Primzahlen

Eine ganze Zahl $p \in \mathbb{Z}$, $p > 1$ heisst Primzahl genau dann, wenn die einzigen Teiler von p die Zahlen ± 1 und $\pm p$. Eine Zahl $n > 1$ heisst zusammengesetzte Zahl, wenn sie keine Primzahl ist.

Satz (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis (der klassische Widerspruchsbeweis).

- Annahme: Es gibt nur endlich viele Primzahlen
- Dann folgt, diese können aufgezählt werden und der Größe nach sortiert werden.

$$P = \{2, 3, 5, 7, \dots, p_n\}$$

- Bilde die Zahl

$$q = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot p_n$$

$\Rightarrow$ q wird ohne Rest durch jede Primzahl geteilt.

- Betrachte $q+1$

Da P alle Primzahlen enthält, muss $q+1$ Teiler aus P enthalten.

- Wegen "+1" bleibt stets der Rest 1, wenn q durch irgendeine Zahl aus P geteilt wird.
- $\Rightarrow$ keine Zahl aus P ist Teiler von $q+1$, also hat $q+1$ einen anderen Primteiler oder ist selbst Primzahl.
- Widerspruch zur Annahme, dass es endliche viele Primzahlen gibt.

$\Rightarrow$ folgt die Aussage.

~~Satz~~ Der zentrale Satz der Zahlentheorie (Fundamentalsatz) sagt aus, dass jede natürliche Zahl $n \in \mathbb{N}$, $n > 2$ eindeutig (bis auf die Reihenfolge der Faktoren) als Produkt von Potenzen von Primzahlen geschrieben werden kann

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

Bsp: $60 = 2 \cdot 30 = 2 \cdot 3 \cdot 5 \cdot 2 = 2^2 \cdot 3^1 \cdot 5^1$

Die Zerlegung einer Zahl in ihre Primfaktoren nennt man Faktorisierung.

$(n = p \cdot q)$

Definition

(a) Seien $a, b \in \mathbb{Z}$, $k \in \mathbb{Z}$, k sei Teiler von a und b, dann heisst k gemeinsamer Teiler

ahh

von a und b. Eine Zahl $v \in \mathbb{Z}$ heisst
<u>gemeinsames Vielfaches</u> von a und b, wenn v durch a und b geteilt wird.

(b) Sei $a \neq 0$ oder $b \neq 0$. Dann heisst die größte Zahl k, die sowohl a als auch b teilt größter gemeinsamer Teiler von a und b,

$$\underline{k = ggT(a, b)}$$

(c) Sei $a \neq 0$, $b \neq 0$, die kleinste natürliche Zahl v, die ein gemeinsames Vielfaches von a und b ist heisst kleinstes gemeinsames Vielfaches von a und b,

$$\underline{v = kgV(a, b)}$$

(d) Def. $ggT(0, 0) = 0$

$kgV(0, a) = kgV(a, 0) = 0. \quad \forall a \in \mathbb{Z}$

<u>Beispiel:</u> $ggT(60, 24) = 12$

Wie berechnet man den ggT?

- Schulmethode:

  Faktorisierung: $ggT(300, 36)$

$$300 = 2 \cdot 150 = 4 \cdot 75 = 2^2 \cdot 3^1 \cdot 5^2$$
$$36 = 2 \cdot 18 = 4 \cdot 9 = 2^2 \cdot 3^2$$

$$ggT = 2^2 \cdot 3^1 = 12$$

- Effektives Verfahren: Euklidischer Algorithmus
  $\longrightarrow$ später.

Def:

Zwei Zahlen $a, b \in \mathbb{Z}$ nennt man coprim, teilerfremd oder relativ prim, wenn sie keinen Primfaktor gemeinsam haben.

Gleichwertig $ggT(a,b) = 1$.

Beispiel $a = 8$, $b = 15$ sind coprim

wenn a, b Primzahlen sind, dann sind sie auch coprim.

Die EULERsche Totientenfunktion

Die EULER-Funktion $\Phi(n)$ sagt aus, wie viele Zahlen a mit $1 \leq a < n$ existieren, mit $ggT(a,n) = 1$.

