 = 2 \cdot (x-2)(x-2)(x - i\sqrt{3})(x + i\sqrt{3})$$

Satz

Hat $p \in \mathbb{C}[x]$ nur reelle Koeffizienten, dann ist für jede Nullstelle $z \in \mathbb{C}\backslash\mathbb{R}$ auch $\overline{z}$ eine Nullstelle, d.h. nicht-reelle Nullstellen treten immer als Paar auf.

Beweis. Man zeigt zunächst, dass für alle $z \in \mathbb{C}$ gilt:

$$\overline{z + z'} = \overline{z} + \overline{z'} \text{ und}$$
$$\overline{z \cdot z'} = \overline{z} \cdot \overline{z'}$$

Ist nun $p(x) = a_0 + \ldots + a_n x^n \in \mathbb{R}[x]$ und $z \in \mathbb{C}\backslash\mathbb{R}$ eine Nullstelle von p, dann gilt:

$$\begin{aligned}
& a_0 + a_1 z + \ldots + a_n z^n = 0 \\
\Rightarrow\ & \overline{a_0 + a_1 z + \ldots a_n z^n} = \overline{0} = 0 \\
\Rightarrow\ & \overline{a_0} + \overline{a_i} \cdot \overline{z} + \ldots + \overline{a_n z^n} = 0 \\
\Rightarrow\ & a_0 + a_1 \overline{z} + \ldots + a_n \overline{z}^n = 0
\end{aligned}$$

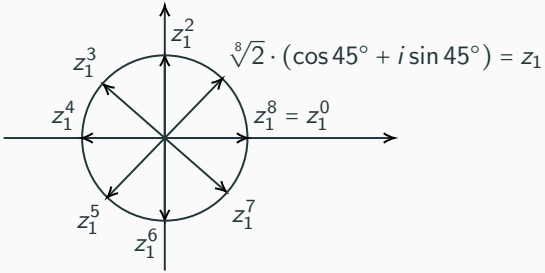
da wegen $a_i \in \mathbb{R}$ auch $\overline{a_i} = a_i$ gilt. ∎

Beispiel

Alle 8 Lösungen der Gleichung $z^8 = 2$:

$z = \sqrt[8]{2} \cdot \ (\cos k \cdot 45° + i \cdot \sin 45°)$ bzw. $z = \left[\sqrt[8]{2} \cdot (\cos 45° + i \cdot \sin 45°)\right]^k$ für $k = 0, 1, \ldots, 7$.

Die 8 Lösungen liegen also äquidistant verteilt auf dem Kreis mit Radius $\sqrt[8]{2}$



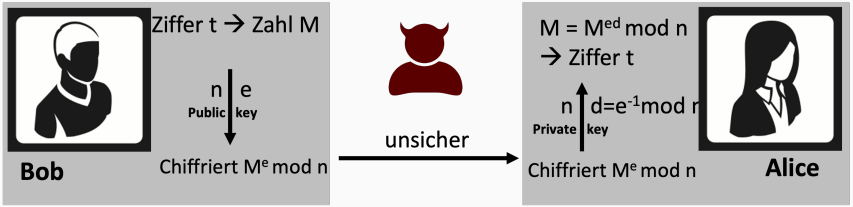
7.2 Endliche Körper

Motivation

Erinnerung: Restklassen und Modulo-Rechnen braucht man für Verschlüsselungsverfahren und viele andere Dinge.

Meist sind dabei auch Primzahlen involviert. Warum? Weil $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p nicht nur ein Ring, sondern ein Körper mit endlich vielen Elementen ist, und deswegen viele nützliche Eigenschaften hat!

Diese Tatsache ist der Knackpunkt des RSA-Verschlüsselungsverfahrens, das wir in diesem Kapitel endlich lernen.



Endliche Körper - Herleitung

Sei $m \in \mathbb{N}$ und $R = \mathbb{Z}/m\mathbb{Z}$ der zugehörige Restklassenring.

Frage: für welche m ist R ein Körper?

