Rivest
Shamir
Adleman

Beiträge der Algebra zu RSA

- große Primzahlen finden
  (probabilistische Tests, die u.a. kleinen Fermat ausnutzen)
- finde zu $\varphi(n)$ teilerfremdes e $\Longrightarrow$ $1 = a \cdot \varphi(n) + b \cdot e$
  (euklidischer Algorithmus) $\quad$ d: Rest von b
- Ausrechnen von Potenzen in $\mathbb{Z}_n$
  (abwechselndes Potenzieren und modulo-Rechnen)
- $d = e^{-1}$ in $\mathbb{Z}^*_{\varphi(n)}$

$$d \cdot e \equiv 1 \pmod{\varphi(n)}$$

(Darstellung des ggT als Linearkombination aus dem Eukl. Algor.)

Primzahlen finden?

$\pi(x)$ = Anzahl der Primzahlen in $\{1, 2, 3, \ldots, x\}$

Primzahlsatz

$$\pi(x) \sim \frac{x}{\ln(x)}$$

asymptotisch gleich, d.h. für $x \to \infty$ geht das Verhältnis gegen 1

Wieviele 100stellige Primzahlen gibt es ungefähr?

$10^{100} - 10^{99} = 9 \cdot 10^{99}$ Anzahl der 100stelligen Zahlen

$$\pi(10^{100}-1) - \pi(10^{99}-1) \approx \frac{10^{100}}{\ln(10^{100})} - \frac{10^{99}}{\ln(10^{99})} = \frac{10^{100}}{100 \cdot \ln(10)} - \frac{10^{99}}{99 \ln(10)}$$

$$\approx \frac{1}{\ln(10)} \cdot \left(10^{98} - 10^{97}\right) = \frac{9}{\ln(10)} \cdot 10^{97}$$ ungefähre Anzahl der 100stelligen PZ

Verhältnis etwa $\frac{1}{\ln(10) \cdot 100} \approx \frac{1}{230} = 0{,}004$

teilerfremde Zahlen finden?

Wieviele Zahlen in $\mathbb{Z}_m$ sind teilerfremd zu m?

Verhältnis $\frac{\varphi(m)}{m}$

$m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ Primfaktorzerlegung

$\varphi(m) = (p_1 - 1) p_1^{\alpha_1 - 1} \cdot \ldots \cdot (p_k - 1) \cdot p_k^{\alpha_k}$

$\frac{\varphi(m)}{m} = \frac{p_1 - 1}{p_1} \cdot \ldots \cdot \frac{p_k - 1}{p_k} = \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$

Der chinesische Restsatz

Ringe $R_1, \dots, R_k$

direktes Produkt $R_1 \times R_2 \times \dots \times R_k = \{ (r_1, r_2, \dots, r_k) \mid r_i \in R_i \}$

mit komponentenweiser Addition und Multiplikation, d.h.

$$(r_1, \dots, r_k) + (s_1, \dots, s_k) = (r_1 + s_1, r_2 + s_2, \dots, r_k + s_k)$$

ist wieder ein Ring mit Null $(0, 0, \dots, 0)$

und Eins $(1, 1, \dots, 1)$

und $-(r_1, \dots, r_k) = (-r_1, \dots, -r_k)$

Achtung: direktes Produkt von Körpern ist (für $k \geq 2$) kein Körper

denn z.B. $(0,1)$ hat kein Inverses, sondern ist Nullteiler

$(0,1) \cdot (1,0) = (0,0)$

Satz (10.7 im Skript) „Chinesischer Restsatz"

$m_1, \dots, m_k$ paarweise teilerfremde Zahlen

Dann ist

$$\mathbb{Z}/(m_1 \cdot \dots \cdot m_k)\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$$

$$a + m_1 \cdot \dots \cdot m_k\mathbb{Z} \longmapsto (a+m_1\mathbb{Z}, \dots, a+m_k\mathbb{Z})$$

ein Ringisomorphismus.

Beweis: Abbildung wohldefiniert?

$$a + m_1 \cdot \dots \cdot m_k\mathbb{Z} = b + m_1 \cdot \dots \cdot m_k\mathbb{Z} \overset{?}{\Leftarrow} a+m_i\mathbb{Z} = b+m_i\mathbb{Z}$$

$$\Updownarrow \qquad\qquad \Updownarrow$$

$$m_1 \cdot \dots \cdot m_k \mid a-b \implies m_i \mid a-b$$

(24h ~ 12 h)

Ringhomomorphismus: es reicht zu zeigen, dass die Komponentenabbildungen $\mathbb{Z}/m_1 \cdot \dots \cdot m_k\mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}$ Ringhomom. sind (Übung!)

