Satz: Die Eulersche φ-Funktion (*Euler's totient*) ist *multiplikativ*; d.h.:

$$(m,n) = 1 \quad \Rightarrow \quad \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

Beweis:

Wir setzen die natürlichen Zahlen m und n als *teilerfremd* voraus (d.h. $(m,n) = 1$) und betrachten die Linearkombinationen $am + bn$ mit $a, b \in \mathbb{Z}$.

Beinahe trivial ist die folgende Bemerkung:

$$a_1 m + b_1 n \equiv a_2 m + b_2 n \pmod{mn} \quad \Leftrightarrow \quad a_1 \equiv a_2 \pmod{n} \ \wedge \ b_1 \equiv b_2 \pmod{m} \qquad \textbf{(1)}$$

Denn die linke Beziehung bedeutet, dass $(a_1 - a_2)m + (b_1 - b_2)n$ Vielfaches von mn ist; und dies ist wegen $(m,n) = 1$ gleichbedeutend mit $n \mid (a_1 - a_2) \ \wedge \ m \mid (b_1 - b_2)$.

Als zweites bemerken wir:

$$(am + bn, mn) = 1 \quad \Leftrightarrow \quad (a,n) = 1 \ \wedge \ (b,m) = 1 \qquad \textbf{(2)}$$

Denn enthält a einen echten Teiler von n oder b einen von m, ist dieser zugleich Teiler von $am + bn$ und von mn; dies zeigt „=>“. Umgekehrt müsste ein gemeinsamer Teiler von mn und $am + bn$, sofern Teiler von m, auch Teiler von bn, also von b sein, und sofern Teiler von n, auch Teiler von am, also von a. Das zeigt „<=“.

Nach (1) durchläuft $am + bn$ einen vollständigen Restesatz modulo mn, wenn a einen solchen modulo n und b einen modulo m durchläuft. Nach (2) bedeutet dies $\varphi(mn) = \varphi(m)\varphi(n)$. ■

Beweis II:

Sei wieder $(m,n) = 1$. Nach dem Chinesischen Restesatz entspricht jedem Paar $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ genau ein $c \in \mathbb{Z}_{mn}$ mit $a \equiv c \pmod{m}$ und $b \equiv c \pmod{n}$ und umgekehrt natürlich jedem c genau ein Paar (a,b). Mit anderen Worten:

$$\Phi: \ c \mapsto (c \bmod m, \ c \bmod n) \quad (c \in \mathbb{Z}_{mn})$$

definiert eine *Bijektion* von $\mathbb{Z}_{mn}$ auf $\mathbb{Z}_m \times \mathbb{Z}_n$.

Es ist sogar eine *Isomorphie* vom Restklassenring $\mathbb{Z}_{mn}$ mit der üblichen Restklassen-Addition und -Multiplikation auf den Ring $\mathbb{Z}_m \times \mathbb{Z}_n$ mit *komponentenweiser* Restklassen-Addition und -Multiplikation, da

$$(a+b) \bmod m \equiv a \bmod m + b \bmod m \pmod{m}, \ \ (a \cdot b) \bmod m \equiv a \bmod m \cdot b \bmod m \pmod{m}$$

sowie die analogen Beziehungen bzgl. des Moduls n; dies sind ja die grundlegenden Identitäten des Restklassenrechnens. Das neutrale Element der komponentenweisen Multiplikation in $\mathbb{Z}_m \times \mathbb{Z}_n$ ist $(1,1) = \Phi(1)$.

Nun gibt es zu jedem $c \in \mathbb{Z}_{mn}^*$ genau ein multiplikatives Inverses $c^{-1} \bmod mn$. Mit $\Phi(c) = (c_1, c_2)$ gilt dann $\Phi(c^{-1} \bmod mn) = (c_1^{-1} \bmod m, c_2^{-1} \bmod n)$, da Φ ja eine Isomorphie ist. Sind umgekehrt $c_1 \in \mathbb{Z}_m^*$ und $c_2 \in \mathbb{Z}_n^*$ und d_1 bzw. d_2 ihre multiplikativen Inversen, so ist aus Isomorphiegründen $d = \Phi^{-1}\big((d_1, d_2)\big)$ das multiplikativ Inverse zu $c = \Phi^{-1}\big((c_1, c_2)\big)$.

Fazit: Zu jedem $c \in \mathbb{Z}_{mn}^*$ gibt es genau ein Paar $(c_1, c_2) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ und umgekehrt. Und das bedeutet nichts anderes als $\varphi(mn) = \varphi(m)\,\varphi(n)$. ■

(Wurde der *Isomorphie*gehalt des Chin. Restesatzes schon *vorher* genau behandelt, *beginnt* der zweite Beweis bei „Nun gibt es zu jedem...“. Anderenfalls ist der *erste* Beweis der einfachere.)