- $\mathbb{Z}/2\mathbb{Z}$ ist ein Körper .
- $\mathbb{Z}/m\mathbb{Z}$ ist ein Ring für alle m.
- $\mathbb{Z}/12\mathbb{Z}$ ist kein Körper, da es z.B. für $\overline{9} \in \mathbb{Z}/12\mathbb{Z}$ kein Inverses bzgl. der Multiplikation gibt. Wir beweisen dies mit Widerspruch: Angenommen, es gebe ein $\overline{b} \in \mathbb{Z}/12\mathbb{Z}$ mit $\overline{9} \odot \overline{b} = \overline{1}$
  Dann gibt es ein $a \in \mathbb{Z}$ mit $9 \cdot b = 1 + a \cdot 12$,
  also $9 \cdot b - 12 \cdot a = 1$
  $\Rightarrow 3 \cdot \underbrace{(3b - 4a)}_{\in \mathbb{Z}} = 1$
  Das ist nicht möglich, da 1 kein Vielfaches von 3 ist. Widerspruch. $\Rightarrow \mathbb{Z}/12\mathbb{Z}$ ist kein Körper.

Beispiel: $\mathbb{Z}/12\mathbb{Z}$

Frage: Zu welchen Elementen $\overline{x} \in \mathbb{Z}/12$ gibt es ein Inverses bzgl. der Multiplikation?

Angenommen es gebe ein $\overline{a} \in \mathbb{Z}/12$ mit einem Inversen $\overline{x} \in \mathbb{Z}/12\mathbb{Z}$, also

$$
\begin{aligned}
& \overline{x} \odot \overline{a} = \overline{1} && \in \mathbb{Z}/12\mathbb{Z} \\
\Rightarrow \quad & x \cdot a = 1 + b \cdot 12 && \in \mathbb{Z} \\
\Rightarrow \quad & x \cdot a - b \cdot 12 = 1 \\
\Rightarrow \quad & ggT(x, 12) \cdot \left(\frac{x}{ggT(x, 12)} \cdot a - \frac{12}{ggT(x, 12)} \cdot b \right) = 1 \\
\Rightarrow \quad & ggT(x, 12) = 1
\end{aligned}
$$

Es kommen somit nur Zahlen in Frage, die mit 12 keinen gemeinsamen Teiler haben. (zum Beispiel 1,5,7,11).

Es bleibt die Frage: Haben alle solchen Zahlen, die mit 12 keinen gemeinsamen Teiler haben, ein Inverses bzgl der Multiplikation in $\mathbb{Z}/12\mathbb{Z}$? Oder nur manche?

Schauen wir uns ein $x \in \mathbb{Z}/12$ an mit $ggT(x, 12) = 1$. Der Euklidische Algorithmus liefert nun Zahlen $s, t \in \mathbb{Z}$, so dass

$$\left.\begin{array}{ll} & 1 = ggT(x,12) = s \cdot x + t \cdot 12 \\ \Rightarrow & sx = 1 - t \cdot 12 \\ \Rightarrow & s \cdot x \equiv 1 \bmod 12 \\ \Rightarrow & (s \bmod 12) \cdot (x \bmod 12) = 1 \end{array}\right\} \Rightarrow s \mod 12 \text{ ist das Inverse zu x.}$$

Somit sind alle Elemente in $\mathbb{Z}/12$, für die $ggT(12, x) = 1$ gilt, invertierbar!

Man bezeichnet die Menge dieser Elemente mit $(\mathbb{Z}/12)^x$, die sog. **multiplikative Gruppe.**

Satz

Sei $m \in \mathbb{N}$ und $\mathbb{Z}/m\mathbb{Z}$ der zugehörige Restklassenring. Dann ist $x \in \mathbb{Z}/m\mathbb{Z}$ genau dann invertierbar bzgl. der modularen Multiplikation, falls $ggT(x, m) = 1$.

$(\mathbb{Z}/m\mathbb{Z})^\times := \{x \in \mathbb{Z}/m\mathbb{Z} \mid ggT(m, x) = 1\}$ ist eine multiplikative Gruppe.

Folgerung

$(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist genau dann ein Körper, wenn m eine Primzahl ist.

Beweis.

Falls $\mathbb{Z}/m\mathbb{Z}$ ein Körper ist, dann müssen alle $x \in \mathbb{Z}/m\mathbb{Z}\backslash\{0\}$ invertierbar sein. Nach obigen Satz gilt daher, dass $ggT(x, m) = 1$ für $x = 1, 2, \ldots, m-1$, was genau dann gilt, wenn m prim ist. ■

Definition

Man nennt $\mathbb{Z}/p\mathbb{Z}$ für p prim auch **"Galois-Körper"** oder **"Galois-Field"**, Bezeichnung ist $GF(p)$.

