Def: Das direkte Produkt von Ringen

R, S Ringe, dann wird $R \times S := \{(r,s) \mid r \in R, s \in S\}$ wird zu einem Ring durch komponentenweise Addition und Multiplikation, d.h.

$$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) := (r_1 \cdot r_2, s_1 \cdot s_2)$$

Insbesondere: $(0,0)$ ist das neutrale Element der Addition

Falls R, S kommutativ sind, so ist $R \times S$ kommutativ,

Falls R, S Ringe mit Eins sind, dann ist $(1,1)$ neutrales Element der Multiplikation!

Achtung: Falls R, S Körper sind, dann ist $R \times S$ kein Körper,

da alle Elemente der Form $(0,s)$ bzw $(r,0)$ keine Inversen haben!

allgemeiner: $R_1, \ldots, R_n$ Ringe, dann wird $R_1 \times \ldots \times R_n := \{(r_1, \ldots, r_n) \mid r_i \in R_i\}$

durch komponentenweise Operationen zu einem Ring!

Satz: (Der chinesische Restsatz)

Seien $m_1, \dots, m_k$ paarweise teilerfremde Zahlen.

Dann ist

$$\varphi: \mathbb{Z}/(m_1 \cdot \dots \cdot m_k)\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$$

$$x + \underbrace{m_1 \cdot \dots \cdot m_k}_{=:m}\mathbb{Z} \longmapsto (x + m_1\mathbb{Z}, x + m_2\mathbb{Z}, \dots, x + m_k\mathbb{Z})$$

ein (Isomorphismus) zwischen Ringen.

Bew: Wohldefiniertheit & Homomorphie kann sich leicht überlegen.

$$|\mathbb{Z}/m\mathbb{Z}| = m = m_1 \cdot m_2 \cdot \dots \cdot m_k$$

$$! \quad \| \quad |\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}| = |\mathbb{Z}/m_1\mathbb{Z}| \cdot \dots \cdot |\mathbb{Z}/m_k\mathbb{Z}| = m_1 \cdot \dots \cdot m_k$$

Reicht zu zeigen, dass die Abbildung φ injektiv.

$x \in \mathrm{Kern}(\varphi)$: $x + m_1\mathbb{Z} = 0 + m_1\mathbb{Z} \iff x \in m_1\mathbb{Z} \iff m_1 \mid x$

$\vdots$

$x + m_k\mathbb{Z} = 0 + m_k\mathbb{Z} \iff m_k \mid x$

$\iff m_1 \cdot \dots \cdot m_k \mid x$ (da $m_1, \dots, m_k$ paarweise teilerfremd)

$\Rightarrow x + m\mathbb{Z} = 0 + m\mathbb{Z}$

d.h. φ injektiv.

□

Bsp:

6, 15, 10 sind teilerfremd, aber nicht paarweise teilerfremd

6, 15, 7 sind nicht paarweise teilerfremd

2, 3, 35 sind paarweise teilerfremd.

$2 \cdot 3 \cdot 5 \cdot 7 = 210$

$6 \mid 210$

$15 \mid 210$

$7 \mid 210$

aber $6 \cdot 15 \cdot 7 \nmid 210$

$\| \quad 630$

Folgerung: $\varphi: \mathbb{Z}/m_1 \cdots m_k\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ ist surjektiv,

d.h. für alle vorgegebenen Reste $r_1, \ldots, r_k \in \mathbb{Z}$ gibt es ein Zahl $x \in \mathbb{Z}$

mit: $x \equiv r_1 \pmod{m_1}$

$\vdots$

$x \equiv r_k \pmod{m_k}$

Bzw., falls $0 \le r_i < m_i$: x lässt Rest r_i bei der Division mit m_i

Falls x eine solche Zahl ist, dann sind sämtliche Lösungen $x + m_1 \cdots m_k\mathbb{Z}$

$= \varphi^{-1}((r_1, \ldots, r_k))$

Wie findet man x?

Fall $k=2$: Suche a_1, a_2 mit $a_1 m_1 + a_2 m_2 = 1$

Setze $b_2 := r_2 \cdot a_1 \cdot m_1 + r_1 \cdot a_2 \cdot m_2$

dann $b_2 \equiv r_1 \cdot a_2 \cdot m_2 \equiv r_1(1 - a_1 m_1) \pmod{m_1}$

$\equiv r_1 - r_1 \cdot a_1 \cdot m_1 \equiv r_1 \pmod{m_1}$

und $b_2 \equiv r_2 \cdot a_1 \cdot m_1 \equiv r_2(1 - a_2 m_2) \equiv r_2 \pmod{m_2}$

Berechne dann induktiv $b_{j+1} \equiv r_{j+1} \pmod{m_{j+1}}$

$b_{j+1} \equiv b_j \pmod{m_1 \cdot \ldots \cdot m_j}$

Dann $b_{j+1} \equiv b_j \equiv r_j \pmod{m_j}$

$\uparrow$ nach Induktion

Schließlich ist b_k eine der gesuchten Ergebnisse.