2, 5, 77
sind paarweise teilerfremd, d.h. der ggT von je zen ist 1

6, 15, 10
sind zusammen teilerfremd, d.h. $\text{ggT}(6,15,10) = 1$
aber nicht paarweise
z.B. $\text{ggT}(6,15) = 3$

bijektiv? (bijektive Ringhomom. sind bereits Isomorphismen)

$$|\mathbb{Z}/m_1 \cdot \ldots \cdot m_k\mathbb{Z}| = m_1 \cdot \ldots \cdot m_k$$

$$|\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}| = |\mathbb{Z}/m_1\mathbb{Z}| \cdot \ldots \cdot |\mathbb{Z}/m_k\mathbb{Z}| = m_1 \cdot \ldots \cdot m_k$$

es reicht zu zeigen, dass der Homomorphismus injektiv ist.

Sei $x \in \ker(\text{Homom})$, d.h. $(x + m_1\mathbb{Z}, \ldots, x + m_k\mathbb{Z}) = (0, \ldots, 0)$

d.h. $m_1 \mid x, \ldots, m_k \mid x$

Da $m_1, \ldots, m_k$ paarweise teilerfremd, folgt $m_1 \cdot \ldots \cdot m_k \mid x$

$\Updownarrow$

$x + m_1 \cdot \ldots \cdot m_k\mathbb{Z} = 0 + m_1 \cdot \ldots \cdot m_k\mathbb{Z}$

d.h. $\ker$ ist trivial.

$\square$

$$\mathbb{Z}/m_1 \cdots m_k\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$$

$$\cup$$

ist inj. surjektiv, d.h. $(r_1 + m_1\mathbb{Z}, \dots, r_k + m_k\mathbb{Z})$

Falls $r_1, \dots, r_k \in \mathbb{Z}$ gegeben sind, dann ex $a \in \mathbb{Z}$

mit $a \equiv r_1 \pmod{m_1}$

$\vdots$

$a \equiv r_k \pmod{m_k}$

sogar $0 \leq a < m_1 \cdots m_k$

Mit eukl. Algorithmus (genauer: Darstellung des ggT)

kann man a konkret ausrechnen, z.B. $k=2$:

ex a_1, a_2 mit $a_1 \cdot m_1 + a_2 \cdot m_2 = 1$ ⟵

$a = r_2 \cdot a_1 m_1 + r_1 \cdot a_2 \cdot m_2$ tut's!

allgemein: Induktion, betrachten m_k u $m_1 \cdots m_{k-1}$ ...

(siehe Skript)

Insbesondere (wenn man Multiplikation vergisst, wird ein Ringisom. ein Gruppenisom.)

$m_1, \dots, m_k$ paarweise teilerfremd

$$\mathbb{Z}/m_1 \cdots m_k\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$$

zyklisch — direktes Produkt zyklischer Gruppen

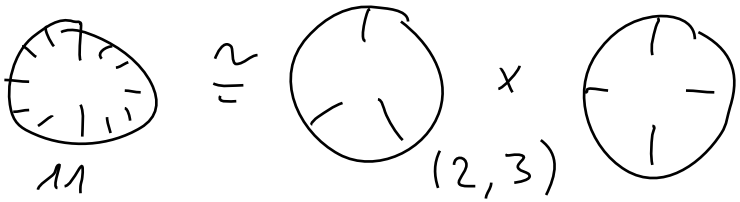
Umgekehrt: m_1, m_2 nicht teilerfremd, dann ist $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ nicht zyklisch

---

$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ Primfaktorzerlegung, dann sind

$m_1 = p_1^{\alpha_1}, \dots, m_k = p_k^{\alpha_k}$ paarweise teilerfremd

Dann $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$



daraus folgt

$$(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^*$$

also $\varphi(m) = \underbrace{\varphi(p_1^{\alpha_1}) \cdot \dots \cdot \varphi(p_k^{\alpha_k})} = (p_1-1)p_1^{\alpha_1-1} \cdot \dots \cdot (p_k-1)p_k^{\alpha_k-1}$

$$= p_1^{\alpha_1} - \frac{p_1^{\alpha_1}}{p_1}$$

$$= p_1^{\alpha_1} - p_1^{\alpha_1-1}$$

$$= (p_1-1)p_1^{\alpha_1-1}$$

ohne Beweis:

- Wenn $p>2$ Primzahl, dann $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \cong \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z}$
  $\cong \mathbb{Z}/(p-1)p^{\alpha-1}$ zyklisch
- $\mathbb{Z}/2\mathbb{Z}^*$ ist triviale Gruppe

  $\alpha \geq 2$ $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\cdot\mathbb{Z}$ nicht zyklisch für $\alpha \geq 3$