$n = 5$ $\Phi(5)$, da 5 eine Primzahl ist, ist jede Zahl < 5 coprim

$\Phi(5) = 4$

1, 2, 3, 4

$n = \cancel{18}\ 22$ $\Phi(22) = 10$ $(a, n-a)$

1, 3, 5, 7, 9, 13, 15, 17, 19, 21

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

$\phi(p) = p - 1$ falls p eine Primzahl ist.

$$\phi(3) \cdot \phi(7) = 2 \cdot 6 = 12$$

$$\phi(3 \cdot 7) = \phi(21) = 12$$

$$\phi(4) \cdot \phi(5) = 2 \cdot 4 = \phi(4 \cdot 5) = \phi(20) = 8$$

$$\phi(n) \cdot \phi(m) = \phi(n \cdot m)$$

aber:

$$\phi(4) \cdot \phi(6) = 2 \cdot 2 = 4$$

$$\phi(24) = 8$$

Es gilt der folgende Satz:

$$\boxed{\text{Wenn } ggT(n,m) = 1 \Rightarrow \phi(m) \cdot \phi(n) = \phi(n \cdot m)}$$

Folgerung: Sind p, q zwei Primzahlen und $n = p \cdot q$, dann ist

$$\phi(n) = \phi(p \cdot q) \overset{ggT(p,q)=1}{=} \phi(p) \cdot \phi(q) \overset{p,q \text{ Primzahlen}}{=} (p-1) \cdot (q-1),$$

Satz: Ist n eine natürliche Zahl und

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

die Primfaktorzerlegung von n. Dann ist

$$\boxed{\phi(n) = \prod_{i=1}^{k} (p_i - 1) \cdot p_i^{\alpha_i - 1}}$$

RSA

(1) Wähle zwei große Pr p, q,

$n = p \cdot q$

(2) Berechne $\phi(n) = (p-1)(q-1)$

⋮

e

$d \cdot e = 1 \mod \phi(n)$

$K_{pub} = (e, n)$, $K_{pri} = (d, n)$

Beispiel $n = 75 = 3 \cdot 5 \cdot 5 = 3^1 \cdot 5^2$.

$$\phi(75) = \prod_{i=1}^{2} (p_i - 1) \cdot p_i^{\alpha_i - 1}$$

$$= (3-1)\cdot 3^0 \cdot (5-1)\cdot 5$$

$$= 2\cdot 4\cdot 5 = \underline{40}$$

$n = 30$ $\qquad 30 = 2\cdot 15 = \underline{2\cdot 3\cdot 5}$

$$\prod_{i=1}^{3} p_i^{\alpha_i} = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot p_3^{\alpha_3}$$

$$\Phi(30) = (p_1 - 1)\, p_1^0 \cdot (p_2 - 1)\, p_2^0\, (p_3 - 1)\, p_3^0$$

$$= 1\cdot 2\cdot 4 = \underline{\underline{8}}$$

Kongruenzen und modulare Arithmetik

Betrachte die Menge $\mathbb{Z}$. Wir definieren auf $\mathbb{Z}$ eine Relation

$$\equiv_n \;\subseteq\; \mathbb{Z}\times\mathbb{Z}$$

mit:

$$x \equiv_n y \quad \text{genau dann, wenn } n \mid x-y.$$

Sind A, B zwei Mengen, dann ist eine <u>Relation</u> R eine Teilmenge des kartesischen Produktes $A\times B$

$$R \subseteq A\times B = \{\underbrace{(a,b)}_{\text{geordnete Paare}} \mid a\in A,\; b\in B\}$$

$A = \{a, b, c\}$, $B = \{1, 2, 3\}$

$$A \times B = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3), (c,1), (c,2), (c,3)\}$$

$$R = \{(a,1), (a,2), (b,3), (c,1)\}$$

A	B
a	1
a	2
b	3
c	1

Die Kongruenzrelation

$x \equiv_n y$ genau dann, wenn $n \mid x - y$

heisst also: x steht in Relation zu y

- wenn $x - y$ ohne Rest durch n geteilt wird.

oder:

- x und y haben den gleichen Rest, wenn sie (getrennt) durch n geteilt werden

oder:

- $x = k \cdot n + r$ $k \in \mathbb{Z}$, $r < n$
  $y = l \cdot n + r$ $l \in \mathbb{Z}$, $r < n$

oder:

- $\boxed{x \equiv y \mod n}$ (x kongruent y modulo n)

oder

- $x = k \cdot n + y$ $k \in \mathbb{Z}$.

