

Übungsblatt № 12

Aufgabe 77

Seien p_1, \dots, p_k paarweise verschiedene Primzahlen und $e_i \in \mathbb{N}$ mit $i = 1, \dots, k$. Zeigen Sie, dass für

$$n = \prod_{i=1}^k p_i^{e_i}$$

die Gleichung

$$\varphi(n) = \prod_{i=1}^k (p_i - 1)p_i^{e_i-1}$$

gilt.

Lemma 1. Es seien $p, q \in \mathbb{N}$ mit $\text{ggT}(p, q) = 1$, dann gilt

$$\varphi(pq) = \varphi(p)\varphi(q)$$

Beweis. Es seien $T = \{t_1, \dots, t_l\}$ die zu p teilerfremden Zahlen und $S = \{s_1, \dots, s_m\}$ die zu q teilerfremden Zahlen. Bekanntermaßen gilt $|T| = \varphi(p)$ und $|S| = \varphi(q)$. Wir wissen ebenfalls, dass alle Produkte $t_i s_j$ teilerfremd zu pq sind. Insgesamt gibt es $|T \times S| = |T| \cdot |S| = \varphi(p)\varphi(q)$ solcher Produkte, womit $\varphi(pq) = \varphi(p)\varphi(q)$ folgt. \square

Aus diesem Lemma ergibt sich durch eine triviale Induktion, dass für paarweise teilerfremde Zahlen p_1, \dots, p_k gilt

$$\varphi\left(\prod_{i=1}^k p_i\right) = \prod_{i=1}^k \varphi(p_i)$$

Wir führen nun einen Induktionsbeweis, dass $\varphi(p^e) = (p-1)p^{e-1}$ gilt. Für $e = 1$ folgt $\varphi(p^1) = (p-1)p^0 = p-1$. Da p prim ist, gilt die Aussage. Für $e \rightarrow e-1$ betrachten wir nun $\{1, 2, \dots, p^e\}$. Offensichtlich teilen nur die Vielfachen von p den Wert p^e , diese sind also $\{p, 2p, 3p, \dots, p^{e-1}p\}$. Es gibt somit p^{e-1} Vielfache von p . Von den gesamt p^e Zahlen in $\{1, \dots, p^e\}$ werden also genau p^{e-1} nicht für $\varphi(p^e)$ verwendet, womit sich $\varphi(p^e) = p^e - p^{e-1} = (p-1)p^{e-1}$ ergibt.

Nun ist die gesuchte Aussage trivial nachzuweisen, da Primzahlpotenzen verschiedener Primzahlen immer noch teilerfremd sind. Damit gilt

$$\varphi(n) = \varphi\left(\prod_{i=1}^k p_i^{e_i}\right) = \prod_{i=1}^k \varphi(p_i) = \prod_{i=1}^k (p_i - 1)p_i^{e_i-1}$$

Aufgabe 78

Beweisen oder widerlegen Sie. Für jedes $n \in \mathbb{N}$ gilt

$$n = \sum_{\substack{k \in \mathbb{N} \\ k|n}} \varphi(k)$$

Lemma 2. Seien $n, k \in \mathbb{N}$, dann gilt

$$1 + \sum_{j=0}^{k-1} n^j (n-1) = n^k$$

Beweis. Wir führen eine Induktion nach k . Für $k = 1$ gilt natürlich

$$1 + \sum_{j=0}^0 n^j(n-1) = 1 + n^0(n-1) = 1 + n - 1 = n = n^1$$

Damit folgt nun

$$1 + \sum_{j=0}^k n^j(n-1) = 1 + n^k(n-1) + \sum_{j=0}^{k-1} n^j(n-1) = 1 + n^k(n-1) + n^k - 1 = 1 + n^k(n-1+1) = n^{k+1}$$

□

Eine direkte Folgerung hiervon ist natürlich

$$\sum_{j=0}^e \varphi(p^j) = 1 + \sum_{j=0}^{e-1} (p-1)p^j = p^e$$

für $p \in \mathbb{P}$. Es sei nun

$$n = \prod_{i=1}^k p_i^{e_i}$$

die Primfaktorzerlegung von n . Wir führen eine Induktion nach k . Mit $k = 1$, also $n = p_1^{e_1}$, gilt natürlich

$$\sum_{\substack{d \in \mathbb{N} \\ d|n}} \varphi(d) = 1 + \sum_{j=0}^{e_1-1} (p_1 - 1)p_1^j = p_1^{e_1}$$

Im Induktionsschritt sei nun $n' = \prod_{j=1}^{k-1} p_j^{e_j}$. Dann ist $n = p_k^{e_k} n'$, womit für $d \in \mathbb{N}$ mit $d|n'$ folgt, dass $p_k^l d|n$ gilt, für $l = 0, \dots, e_k$. Daraus folgt, unter der Verwendung, dass $\text{ggT}(p_k, d) = 1$ mit $d|n'$ gilt:

$$\begin{aligned} \sum_{\substack{d \in \mathbb{N} \\ d|n}} \varphi(d) &= \sum_{\substack{d \in \mathbb{N} \\ d|n'}} \sum_{j=0}^{e_k} \varphi(p_k^j d) = \sum_{\substack{d \in \mathbb{N} \\ d|n'}} \sum_{j=0}^{e_k} \varphi(d) \varphi(p_k^j) = \sum_{\substack{d \in \mathbb{N} \\ d|n'}} \varphi(d) \sum_{j=0}^{e_k} \varphi(p_k^j) \\ &= \sum_{\substack{d \in \mathbb{N} \\ d|n'}} \varphi(d) p_k^{e_k} = p_k^{e_k} \sum_{\substack{d \in \mathbb{N} \\ d|n'}} \varphi(d) = p_k^{e_k} n' = n \end{aligned}$$

Aufgabe 79

Für gegebene $a, b \in \mathbb{N}$ sei $M_{a,b} = \{a\mu + b\lambda \mid \mu, \lambda \in \mathbb{Z}\}$. Geben Sie eine notwendige und hinreichende Bedingung dafür an, dass $M_{a,b} = \mathbb{Z}$ gilt.

Eine hinreichende Bedingung für $M_{a,b} = \mathbb{Z}$ ist, dass $1 \in M_{a,b}$, denn gibt es $\lambda_0, \mu_0 \in \mathbb{Z}$ mit $a\lambda_0 + b\mu_0 = 1$ folgt somit für $k \in \mathbb{Z}$:

$$k = k \cdot 1 = k(a\lambda_0 + b\mu_0) = ak\lambda_0 + bk\mu_0 \in M_{a,b}$$

Eine notwendige Bedingung ist somit, dass $\text{ggT}(a, b) = 1$, denn dann gilt nach dem Lemma von Bézout, dass es $\lambda_0, \mu_0 \in \mathbb{Z}$ gibt, mit $a\lambda_0 + b\mu_0 = 1$.

Aufgabe 83

Zeigen Sie, dass man bei dem RSA-Verfahren aus der Kenntnis der öffentlichen Schlüssel n und k und einer der beiden Primzahlen p und q den geheimen Schlüssel ℓ berechnen kann.

Wir erinnern uns, dass $n = pq$ gilt, dann ist k derart gewählt, dass $\text{ggT}(k, \varphi(n)) = 1$ gilt. Für ℓ folgt dann $k\ell \equiv 1 \pmod{\varphi(n)}$. Kennen wir nun oBdA p , dann können wir $q = \frac{n}{p}$ berechnen. Mit q können wir dann auch $\varphi(n) = (p-1)(q-1)$ bestimmen und dann mittels des euklidischen Algorithmus auch ℓ .