Folgerung aus dem chin. Restsatz:

Wenn $n = p_1^{k_1} \cdot \ldots \cdot p_\ell^{k_\ell}$ Primfaktorzerlegung, dann sind $p_1^{k_1}, p_2^{k_2}, \ldots, p_\ell^{k_\ell}$ paarweise teilerfremde Zahlen, deren Produkt n ergibt.

Also $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_\ell^{k_\ell}\mathbb{Z}$

und damit $\left(\mathbb{Z}/n\mathbb{Z}\right)^* \cong \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right)^* \times \ldots \times \left(\mathbb{Z}/p_\ell^{k_\ell}\mathbb{Z}\right)^*$

also $\varphi(n) = \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_\ell^{k_\ell}) = (p_1 - 1) \cdot p_1^{k_1 - 1} \cdot \ldots \cdot (p_\ell - 1) \cdot p_\ell^{k_\ell - 1}$

Beweis von $\varphi(p^k) = (p-1)p^{k-1}$: p Primzahl

x ist teilerfremd zu $p^k \iff p \nmid x$

Vielfache zwischen 1 und p^k werden von p geteilt? $\frac{p^k}{p} = p^{k-1}$ viele Zahlen

Also $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$ ☑

Diverses:

1) alter ISBN-Code $(a_1, \ldots, a_9, a_{10})$ ↑ Prüfziffer

Information

$a_1, \ldots, a_9 \in \{0, 1, \ldots, 9\}$ werden aufgefasst als Elemente in $\mathbb{F}_{11}$, $\mathbb{Z}/11\mathbb{Z}$

a_{10} wird so gewählt, dass $\sum_{j=1}^{10} j \cdot a_j = 0$ in $\mathbb{F}_{11}$

(falls $a_{10} = 10$, so schreibt man X dafür)

$$a_{10} = \frac{1}{10} \cdot \left(\sum_{j=1}^{9} j \cdot a_j \right)$$

Dieser Code erkennt ein falsch. Ziffer und die Vertauschung von zwei Ziffern

$(a_1, \dots, a_9, a_{10})$ $\xrightarrow{\text{i-Fehler}}$ $(a_1, \dots, a_i' \dots a_9, a_{10})$

$$\sum_{j=1}^{10} j \cdot a_j = 0 \qquad \sum_{\substack{j=1 \\ j \neq i}}^{10} j \cdot a_j + i \cdot a_i' = 0$$

Differenz: $i \cdot a_i - i \cdot a_i' = 0$

$$i \cdot (a_i - a_i') = 0$$

$i \neq 0$, $\mathbb{F}_{11}$ Körper $\Longrightarrow$ $a_i - a_i' = 0$

$a_i = a_i'$

$(a_1, \dots, a_9, a_{10})$ $\xrightarrow[\text{von } i \text{ und } k \text{ mit } i<k]{\text{Vertauschung}}$ $(a_1 \dots, a_k \dots a_i \dots a_9, a_{10})$

$$\sum_{j=1}^{10} j \cdot a_j = 0 \qquad \sum_{\substack{j=1 \\ j \neq i,k}}^{10} j \cdot a_j + i \cdot a_k + k a_i = 0$$

Differenz: $k \cdot a_k + i \cdot a_i - i \cdot a_k - k \cdot a_i$

$= k(a_k - a_i) - i(a_k - a_i)$

$= (k-i)(a_k - a_i) = 0 \Longrightarrow a_k = a_i$ ⇒

($k - i \neq 0$)

2) neuer ISBN-Code: zwölfstellige Zahl $(b_1, \dots, b_{12})$ + Prüfziffer b_{13} in $\mathbb{Z}/10\mathbb{Z}$

b_{13} wird so ausgerechnet, dass $b_1 + 3b_2 + b_3 + 3b_4 + \dots + 3b_{12} + b_{13} = 0$ in $\mathbb{Z}_{10}$

Hinweis: $3 \in \mathbb{Z}_{10}^*$, $3^{-1} = 7$

Code erkennt 1 Fehler und gewisse Vertauschungen

3) Quadrate von Zahlen $\neq 0$

$p = 11$

1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2	9^2	10^2
"	"	"	"	"	"	"	"	"	"
1	4	9	5	3	3	5	9	4	1

$\frac{p-1}{2}$ Quadratzahlen $\neq 0$

$n = 15$

1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2	9^2	10^2	11^2	12^2	13^2	14^2
"	"	"	"	"	"	"	"	"	"	"	"	"	"
1	4	9	1	10	6	4	4	6	10	1	9	4	1

$x^2 = 1$ hat 4 Lösungen!

5 Quadratzahlen $\neq 0$

$\frac{15-1}{2} = 7$

$n = 9$

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

3 Quadratzahlen $\neq 0$