Primzahlen

Eine Zahl p heisst Primzahl, wenn die einzigen Teiler von p die Zahlen p und ± 1 sind.

Fundamentalsatz der Zahlentheorie

Jede natürliche Zahl $n > 2$ lässt sich als Produkt von Primzahlen darstellen, d.h.

$$n = \prod_{i=1}^{n} p_i^{\alpha_i} = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$$

und $p_1 < p_2 < \ldots < p_n$ sind Primzahlen $\alpha_i > 0$, $\alpha_i \in \mathbb{N}$.

Die Zerlegung einer Zahl $n \in \mathbb{N}$ in ihre Primfaktoren heisst <u>Faktorisierung</u>.

<u>Definition</u>:

(a) Seien $a, b \in \mathbb{Z}$, $k \in \mathbb{Z}$. Sei k Teiler von a und b. Dann nennt man k <u>gemeinsamer Teiler</u> von a und b. Analog nennt man eine Zahl v, die von a und b geteilt wird, ein <u>gemeinsames Vielfaches</u> von a und b

(b) Sei $a \neq 0$ oder $b \neq 0$, dann ist die <u>größte</u> Zahl $k \in \mathbb{N}$ die gemeinsamer Teiler von a und b ist, der größte gemeinsame Teiler von a, b, schreibe

$$k = ggT(a, b).$$

(c) Sei $a \neq 0$ oder $b \neq 0$. Die kleinste natürliche Zahl v, die ein gemeinsames Vielfaches von a und b ist, heißt das kleinste gemeinsame Vielfache von a, b,

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

(d) Def.

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

Bestimmung des ggTs:

Schulmethode: Faktorisierung

$$\mathrm{ggT}(36, 300)$$

$$36 = 4 \cdot 9 = 2^2 \cdot 3^2$$

$$300 = 4 \cdot 25 \cdot 3 = 2^2 \cdot 3^1 \cdot 5^2$$

$$\Rightarrow \mathrm{ggT}(36, 300) = 2^2 \cdot 3^1 = 12.$$

Es gibt ein effektives Verfahren, den ggT zu bestimmen, Euklidischer Algorithmus. (→ später).

Relativ prime Zahlen

Def

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

Der Begriff coprim ist gleichwertig dazu, zu sagen,

$$\mathrm{ggT}(a,b) = 1.$$

Beispiele:

$ggT(8, 15) = 1$, daher sind 8, 15 coprim.

$ggT(19, 23) = 1$, $ggT(p_1, p_2) = 1$ falls p_1, p_2 Primzahlen sind.

Ein wichtiges Konzept ist die EULER-Funktion, oder EULER-Totientenfunktion.

$\phi(n)$ gibt an, wieviele Zahlen $a \in \mathbb{N}$, $a \geq 1$ existieren und $a < n$ und $ggT(a, n) = 1$.

$\phi(n)$ gibt, wieviele coprime Zahlen $< n$ existieren.

(1) $n = 5$ $\quad \phi(5) = 4$,

~~ggT~~ $ggT(1,5) = ggT(2,5)$
$= ggT(3,5)$
$= ggT(4,5) = 1$

(2) $n = 18$

$\phi(18) = 6$ $\quad ggT(a, 18) = 1$

weil $\underbrace{1, 5, 7, 11, 13, 17}$ $\quad a = 1, \dots, 17$

$a, n - a$

(3) $n = 10$ $\quad \phi(10) = 4$

1, 3, 7, 9.

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

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

wenn ~~gT~~ $ggT(a,n) = 1 \Rightarrow ggT(n-a, n) = 1$

$\Rightarrow \phi(n)$ ist gerade, $a, n-a$.

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

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

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

$\phi(3) \cdot \phi(9) = 2 \cdot 6 = 12$

$\phi(27) = 18$

Satz:

Wenn $ggT(m,n) = 1 \Rightarrow \phi(m) \cdot \phi(n) = \phi(m \cdot n)$

Folgerung

Wenn p, q zwei Primzahlen sind und $n = p \cdot q$

$$\Rightarrow \quad \phi(n) = \phi(p \cdot q) \overset{ggT(p,q)=1}{=} \phi(p) \cdot \phi(q)$$

p, q Primzahlen
$\Rightarrow \phi(p) = p-1$

$$= (p-1) \cdot (q-1)$$

Die Art & Weise, wie man $\phi(n)$ im allgemeinen Fall berechnen kann, liefert der Fundamentalsatz der Zahlentheorie

Satz: Ist n eine natürliche Zahl, und

$$n = \prod_{j=1}^{n} p_j^{\alpha_j} = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n},$$

$$\Rightarrow \quad \phi(n) = \prod_{j=1}^{n} (p_j - 1) \cdot p_j^{\alpha_j - 1} \qquad (*)$$

$\Rightarrow$ Wichtig: Um $\phi(n)$ im allgemeinen zu berechnen, ist die Primfaktorzerlegung von n Voraussetzung.

