24.01.18

Mittwoch, 17. Januar 2024 11:42

Definition 184 Die Eulersche φ-Funktion ist die Abb.

bildung $\varphi : \mathbb{N} \to \mathbb{N}$, $\varphi(n) = |\{q \in \mathbb{N} \mid ggT(q,n) = 1\}$ $\hat{=}$ Anzahl an n teilerfremde Zahlen $< n$

Satz 185 Für teilerfremde Zahlen $m, n \in \mathbb{N}$ gilt

$\varphi(m \cdot n) = \varphi(n) \cdot \varphi(n)$.

Beweis unten, aber nur für Primzahlen $\square$

Lemma 186 Es seien p, q Primzahlen und

$x \equiv 1 \mod p$, $x \equiv 1 \mod q$. Dann gilt $x \equiv$

$\equiv 1 \mod pq$

Beweis $x \equiv 1 \mod p \Rightarrow x = 1 + Np$, $N \in \mathbb{N}$

$x \equiv 1 \mod q \Rightarrow x = 1 + Mq$, $M \in \mathbb{N}$

$\Rightarrow Np = Mq \Rightarrow \frac{N}{q} p \in \mathbb{Z}$, $\frac{M}{p} q \in \mathbb{Z}$

prim

$\Rightarrow q \mid N$, $p \mid M \Rightarrow N = q \cdot N'$, $M = p \cdot M'$

$\Rightarrow Np = qpN' \Rightarrow x = 1 + qpN'$

$\Rightarrow \quad X \equiv 1 \mod qp$ □

Satz 187 (Euler) Sei $n = pq$ und $p \neq q$ Primzahlen. Dann gilt für alle $k, m \in \mathbb{N}$:

$$m^{k \cdot \varphi(n) + 1} \equiv m \mod n$$

Beweis Zunächst gilt: $\varphi(pq) \overset{185}{=} \varphi(p)\varphi(q)$

$\overset{\text{Def}}{=} (p-1)(q-1)$. Damit berechnet man

$$m^{k\varphi(n)} \equiv m^{k(p-1)(q-1)} \equiv \left(m^{p-1}\right)^{k(q-1)}$$

$$\overset{\text{Sv. Fermat}}{\equiv} 1^{k(q-1)} \equiv 1 \mod p$$

Analog ergibt sich $m^{k\varphi(n)} \equiv 1 \mod q$. Daher folgt $m^{k\varphi(n)} \equiv 1 \mod pq \equiv 1 \mod n$

also $m^{k\varphi(n)+1} \equiv m \mod n$ □

RSA-Algorithmus

1) Wähle ein <u>RSA-Modul</u> $n = p \cdot q$, mit $p \neq q$ Primzahlen. In den Anwendungen sind p, q sehr groß. Berechne $\varphi(n) = (p-1)(q-1)$

2) Wähle $e \in \mathbb{N}$ mit $\text{ggT}(e, \varphi(n)) = 1$ und be-

stimme mit dem erweiterten euklidischen Algorithmus ein $d \in \mathbb{Z}$ mit $e \cdot d \equiv 1 \bmod \varphi(n)$ also gilt $e \cdot d = 1 + k \cdot \varphi(n)$ für ein $k \in \mathbb{Z}$.

3) Veröffentliche (e, n) als öffentlichen Schlüssel und behalte (d, n) als privaten Schlüssel geheim.

4) Stelle die zu verschlüsselnde Nachricht als Zahl $m \in \mathbb{N}$ dar mit $m < n$.

5) a) Nachrichtenverschlüsselung

Wende auf m das RSA-Verschlüsselungsschema an: Der Sender verschlüsselt m mithilfe des öffentlichen Schlüssels des Empfängers zu $c := m^e \bmod n$. Dann versendet der Sender die Nachricht c. Diese wird vom Empfänger mit seinem privaten Schlüssel (d, n) entschlüsselt indem er $c^d \bmod n$ berechnet:

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\varphi(n)+1} \equiv m \bmod n$$

Also ergibt sich der Klartext m. ($m < n$!)

56) Authentifizierung: Wende auf m das RSA-Signaturschema an: Der Signierende erstellt seinen privaten Schlüssel (d, n), das signierte Dokument $sig(m) := m^d \bmod n$ und übermittelt m und $sig(m)$. Der Empfänger prüft die Signatur, indem er $(sig(m))^e \bmod n$ berechnet und mit m vergleicht. Stimmen beide überein, so wurde m mit dem privaten Schlüssel signiert, denn:

$$(sig(m))^e = (m^d)^e = m^{de} = m^{k\varphi(n)+1} = m \bmod n$$

Beispiel 188 Sender wählt

→ wählt $p := 11$, $q := 5 \Rightarrow n = 55$, $\varphi(n) = 40$

→ wählt $e = 7$, $ggT(7, 40) = 1$

→ öffentlicher Schlüssel ist $(7, 55) =$

→ wählt Nachricht $m = 8 < 55 = n$

→ verschlüsselt $m = 8$ mit $(e, n) = (7, 55)$

$$c = 8^7 \bmod 55 \equiv (64)^3 \cdot 8 \bmod 55$$

$$\equiv 9^3 \cdot 8 \bmod 55 \equiv 81 \cdot 72 \bmod 55$$

$$\equiv 26 \cdot 17 \bmod 55 \equiv 442 \bmod 55$$

$$\equiv 2 \bmod 55$$

⟶ übermittelt $c = 2$ und $(7, 55)$ an Empfänger

Empfänger

→ bestimmt privaten Schlüssel (d, n) aus

$e \cdot d \equiv 1 \bmod 40$ mit dem euklidischen Algorithmus:

