Wiederholung

Satz 3.8: Sei $(R, +, \cdot)$ ein endlicher Ring mit Eins, $R \neq \{0\}$

R ist ein Körper $\iff$ R hat keine Nullteiler

Beweis: $\Rightarrow$: Angenommen $a, b \in R \setminus \{0\}$ und $ab = 0$

Da R ein Körper ist, existieren c, d sodass $ac = bd = 1$

Also $abcd = 1$

Aber $abcd = 0 \cdot cd = 0$

also ist $0 = 1$

Aber $\forall\, x \in R$ gilt $0 = 0 \cdot x = 1 \cdot x = x$ also $x = 0$ ↯

$\Leftarrow$: Wie oben ist $0 \neq 1$

Wir müssen beweisen, dass zu jedem $a \in R \setminus \{0\}$ existiert $b \in R$ sodass $ab = 1$

Wären $b, c \in R \setminus \{0\}$ verschieden mit $ab = ac$, so wäre $a(b-c) = 0$ mit $a, b-c \neq 0$ ↯

Also sind die Elemente ab immer verschieden für verschiedene b, und ungleich 0.

Also $|\{ab : b \in R \setminus \{0\}\}| = |\{b \in R \setminus \{0\}\}|$

$= |R \setminus \{0\}|$

und $\{ab : b \in R \setminus \{0\}\} \subseteq R \setminus \{0\}$

also ist $\{ab : b \in R \setminus \{0\}\} = R \setminus \{0\}$

Insbesondere existiert ein $b \in R \setminus \{0\}$ sodass $ab = 1 \in R \setminus \{0\}$ □

Def: Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe

Der Produktring $(R \times S, +, \cdot)$ ist definiert durch

$$R \times S := \{(r,s) : r \in R, s \in S\}$$
$$(r_1, s_1) + (r_2, s_2) := (r_1 +_R r_2, s_1 +_S s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) := (r_1 \cdot_R r_2, s_1 \cdot_S s_2)$$

Proposition 3.10: $(R \times S, +, \cdot)$ ist ein Ring
$R \times S$ hat eine Eins $\Leftrightarrow$ R und S haben jeweils eine Eins
in diesem Fall ist $1_{R \times S} = (1_R, 1_S)$

Beweis: Aufgabe

Wir betrachten wieder $\mathbb{Z}/m\mathbb{Z}$
Wir schreiben ab für $a \cdot b$
Wir schreiben $[x]_m$ für $[x]_{m\mathbb{Z}}$

Def: Wir sagen $x \equiv y \bmod m$ wenn $[x]_m = [y]_m$
$\Leftrightarrow [x-y]_m = [0]_m$
$\Leftrightarrow m \mid x-y$

Satz 3.11 (Chinesischer Restsatz)
Seien $m_1, \dots, m_n \in \mathbb{N}^+$ paarweise teilerfremd und
$a_1, \dots, a_n \in \mathbb{Z}$. Dann existiert ein $x \in \mathbb{Z}$ sodass
$x \equiv a_i \bmod m_i \ \forall\, 1 \le i \le n$
und x ist modulo $m_1 \cdot m_2 \cdot \dots \cdot m_n$ eindeutig bestimmt.

Beweis: Wir beweisen als erstes die Existenz mit Induktion über n.

Für $n=1$ wählen wir $x = a_1$.

Für den Induktionsschritt nehmen wir an, dass die Aussage für $n-1$ gilt.

Es gilt auch $ggT(m_1, m_2 \cdot m_3 \cdot \dots \cdot m_n) = 1$

also existieren $b, c \in \mathbb{Z}$ sodass $b m_1 + c m_2 \dots m_n = 1$ (S 1.3)

Sei $u = b m_1$

$v = c m_2 \dots m_n$

Dann ist $u \equiv 1 \mod m_2 \cdot \dots \cdot m_n$

$u \equiv 0 \mod m_1$

und $v \equiv 0 \mod m_2 \dots m_n$

$v \equiv 1 \mod m_1$

Nach Induktionsvoraussetzung existiert ein y sodass

$$y \equiv a_2 \mod m_2$$
$$y \equiv a_3 \mod m_3$$
$$\vdots$$
$$y \equiv a_n \mod m_n$$

Sei nun $x = yu + a_1 v$

Dann ist $x \equiv y \cdot 0 + a_1 \cdot 1 \mod m_1$

$\equiv a_1 \mod m_1$

und $x \equiv y \cdot 1 + a_1 \cdot 0 \mod m_2 \dots m_n$

$\equiv y \mod m_2 \dots m_n$

also $x \equiv y \mod m_i$

$\equiv a_i \mod m_i \quad \forall\ 2 \le i \le n$

Als letztes beweisen wir die Eindeutigkeit modulo $m_1 \cdot \ldots \cdot m_n$

Seien x, y zwei Lösungen

Dann ist $x - y \equiv 0 \mod m_i \quad \forall\, 1 \leq i \leq n$

also $m_i \mid x - y \quad \forall\, 1 \leq i \leq n$

$\Rightarrow m_1 \cdot \ldots \cdot m_n \mid x - y$ (da die m_i paarweise teilerfremd sind)