Bsp: Tabelle $\phi(30) = 8$

$$30 = 2 \cdot 3 \cdot 5 = p_1^1 \cdot p_2^1 \cdot p_3^1 \qquad p_1 = 2, \; p_2 = 3, \; p_3 = 5$$

$$\phi(30) \overset{(*)}{=} (2-1) \cdot 2^0 \cdot (3-1) \cdot 3^0 \cdot (5-1) \cdot 5^0$$

$$= 2 \cdot 4 = 8 \checkmark$$

Kongruenzen, Restklassen & friends

Betrachte $\mathbb{Z}$; auf $\mathbb{Z} \times \mathbb{Z}$ führt man eine Relation ein

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

[Relation ist eine Teilmenge des kartesischen Produkts zweier Mengen]

mit $x \equiv_n y$ genau dann, wenn $n \mid x-y$, n fest $n \in \mathbb{N}$.

Oder: Zwei Zahlen $x, y \in \mathbb{Z}$ stehen in Relation genau dann, wenn

$x - y$ ohne Rest durch n teilbar ist

oder

x durch n geteilt bleibt Rest r

und y " " " " ebenfalls Rest r.

oder

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

oder

$$\boxed{x \equiv y \mod n}$$

Beispiele:

$$2 \equiv 7 \equiv 12 \equiv 17 \mod 5.$$

$$-1 \equiv -6 \equiv 4 \mod 5$$

$$178 \equiv 17 \equiv 3 \mod 7$$

$17 - 3 = 14$ ist ohne Rest durch 7 teilbar.

~~6 − 4~~

$$-6 \equiv 4 \mod 5$$

$-6 - 4 = -10$ ist ohne Rest durch 5 teilbar.

Satz

Die Kongruenzrelation

$$x \equiv y \mod n$$

ist eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis: Zu zeigen:
- reflexiv
- symmetrisch
- transitiv

1) Reflexiv heisst: $x \equiv x \mod n$, $\forall x \in \mathbb{Z}$.

oder ~~weil~~ $x - x$ wird durch n ohne Rest geteilt
0 " " " "

✓

2) Symmetrisch heisst:

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

wenn $x \equiv y \mod n \Rightarrow x - y = k \cdot n$, $k \in \mathbb{Z}$

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

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

3) transitiv heisst

wenn $x \equiv y \mod n$ und $y \equiv z \mod n$

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

$x \equiv y \mod n \Rightarrow x - y = kn$ $\quad k, l \in \mathbb{Z}$

$y \equiv z \mod n \Rightarrow y - z = ln$

$\Rightarrow (x-y) + (y-z) = k \cdot n + l \cdot n$

$\Leftrightarrow x - z = (k+l) \cdot n$

$\Rightarrow x - z = m \cdot n \quad m \in \mathbb{Z}$

$\Rightarrow x \equiv z \mod n$

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

Bsp: $M = \{1, 2, 3\}$

$R \subseteq M \times M = \{(1,1)(2,2),(3,3),(2,1),(1,2)\}$

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

sym. wenn $(x,y) \in R \Rightarrow (y,x) \in R$

Äquivalenzklassen:

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

$[1] = \{1, 2\}$

$[2] = \{2, 1\} = [1]$ $\Big\}$ 2 Äquivalenz-klassen

$[3] = \{3\}$

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

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

Partitionierung, d.h. die Zerlegung einer Menge M in $\emptyset$

paarweise disjunkte Äquivalenzklassen.

Noch ein Bsp.

M = Menge aller DHBW Studenten in Mosbach.

$R \subseteq M \times M$

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

reflexiv: $(x,x) \in R \ \forall x \in M.$ ✓

sym. $(x,y) \in R \Rightarrow (y,x) \in R.$ ✓

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

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

$[x] \cap [y] = \emptyset$

Wissen: $x \equiv y \mod n$ ist eine Äquivalenzrelation über $\mathbb{Z}$.

wie sehen die zugehörigen Äquivalenzklassen aus?

$\Rightarrow$ Restklassen.