$$40 = 7 \cdot 5 + 5$$
$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$

$$\Rightarrow 1 = 5 - 2 \cdot 2 = 5 - 2(7 - 5 \cdot 1) = 3 \cdot 5 - 2 \cdot 7$$

$$= 3 \cdot (40 - 7 \cdot 5) - 2 \cdot 7 = 3 \cdot 40 + (-17) \cdot 7$$

$$\Rightarrow 1 = 3 \cdot \varphi(n) + (-17) \cdot e \Rightarrow d = -17 \bmod 40$$

$$\Rightarrow d \equiv 23 \bmod 40$$

$\Rightarrow$ $(23, 55)$ ist privater Schlüssel

$\rightarrow$ entschlüsselt $c = 2$ zu

$$c^d \equiv 2^{23} \equiv (2^6)^3 2^5 \equiv (64)^3 \cdot 32$$

$$\equiv 9^3 \cdot 32 \equiv 81 \cdot 288 \equiv 26 \cdot 13$$

$$\equiv 338 \mod 55$$

$$\equiv 8 \mod 55 \equiv m \mod 55$$ □

Bemerkung 185 zur Sicherheit des RSA-Verfahrens.

Theoretisch kann man den privaten aus dem öffent

Beweis Satz 185. Es seien $m = p$, und $n = q$ Primzahlen. Zu zeigen ist $\varphi(pq) = \varphi(p)\varphi(q)$. Wir wissen sofort dass $\varphi(p) = p-1$, denn $\{1, \dots, p-1\}$ sind zu p teilerfremd. Es ist $\mathbb{Z}_p$ ein Körper daher sind $(\mathbb{Z}_p)^* := \{1, \dots, p-1\} \subset \mathbb{Z}_p$ die invertierbaren Elemente in $\mathbb{Z}_p$. Genauso gilt $\varphi(pq) =$ Anzahl invertierbare Elemente in $\mathbb{Z}_{pq}$. Wir betrachten ein Abbil-

Elemente in $\mathbb{Z}_{pq}$. Wir betrachten eine Abbildung

$$\phi : (\mathbb{Z}_{pq})^* \to (\mathbb{Z}_p)^* \times (\mathbb{Z}_q)^*$$
$$[x]_{pq} \longmapsto ([x]_p, [x]_q)$$

Zuerst zeigen wir, dass ϕ wohldefiniert ist, also zz: $[x]_p \in (\mathbb{Z}_p)^*$, $[x]_q \in (\mathbb{Z}_q)^*$. Es gilt: $[x]_{pq}$ invertierbar in $\mathbb{Z}_{pq} \Rightarrow ggT(x, pq) = 1 \Rightarrow$

$\exists M, N \in \mathbb{Z}: 1 = xN + pqM \Rightarrow Nx \equiv 1 \mod p$

und $Nx \equiv 1 \mod q \Rightarrow [x]_p \in (\mathbb{Z}_p)^*$, $[x]_q \in (\mathbb{Z}_q)^*$

Nun zeigen wir dass ϕ injektiv ist: Es sei dazu

$\phi([x]_{pq}) = \phi([y]_{pq}) \Rightarrow [x]_p = [y]_p$, $[x]_q = [y]_q$

$\Rightarrow x \equiv y \mod p$, $x = y \mod q \Rightarrow \exists K, L \in \mathbb{Z}$:

$x = y + pL$, $x = y + qK \Rightarrow pL = qK \Rightarrow$

$q \mid L$, $p \mid K \Rightarrow L = qL'$, $K = pK' \Rightarrow pL = pqL'$

$\Rightarrow x = y + pqL' \Rightarrow x \equiv y \mod pq \Rightarrow$

$[x]_{pq} = [y]_{pq}$

Nun zeigen wir, dass ϕ surjektiv ist. Sei dazu $[x]_p$

$\in (\mathbb{Z}_p)^*$ und $[y]_q \in (\mathbb{Z}_q)^*$. Zu zeigen ist: es gibt $[z] \in (\mathbb{Z}_{pq})^*$ mit $\phi([z]) = ([x]_p, [y]_q)$. Wegen $ggT(p,q) = 1$ gibt es $K, L \in \mathbb{Z}$ mit: $1 = pK + qL$.

Setze $\alpha := x - y$. Dann: $x - y = \alpha = p\underbrace{(K\alpha)}_{=:-T} + q\underbrace{(L\alpha)}_{=:S}$

$\Rightarrow x + pT = y + qS =: z \in \mathbb{Z}$

Also gilt: $z \equiv x \bmod p \Rightarrow [z]_p = [x]_p$

$z \equiv y \bmod q \Rightarrow [z]_q = [y]_q$

Zu zeigen bleibt $[z]_{pq} \in (\mathbb{Z}_{pq})^*$, also reicht es zu zeigen dass $ggT(z, pq) = 1$. Angenommen: $p \mid z$

$\Rightarrow p \mid x + pT \Rightarrow p \mid x$ im $\mathbb{Z}$ da $ggT(x,p) = 1$

Also $p \nmid z$. Analog folgt $q \nmid z$, also $ggT(pq, z) = 1$

Insgesamt ist ϕ also bijektiv, daher hat $(\mathbb{Z}_{pq})^*$ genau so viele Elemente wie $(\mathbb{Z}_p)^* \times (\mathbb{Z}_q)^*$. Das sind aber $(p-1)\cdot(q-1)$ Stück. Also $\varphi(pq) =$

$= |(\mathbb{Z}_{pq})^*| = (p-1)(q-1) = \varphi(p)\,\varphi(q)$. $\square$