Satz: Die Kongruenzrelation $x \equiv y \mod n$ ist eine Äquivalenzrelation.

Intermezzo: Äquivalenzrelationen

Betrachte die Menge

$$M = \{1, 2, 3, 4, 5\}$$

Definiere auf M die Relation

$$\begin{aligned} R &\subseteq M \times M \\ &= \{(1,1), (2,2), (3,3), (4,4), (5,5), \\ &\quad (1,2), (2,1), (2,5)(5,2), (1,5), (5,1), \\ &\quad (3,4), (4,3)\} \end{aligned}$$

R ist reflexiv, d.h.

$$(x,x) \in R \quad \forall x \in M.$$

R ist symmetrisch

Wenn $(x,y) \in R$ dann auch $(y,x) \in R$

$(1,2), (2,1)$, $(2,5), (5,2)$, $(1,5), (5,1)$ ...

R ist transitiv

Wenn $(x,y) \in R$, und $(y,z) \in R$

$\rightarrow (x,z) \in R.$

$(1,2) \in R$ und $(2,5)$ $\rightarrow (1,5) \in R.$

Ist R reflexiv, symmetrisch und transitiv, dann ist R eine Äquivalenzrelation.

R ist transitiv, d.h.

$$(x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R.$$

$$[\text{Jochim}] = \{y \in M \mid (\text{Jochim}, y) \in R\}$$

$$= \text{INF16A}$$

$$[\text{Meyer}] = \text{INF16B}$$

$$[\text{Jochim}] \cap [\text{Meyer}] = \emptyset$$ paarweise disjunkt.

$$[\text{Jochim}] \cup [\text{Meyer}] \cup \ldots = M$$

$x \equiv y \mod n$ ist eine Äquivalenzrelation

1) Reflexivität: $(x,x) \in R$, $x \equiv x \mod n$. $\forall x \in M$.

$$\Rightarrow x - x = k \cdot n$$

$$0 = k \cdot n \quad k \in \mathbb{Z},\ k = 0$$

2) Symmetrie: $(x,y) \in R \Rightarrow (y,x) \in R$

$$x \equiv y \mod n \Rightarrow y \equiv x \mod n.$$

$$x - y = k \cdot n \quad k \in \mathbb{Z}$$

$$\Rightarrow y - x = -k \cdot n, \quad -k \in \mathbb{Z} = \text{mathbb}$$

$\Rightarrow$ $y - x$ ist Vielfaches von n

$$y \equiv x \mod n.$$

Betrachte Äquivalenzklassen:

$$[x] = \{ y \in M \mid (x,y) \in R \}$$

$$[1] = \{ y \in M \mid (1,y) \in R \}$$
$$= \{1, 2, 5\}$$

$$[2] = \{ y \in M \mid (2,y) \in R \} = \{1,2,5\} = [1] = [5]$$

$$[3] = \{ y \in M \mid (3,y) \in R \} = \{3,4\} = [4]$$

Durch obige Äquivalenzrelation zerfällt die Grundmenge M in zwei Äquivalenzklassen

$$[1] \; (= [2] = [5]) = \{1,2,5\}$$
$$[3] \; (= [4]) = \{3,4\}$$

$$[1] \cap [3] = \emptyset$$
$$[1] \cup [3] = M$$

Partitionierung von M.

$M = \{$ Studenten der DHBW Mosbach $\}$

$R \subseteq M \times M$

$= \{ (x,y) \in M \times M \mid x$ ist im gleichen Kurs wie $y \}$

R ist eine Äquivalenzrelation, denn

R ist reflexiv, d.h. $(x,x) \in R \; \forall x \in M$. ✓

R ist symm. d.h. wenn $(x,y) \in R \Rightarrow (y,x) \in R$. ✓

3) Transitivität

$$(x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R$$

zu zeigen $x \equiv y \bmod n$ und $y \equiv z \bmod n \Rightarrow x \equiv z \bmod n$