Bsp. $n = 5$ $\quad x \equiv y \mod 5$

$$[0] = \{y \in \mathbb{Z} \mid y \text{ geteilt durch 5 bleibt Rest } 0\}$$
$$= \{y \in \mathbb{Z} \mid y = k \cdot 5 \quad k \in \mathbb{Z}\}$$
$$= \{\dots, -15, -10, -5, 0, 5, 10, \dots\}$$
$$[1] = \{y \in \mathbb{Z} \mid y = k \cdot 5 + 1, \; k \in \mathbb{Z}\}$$
$$= \{\dots -14, -9, -4, 1, 6, 11, \dots\}$$
$$[2] = \{y \in \mathbb{Z} \mid y = k \cdot 5 + 2 \quad k \in \mathbb{Z}\}$$
$$= \{\dots -13, -8, -3, 2, 7, \dots\}$$
$$[3] = \{\dots -12, -7, -2, 3, 8, 13, \dots\}$$
$$[4] = \{\dots -11, -6, -1, 4, 9, 14, \dots\}$$
$$[5] = [0]$$
$$[1] \cap [2] = \emptyset \quad \Big| \quad [0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}$$

Definiere $\quad \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

ist die Menge der Restklassen mod 5.

Schreibweise ("S-ung"): Man schreibt $\quad \mathbb{Z}_5 = \{0, \dots, 4\}$

Analog: Wenn man die Relation $x \equiv y \mod n$ betrachtet, wird $\mathbb{Z}$ in n Restklassen

$$\mathbb{Z}_n = \{0, \dots, n-1\}$$ zerlegt.

Auf der Menge der Restklassen modulo n lassen sich zwei binäre Operationen definieren.

Def:

$$\oplus_n : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$[x], [y] \longmapsto [x] \oplus_n [y] = (x+y) \bmod n$$

Addition modulo n

$$\otimes_n : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$[x], [y] \longmapsto [x] \otimes_n [y] = (x \cdot y) \bmod n.$$

Multiplikation mod n.

Bsp: $n = 5$

$\oplus_5$: $(x+y) \bmod 5$

$\oplus_5$	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

$\mathbb{Z}_5$ ist abgeschlossen unter $\oplus_5$

Aus Z1 oder Spalte 1 → 0 ist neutrales Element der Add. mod 5

$$(0 + a) \bmod 5 = a \bmod 5$$

und ~~A~~ $[1] + [4] = [0]$

$[2] + [3] = [0]$

d.h. für jedes Element a aus $\mathbb{Z}_5$ gibt es ein Element $-a$ mit $a + (-a) \equiv 0 \bmod 5$

$-1 \equiv 4 \mod 5$

$-2 \equiv 3 \mod 5$

$-3 \equiv 2 \mod 5$

$-4 \equiv 1 \mod 5$

Wie sieht's mit $\otimes_5$ aus?

$x \cdot y \bmod 5$

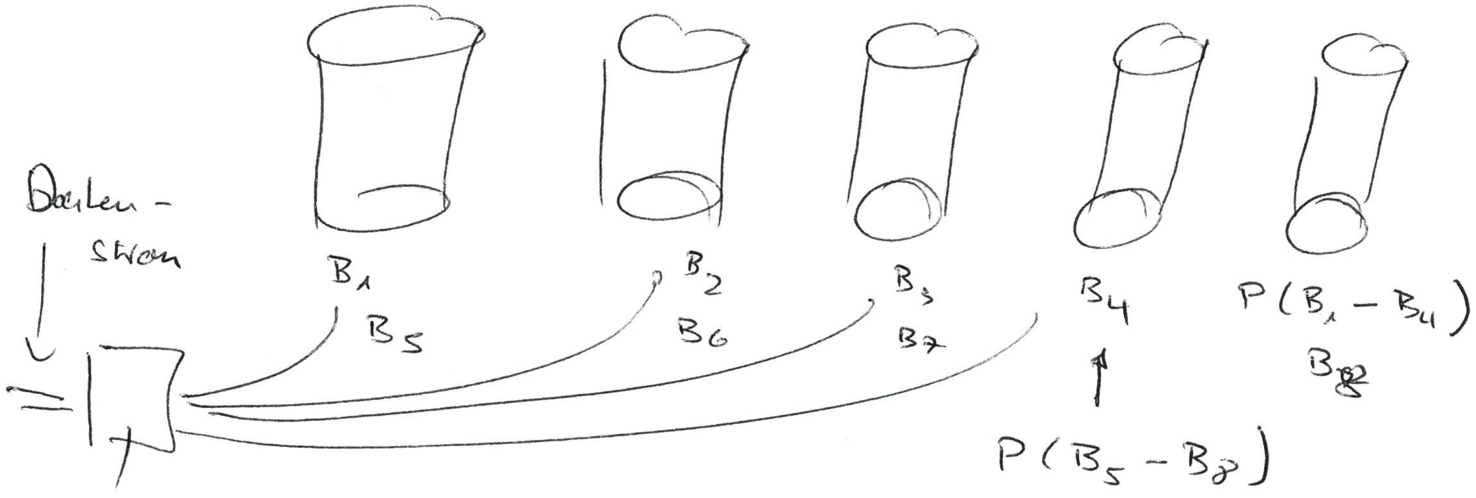
$\otimes_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_5 = \{0, \dots, 4\}$