Beispiele

- $\mathbb{Z}/8\mathbb{Z}$ ist kein Körper, da 8 nicht prim ist.
- $\mathbb{Z}/5\mathbb{Z}$ ist ein Körper, z.B. $\overline{3}^{-1} = \overline{2}$, da $\overline{3} \odot \overline{2} = \overline{6} = \overline{1}$ und $\overline{4}^{-1} = \overline{4}$, da $\overline{4} \odot \overline{4} = \overline{16} = \overline{1}$.
- $\mathbb{Z}/27\mathbb{Z}$ ist kein Körper.
- $\mathbb{Z}/19\mathbb{Z}$ ist ein Körper.
- $\mathbb{Z}/101\mathbb{Z}$ ist ein Körper, da 101 eine Primzahl ist. Das heißt es gibt ein Inverses für jede Zahl in $\{\overline{1}, \overline{2}, \ldots, \overline{100}\}$! Diese sind aber nicht ganz so offensichtlich und leicht zu erraten wie bei $\mathbb{Z}/5\mathbb{Z}$. Beispiel: $\overline{13}^{-1} = \overline{70}$, da $\overline{13} \odot \overline{70} = \overline{910} = \overline{9 \cdot 101 + 1} = \overline{1}$. Wie kommt man darauf? Mit dem erweiterten Euklidischen Algorithmus!

Beispiele

in $\mathbb{Z}/101\mathbb{Z}$: Wir suchen ein $\overline{a} \in \mathbb{Z}/101\mathbb{Z}$ mit $\overline{13} \cdot \overline{a} = \overline{1}$, also ein $a \in \{1, 2, \ldots, 100\}$ mit $a \cdot 13 = 1 \mod 101$.

Erweiterter Euklidischer Algorithmus:

$$
\begin{array}{lcll}
101 & = & 7 \cdot 13 + 10 & 10 = 101 - 7 \cdot 13 \\
13 & = & 1 \cdot 10 + 3 & 3 = 13 - 10 \\
 & & & = 13 - (101 - 7 \cdot 13) \\
 & & & = 8 \cdot 13 - 101 \\
10 & = & 3 \cdot 3 + 1 & \Rightarrow 1 = 10 - 3 \cdot 3 \\
 & & & = (101 - 7 \cdot 13) - 3 \cdot (8 \cdot 13 - 101) \\
 & & & = 4 \cdot 101 - 31 \cdot 13 \\
 & & & \Rightarrow 1 = 4 \cdot 101 - 31 \cdot 13 \\
 & & & \Rightarrow (-31) \cdot 13 = 1 - 4 \cdot 101 \\
 & & & \Rightarrow \overline{(-31 \mod 101)} \odot \overline{13} = \overline{1} \text{ (Multiplikation in } \mathbb{Z}/101) \\
 & & & \Rightarrow \overline{70} \odot \overline{13} = \overline{1} \\
 & & & \Rightarrow \overline{13}^{-1} = \overline{70}
\end{array}
$$

Kleiner Fermat für RSA-Verschlüsselung

Satz (Kleiner Fermat)

Ist p eine Primzahl, so gilt für alle $\overline{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$:

$$\overline{a}^{p-1} = \overline{1}.$$

Beispiele:

- $p = 7,\ a = 3$: in $\mathbb{Z}/7\mathbb{Z}$ ist $\overline{3}^{p-1} = \overline{3}^{6} = \overline{3^2}^{3} = \overline{9}^{3} = \overline{2}^{3} = \overline{8 \bmod 7} = \overline{1}$.
- $p = 5,\ a = 4$: in $\mathbb{Z}/5\mathbb{Z}$ ist $\overline{4}^{p-1} = \overline{4}^{4} = \overline{4^2}^{2} = \overline{16}^{2} = \overline{1}^{2} = \overline{1}$.
- $p = 11,\ a = 5$: in $\mathbb{Z}/11\mathbb{Z}$ ist $\overline{5}^{p-1} = \overline{5}^{10} = \overline{5^2}^{5} = \overline{25}^{5} = \overline{3}^{5} = \overline{3}^{3} \odot \overline{3}^{2} = \overline{27} \odot \overline{9} = \overline{5} \odot \overline{9} = \overline{45} = \overline{1}$.