$$x - y = kn \qquad y - z = ln \qquad k, l \in \mathbb{Z}$$

$$\cancel{x}(x - y) + (y - z) = k \cdot n + l \cdot n$$

$$\Rightarrow (x - z) = \underbrace{(k + l)}_{m} \cdot n \quad , m \in \mathbb{Z}$$

$$(x - z) = m \cdot n$$

$$\Rightarrow x \equiv z \bmod n$$

Beispiele:

$$-8 \equiv -3 \equiv 2 \equiv 7 \equiv 12 \equiv 17 \bmod 5$$

$$-4 \equiv 1 \bmod 5$$

$$-8 \equiv 10 \bmod 18$$

Restklassen und modulare Arithmetik

(d.h. Rechnen mit mod)

Beispiel $n = 5$

$$[0] = \{ y \in \mathbb{Z} \mid y \text{ geteilt durch } 5 \text{ bleibt Rest } 0 \}$$
$$= \{ y \in \mathbb{Z} \mid y = k \cdot 5 + 0 \quad k \in \mathbb{Z} \}$$
$$= \{ \ldots, -10, -5, 0, 5, 10, \ldots \}$$

$$[1] = \{ y \in \mathbb{Z} \mid y = k \cdot 5 + 1, k \in \mathbb{Z} \}$$
$$= \{ \ldots, -9, -4, 1, 6, 11, 16, \ldots \}$$
$$[2] = \{ y \in \mathbb{Z} \mid y = k \cdot 5 + 2, k \in \mathbb{Z} \}$$
$$= \{ \ldots, -8, -3, 2, 7, 12, \ldots \}$$
$$[3] = \{ \ldots, -7, -2, 3, 8, 13 \ldots \}$$
$$[4] = \{ \ldots, -6, -1, 4, 9, 14, \ldots \}$$

$[0] \cap [1] = \emptyset$

$[0] \cap [2] = \emptyset$ usw. paarweise disjunkt

$$[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$$

Man bezeichnet mit $\mathbb{Z}_5 = \{ [0], [1], .., [4] \}$

die Menge der Restklassen modulo 5

Allgemein: $\mathbb{Z}_n = \{ [0], \ldots, [n-1] \}$

Menge der Restklassen mod n.

Schreibe

$$\mathbb{Z}_n = \underbrace{\{ 0, \ldots, n-1 \}}_{n \text{ "Zahlen"}}.$$

Definition

Die binäre Operation:

$$\oplus_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$[x], [y] \longmapsto [x] \oplus_n [y]$$
$$= (x+y) \bmod n$$

heisst Addition modulo n

und

$$\otimes_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$[x], [y] \longmapsto [x] \otimes_n [y]$$
$$= (x \cdot y) \bmod n$$

heisst Multiplikation mod n.

Beispiel $n = 5$

Betrachte die Addition mod 5 auf $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$\to \mathbb{Z}_5$

$\downarrow \mathbb{Z}_5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$(x+y) \bmod 5$

0 ist neutrales Element der Add. mod 5.

$$(0 + a) \bmod 5 = a \quad \forall a \in \mathbb{Z}_5$$

Für jedes $a \in \mathbb{Z}_5$ existiert ein $(-a) \in \mathbb{Z}_5$

mit

$$a + (-a) \equiv 0 \mod 5$$ (additives Inverses)

$$0 + 0 \equiv 0 \mod 5$$

$$\cancel{1} + 4 \equiv 0 \mod 5$$

$$2 + 3 \equiv 0 \mod 5$$

$$3 + 2 \equiv 0 \mod 5$$

$$4 + 1 \equiv 0 \mod 5.$$

Multiplikation mod 5 $\qquad x \cdot y \mod 5$

$x \downarrow$ / $\to y$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Es gilt: $\forall x \in \mathbb{Z}_5 \setminus \{0\} \; \exists x^{-1} \in \mathbb{Z}_5$ mit

$$x \cdot x^{-1} \equiv 1 \mod 5$$

für jedes $x \in \mathbb{Z}_5 \setminus \{0\}$ existiert das multiplikative Inverse

$\Rightarrow (\mathbb{Z}_5, +, \cdot \mod 5)$ ist ein endlicher Körper!