1 ist neutrales Element $[1] \otimes_5 [a] = [a] \quad \forall [a] \in \mathbb{Z}_5$

Zu jedem $x \in \mathbb{Z}_5 \setminus [0]$ existiert ein x^{-1} mit $x \cdot x^{-1} \equiv 1 \bmod 5$

Kurzes Intermezzo RAID Level 5



Raid-Controller

$$
\begin{array}{ll}
B_1 & 10110 \\
B_2 & 01001 \\
B_3 & 11101 \\
B_4 & 10001 \\
\hline
P_{1-4} & = 10011
\end{array}
\quad +
$$

Lw 3 gibt den Geist auf. Der RAID-Controller rekonstruiert im laufenden Betrieb die verlorenen Datenblöcke auf eine Ersatzplatte (hot spare)

$$
\begin{array}{ll}
B_1 & 10110 \\
B_2 & 01001 \\
B_4 & 10001 \\
\hline
\text{Neue P.} & 01110
\end{array}
$$

Syndrom:

$P_{alt} \oplus P_{neu}$

$$
\begin{array}{ll}
10011 & \\
01110 & \\
\hline
11101 & B_3
\end{array}
$$

Das klappt:

$$P_{alt} \oplus P_{neu} = [B_1 \oplus B_2 \oplus B_3 \oplus B_4] \oplus [B_1 \oplus B_2 \oplus B_4]$$

$$= (B_1 \oplus B_1) \oplus (B_2 \oplus B_2) \oplus B_3 \oplus (B_4 \oplus B_4)$$

$$= 0 \oplus 0 \oplus B_3 \oplus 0 = \underline{\underline{B_3}}$$

Multiplikation auf $\mathbb{Z}_2$ $\qquad x \cdot y \mod 2$

$\otimes_2$	0	1
0	0	0
1	0	1

x	y	$x \cdot y \mod 2$
0	0	0
0	1	0
1	0	0
1	1	1

AND-Funktion

Beachte: In $\mathbb{Z}_2$ gilt der Traum aller Schüler:

$$(x+y)^2 = x^2 + y^2 \quad !$$

---

in $\mathbb{Z}_5$: $(x+y)^5 = x^5 + y^5$

$\mathbb{Z}_5$ ist ebenfalls ein Körper.

d.h. es gibt für jedes $x \in \mathbb{Z}_5 \setminus \{0\}$ ein multiplikatives Inverses x^{-1}

$$1^{-1} = 1$$
$$2^{-1} = 3$$
$$3^{-1} = 2$$
$$4^{-1} = 4$$

$\Rightarrow (\mathbb{Z}_5, +, \times)$ ist ein endlicher Körper

---

$n=2$ $\mathbb{Z}_2 = \{0, 1\}$

$x + y \mod 2$

	0	1
0	0	1
1	1	0

x	y	x+y mod
0	0	0
0	1	1
1	0	1
1	1	0

auf $\mathbb{Z}_2$ ist die Addition gleich der Subtraktion!

$$0 + 0 = 0$$
$$1 + 1 = 0$$

$$a + (-a) = 0$$

$n = 9$ $\boxed{x \cdot y \bmod 9}$ (~~Übung n = 365~~)

	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Es gibt <u>nicht</u> zu jedem $x \in \mathbb{Z}_9$ ein x^{-1} mit

$$x \cdot x^{-1} \equiv 1 \mod 9 .$$

Funktioniert bei $x = 1, 2, 4, 5, 7, 8$ $\quad ggT(x, 9) = 1$

" nicht $x = 3, 6$

Wenn $ggT(x, 9) = 1 \Rightarrow$ es existiert ein $x^{-1} \in \mathbb{Z}_9$ mit

$$x \cdot x^{-1} \equiv 1 \mod 9$$