Die Multiplikativität ist der Schlüssel zur generellen Berechnung der φ-Funktion, da $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ für Primzahlen p sich durch eine triviale Überlegung ergibt: Nur Vielfache von p, also $p, 2p, 3p, \ldots, p^{\alpha-1}p$ sind nicht teilerfremd zu p^α, also in $\mathbb{Z}_{p^\alpha}$ genau $p^{\alpha-1}$ Zahlen. Es folgt also

$$\boldsymbol{\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})\cdots(p_k^{\alpha_k} - p_k^{\alpha_k-1}) = n(1-1/p_1)\cdots(1-1/p_k)} \qquad \boldsymbol{(*)}$$

mit der Primfaktorzerlegung $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$.

Z.B.: $\varphi(100) = \varphi(2^2\cdot 5^2) = (4-2)(25-5) = 40$, $\varphi(1000) = (8-4)(125-25) = 400$, $\varphi(101) = 100$, $\varphi(1001) = \varphi(7\cdot 11\cdot 13) = 6\cdot 10\cdot 12 = 720$.

(Da nicht durch $2, 3, 5, 7$ teilbar, ist 101 Primzahl.)

Ergänzende Bemerkungen:

a) Da offensichtlich $p^\alpha - p^{\alpha-1} \mid p^\beta - p^{\beta-1}$ für $0 < \alpha \le \beta$, gilt $\boldsymbol{m \mid n \Rightarrow \varphi(m) \mid \varphi(n)}$.

b) Es gilt $\boldsymbol{\sum_{d\mid n} \varphi(d) = n}$.

Beweis: Wir zeigen es zunächst für $n = p^\alpha$. Die Teiler von n sind in diesem Spezialfall einfach $1, p, p^2, \ldots, p^\alpha$, also $\sum_{d\mid n} \varphi(d) = 1 + \sum_{i=1}^{\alpha}(p^i - p^{i-1}) = p^\alpha = n$.

Nun zeigen wir:

Die Funktion $\Phi(n) := \sum_{d\mid n} \varphi(d)$ ist *multiplikativ*, d.h. $\Phi(mn) = \Phi(m)\,\Phi(n)$ für $(m,n) = 1$.

Gegeben zwei teilerfremde natürliche Zahlen m und n, seien $d_1 = 1, d_2, \ldots, d_k = m$ bzw. $t_1 = 1, t_2, \ldots, t_l = n$ jeweils ihre verschiedenen Teiler. Dann sind die verschiedenen Teiler von mn alle verschiedenen Produkte $d_i t_j$ $(1 \le i \le k,\ 1 \le j \le l)$. Also

$$\Phi(mn) = \sum_{i=1}^{k}\sum_{j=1}^{l}\varphi(d_i t_j) = \sum_{i=1}^{k}\sum_{j=1}^{l}\varphi(d_i)\varphi(t_j) = \Big(\sum_{i=1}^{k}\varphi(d_i)\Big)\Big(\sum_{j=1}^{l}\varphi(t_j)\Big) = \Phi(m)\Phi(n).$$

Da jedes n als Produkt von Potenzen verschiedener Primzahlen darstellbar ist, ergibt sich praktisch unmittelbar: $\Phi(n) = n$ $(n \in \mathbb{N})$. ■

(Beim Multiplikativitätsbeweis für Φ haben wir von φ *nur* die Multiplikativität benutzt: Also ist $\Phi(n) := \sum_{d\mid n}\varphi(d)$ multiplikativ für *jede beliebige multiplikative* zahlentheoretische Funktion φ.)

c) Die Isomorphie $\Phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ mit $(m,n) = 1$ (und allgemeiner die Isomorphie $\Phi : \mathbb{Z}_{m_1\cdots m_n} \to \mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_n}$ mit $(m_1,\ldots,m_n) = 1$) aus „Beweis II“ hat nicht nur eine theoretische, sondern genauso eine *rechenpraktische* Bedeutung. Denn sie impliziert ja, dass man das ganzahlige Modulo-Rechnen in einem sehr großen Restklassenring *parallelisieren* kann, indem man in mehreren viel kleineren Restklassenringen gleichzeitig rechnet. In dem Zusammenhang ist auch noch folgende bemerkenswerte Identität praktisch nützlich:

$$\boldsymbol{\big(2^m - 1,\ 2^n - 1\big) = 2^{(m,n)} - 1}$$

Beweis der Identität:

Generell offensichtlich $(m,n) = (m + k\cdot n, n)$ $(k \in \mathbb{Z})$. Also mit $m = kn + r$ (Division mit Rest) $(2^m - 1,\ 2^n - 1) = \big(2^m - 1 - 2^{m-n}(2^n - 1),\ 2^n - 1\big) = \big(2^{m-n} - 1,\ 2^n - 1\big) = \cdots = \big(2^r - 1,\ 2^n - 1\big)$. Durch Fortsetzung mit abwechselnd vertauschten Rollen (Euklid= „Wechselwegnahme“) gelangt man zu $\big(2^{(m,n)} - 1, 2^{(m,n)\cdot q} - 1\big)$ (der *vorletzte* von 0 verschiedene Rest ist ein Vielfaches des *letzten*, des ggT (m,n)), und $(2^{(m,n)})^q - 1 = (2^{(m,n)} - 1)\big(1 + 2^{(m,n)} + \cdots + (2^{(m,n)})^{q-1}\big)$. ■

d) Zwei etwas *direktere* Herleitungen der φ-*Berechnungsformel* **(∗)**

Erste Herleitung: Dies ist eine Variante von „Beweis II“, nun aber nicht auf die *Multiplikativität* von φ ausgerichtet, sondern direkt auf (∗).