Beweis

Beweis. (Direkter Beweis) Sei $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$. Betrachte folgende Mengen in $\mathbb{Z}/p\mathbb{Z}$:

$\mathbb{Z}/p\mathbb{Z}\backslash\{\overline{0}\} = \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}\}, \quad M = a \odot \mathbb{Z}/p\mathbb{Z}\backslash\{\overline{0}\} = \{\overline{a} \odot \overline{1}, \overline{a} \odot \overline{2}, \overline{a} \odot \overline{3}, \ldots, \overline{a} \odot \overline{p-1}\}$

Die beiden Mengen sind gleich, da $a \cdot i \neq a \cdot j$ wegen $a \cdot (i-j) \neq 0$

Es gilt somit auch, dass die jeweiligen Produkte alle Elemente gleich sein müssen:

$$\underbrace{1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)}_{\cancel{(p-1)!}} = \underbrace{(a \cdot 1)(a \cdot 2) \cdot \ldots \cdot (p-1)}_{a^{p-1} \cdot \cancel{(p-1)!} \bmod p} \bmod p$$

$$1 = a^{p-1} \bmod p$$

■

RSA-Algorithmus (Publik Key Verschlüsselung)

Aufgabe: Person A möchte Nachrichten erhalten (von Person B). Die übertragende Nachricht soll verschlüsselt sein und nur von A entschlüsselt werden können.

1. Schritt (Erzäugung eines Schlüssels durch Person A)

- Wahl von zwei großen Primzahlen p, q $(p, q \approx 2^{1024})$
- Berechnung von $n = p \cdot q$ und $m = (p-1)(q-1)$
- e= Encryption key, zufällig gewählt in $(\mathbb{Z}/m)^x = \{x \in \mathbb{Z}/m \mid ggT(x, m) = 1\}$
- Berechnung von $d = e^{-1}$ in $(\mathbb{Z}/m)^x$, d.h $e \cdot d \equiv 1 \mod m$ mit dem Euklidischen Algorithmus

Public Key: e, n (kann jeder abfragen)

Private Key: d (kennt nur A)

Wir "glauben" (schlaue Mathematiker glauben):

- d kann man nicht berechnen in vernünftiger Zeit, wenn man m nicht kennt.
- p, q können nicht in vernünftiger Zeit berechnet werden.

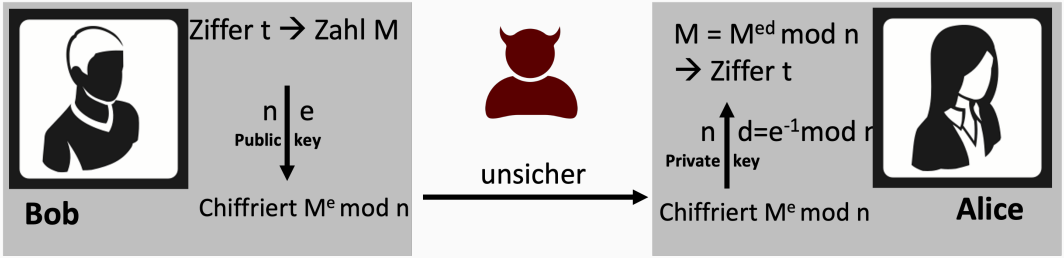
2. Schritt Verschlüsseln/Entschlüsseln

Person B möchte Nachricht $M \in \{1, \ldots, n-1\}$ an Person A schicken.

Verschlüsseln: Berechne $S = M^e \bmod n$ (das macht Person B)

Entschlüsseln: Person A berechnet $M' = S^d \bmod n$
(Jemand, der d nicht kennt, kann diesen Schritt nicht ausführen!)

Behauptung: $M = M'$
(also $M = M^{ed} \bmod p \cdot q$ für $d = e^{-1} \bmod (p-1) \cdot (q-1)$.)



Beweis.

- $e \cdot d \mod (p-1)(q-1) = 1$
  $\Rightarrow e \cdot d = k \cdot (p-1) \cdot (q-1) + 1$ fur ein $k \in \mathbb{Z}$
  $\Rightarrow e \cdot d$ lässt Rest 1 bei Teilung durch $p-1$
  $\Rightarrow e \cdot d$ lässt Rest 1 bei Teilung durch $q-1$
- $S = M^e \mod n$
  $M' = S^d \mod n = (M^e)^d \mod n$
  $= M^{e \cdot d} \mod n$
  Wir haben im ersten Schritt gezeigt, dass $e \cdot d = k_i(p-1) + 1$
  $\Rightarrow M^{e \cdot d} \mod p = M^{k_i \cdot (p-1)+1} \mod p$
  $= \left(M^{p-1}\right)^{k_1} \mod p \cdot M = 1 \cdot M = M$
  (da $M^{p-1} = 1$ wegen Fermat)

Analog zeigt man $M^{ed} \mod q = M$. Somit haben wir gezeigt, dass $M^{ed} - M$ durch p und durch q teilbar sind. Also ist auch $M^{ed} - M$ durch $n = p \cdot q$ teilbar

$\Rightarrow M' = M^{ed} \mod n = M$ ■