$\Rightarrow x \equiv y \mod m_1 \cdot \ldots \cdot m_n$ □

Eine äquivalente Formulierung des Satzes ist

Korollar 3.12: Seien $m_1, m_2, \ldots, m_n \in \mathbb{N}^+$ paarweise teilerfremd

Dann gilt

$$\mathbb{Z}/_{m_1 \cdot \ldots \cdot m_n \mathbb{Z}} \cong \mathbb{Z}/_{m_1 \mathbb{Z}} \times \mathbb{Z}/_{m_2 \mathbb{Z}} \times \ldots \times \mathbb{Z}/_{m_n \mathbb{Z}}$$

mit Isomorphismus

$$f : [x]_{m_1 \cdot \ldots \cdot m_n} \mapsto ([x]_{m_1}, [x]_{m_2}, \ldots, [x]_{m_n})$$

Beweis: Aufgabe

man muss zeigen: f ist eine Bijektion

$$f(x+y) = f(x) + f(y)$$

$$f(x \cdot y) = f(x) \cdot f(y)$$

Def: Eine prime Restklasse in einem Restklassenring R/I ist eine Restklasse $[a]_I$ die bezüglich Multiplikation invertierbar ist, d.h. $\exists b \in R$ sodass $[a]_I \cdot [b]_I = [1]_I$

Die Menge der primen Restklassen bezeichnen wir mit $(R/I)^\times$

Lemma 3.13: Sei $[a]_I, [b]_I \in (R/I)^\times$

dann ist $[a]_I \cdot [b]_I \in (R/I)^\times$

Insbesondere gilt

$[a]_I \cdot [b]_I = [0]_I \Rightarrow [a]_I$ oder $[b]_I$ ist nicht invertierbar.

Beweis: Seien $c, d \in R$ sodass $[a]_I \cdot [c]_I = [b]_I \cdot [d]_I = [1]_I$

Dann ist $([a]_I \cdot [b]_I) \cdot ([c]_I \cdot [d]_I) = ([a]_I \cdot [c]_I) \cdot ([b]_I \cdot [d]_I)$

$= [1]_I \cdot [1]_I$

$= [1]_I$

$[0]_I$ ist nicht invertierbar, also wenn $[a]_I \cdot [b]_I = [0]_I \notin (R/I)^\times$

dann ist $[a]_I \notin (R/I)^\times$ oder $[b]_I \notin (R/I)^\times$ □

was sind die primen Restklassen in $\mathbb{Z}/m\mathbb{Z}$?

Lemma 3.14: Sei $m \in \mathbb{N}^+$ und $a \in \mathbb{Z}$

$$[a]_m \in (\mathbb{Z}/m\mathbb{Z})^\times \iff (a, m) = 1$$

Insbesondere gilt für $p \in \mathbb{P}$, dass es in $\mathbb{Z}/p\mathbb{Z}$ genau $p-1$ prime Restklassen gibt.

Beweis: $\exists b \in \mathbb{Z}$ sodass $[a]_m [b]_m = [1]_m$

$\Leftrightarrow \exists b \in \mathbb{Z}$ sodass $ab \equiv 1 \mod m$

$\Leftrightarrow \exists b, c \in \mathbb{Z}$ sodass $ab = cm + 1$

$\Leftrightarrow \exists b, c \in \mathbb{Z}$ sodass $ba + (-c)m = 1$

$\Leftrightarrow (a, m) = 1$ (S 1.3) □

Kapitel 4: Kongruenzen

Def: Die Eulersche ϕ-Funktion ist definiert durch

$$\phi: \mathbb{N}^+ \to \mathbb{N}^+$$

$$m \mapsto \begin{cases} \left|(\mathbb{Z}/m\mathbb{Z})^\times\right| = \text{Anzahl der primen Restklassen in } \mathbb{Z}/m\mathbb{Z} & \text{für } m > 1 \\ 1 & \text{für } m = 1. \end{cases}$$

Lemma 4.1 Seien $m, n \in \mathbb{N}^+$ teilerfremd

Dann ist $\phi(mn) = \phi(m)\phi(n)$

Beweis: Die Aussage folgt z.B. aus Korollar 3.12 oder Lemma 3.14 □

Lemma 4.2: Sei $p \in \mathbb{P}$, $n \in \mathbb{N}^+$. Dann gilt $\phi(p^n) = (p-1)p^{n-1}$

Beweis: Es sind $\frac{p^n}{p} = p^{n-1}$ Zahlen aus $0, \dots, p^n - 1$ durch p teilbar

Alle anderen sind zu p teilerfremd ($p \in \mathbb{P}$)

Also sind $p^n - p^{n-1} = (p-1)p^{n-1}$ Zahlen aus $0, \dots, p^n - 1$

zu p teilerfremd

also gibt es $(p-1)p^{n-1}$ prime Restklassen in $\mathbb{Z}/p^n\mathbb{Z}$ (L 3.14) □

Korollar 4.3: $\forall\, n \in \mathbb{N}^+$

$$\phi(n) = \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} (p-1)\, p^{\nu_p(n)-1}$$

Diese Formel ist aber rein theoretisch

z.B. was ist $\phi(48395077)$

Ohne die Primfaktorzerlegung können wir die Formel nicht nutzen

Dieses „Problem" kann aber auch nützlich sein - die Sicherheit des kryptographische RSA-Verfahrens hängt davon ab.

$(48395077 = 6421 \cdot 7537)$