Sei $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ die Primfaktorzerlegung von n. Infolge des Chinesischen Restesatzes entspricht jedem $a \in \mathbb{Z}_n$ *umkehrbar eindeutig* ein k-Tupel

$$\left(a \mod p_1^{\alpha_1}, \ldots, a \mod p_k^{\alpha_k}\right) \in \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} .$$

Im Falle $a \in \mathbb{Z}_n^*$ muss dabei auch $a \bmod p_i^{\alpha_i} \in \mathbb{Z}^*_{p_i^{\alpha_i}}$ $(1 \le i \le k)$ gelten und umgekehrt; denn a ist ja dann und nur dann teilerfremd zu n, wenn es teilerfremd ist zu allen p_i. Das aber bedeutet: Wenn a ganz $\mathbb{Z}_n^*$ durchläuft, durchläuft $\left(a \mod p_1^{\alpha_1}, \ldots, a \mod p_k^{\alpha_k}\right)$ ganz $\mathbb{Z}^*_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}^*_{p_k^{\alpha_k}}$. D.h.:

$$\boldsymbol{\varphi(n) = \left|\mathbb{Z}_n^*\right| = \left|\mathbb{Z}^*_{p_1^{\alpha_1}}\right| \cdots \left|\mathbb{Z}^*_{p_k^{\alpha_k}}\right|}$$

Da unter den Zahlen $1, 2, \ldots, p^\alpha$ nur die Vielfachen von p, also die $p^{\alpha-1}$ Zahlen $p, 2p, 3p, \ldots, p^{\alpha-1}p$, *nicht* teilerfremd sind zu p^α, gilt $\left|\mathbb{Z}^*_{p^\alpha}\right| = \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Damit folgt insgesamt:

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})\cdots(p_k^{\alpha_k} - p_k^{\alpha_k-1}) = p_1^{\alpha_1}(1-\tfrac{1}{p_1})\cdots p_k^{\alpha_k}(1-\tfrac{1}{p_k}) = n(1-\tfrac{1}{p_1})\cdots(1-\tfrac{1}{p_k})$$

Zweite Herleitung: Gegeben die Primfaktorzerlegung $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ von n, sei A_i die Menge der durch p_i teilbaren unter den Zahlen $1, 2, \ldots, n$; die Menge der zu n *nicht* teilerfremden dieser Zahlen ist $A_1 \cup \cdots \cup A_k$, und es gilt $\varphi(n) = n - \left|A_1 \cup \cdots \cup A_k\right|$. Mit $A_i = \{p_i, 2\cdot p_i, \ldots, \frac{n}{p_i}\cdot p_i\},\ |A_i| = \frac{n}{p_i}$, $A_i \cap A_j = \{p_ip_j, 2\cdot p_ip_j, \ldots, \frac{n}{p_ip_j}\cdot p_ip_j\},\ |A_i \cap A_j| = \frac{n}{p_ip_j}$, usw., folgt (*Inklusions-Exklusions-Formel*)

$$\left|A_1 \cup \cdots \cup A_k\right| = n\Big(\sum \tfrac{1}{p_i} - \sum \tfrac{1}{p_{i_1}p_{i_2}} + \sum \tfrac{1}{p_{i_1}p_{i_2}p_{i_3}} - + \cdots + (-1)^{k-1}\tfrac{1}{p_1p_2\cdots p_k}\Big) = n\Big(1 - \big(1-\tfrac{1}{p_1}\big)\cdots\big(1-\tfrac{1}{p_k}\big)\Big)$$

und damit $\varphi(n) = n\big(1-\frac{1}{p_1}\big)\cdots\big(1-\frac{1}{p_k}\big)$.

Die letzte Herleitung kommt mit nur wenigen zahlentheoretischen Fakten aus, ist die schnellste, in gewissem Sinne eleganteste, aber sicher nicht die *aufschlussreichste*. Die zu Anfang gegebenen zwei Herleitungswege über die Multiplikativität vermitteln meines Erachtens mehr an unmittelbarem *Zusammenhangsverständnis* als die letzten beiden; der letzte Weg ist trotz seiner Kürze der unergiebigste, aber dennoch ein *typisches* Inklusions-Exklusions-Beispiel.