4. Die Sätze von Euler, Fermat und Wilson

Satz 46 Es sei $m \in \mathbb{N}$, $m \geq 2$ und $a \in \mathbb{Z}$. Äquivalent sind:

(i) $\exists x \in \mathbb{Z} : ax \equiv 1 \ (m)$,

(ii) $ggT(a,m) = 1$.

Beweis: (i) $\Rightarrow$ (ii) Aus $ax \equiv 1 \ (m)$ folgt (wegen Satz 36), dass $\exists k \in \mathbb{Z} : ax = 1 + km$. Da $ggT(a,m) \mid a$ und $ggT(a,m) \mid m$ folgt (mit Hilfe von Satz 1(x)) $ggT(a,m) \mid 1$ und daher $ggT(a,m) = 1$.

(ii) $\Rightarrow$ (i) Wegen Korollar 6 $\exists x, y \in \mathbb{Z} : ax + my = 1$ und daher $ax \equiv 1 \ (m)$.

Lemma 47 Es sei $m \in \mathbb{N}$, $m \geq 2$, $a \in \mathbb{Z}$ mit $ggT(a,m) = 1$ und $x \in \mathbb{Z}$ sodass $ax \equiv 1 \ (m)$.

(i) Ist $b \in \mathbb{Z}$ und $b \equiv a \ (m)$, so ist $ggT(b,m) = 1$ und $bx \equiv 1 \ (m)$,

(ii) Ist $y \in \mathbb{Z}$ und $y \equiv x \ (m)$, so gilt $ay \equiv 1 \ (m)$,

(iii) Ist $y \in \mathbb{Z}$ und $ay \equiv 1 \ (m)$, so gilt $y \equiv x \ (m)$.

Beweis: (i) Nach Satz 36 $\exists k \in \mathbb{Z} : b = a + km$. Ist $d \in \mathbb{N}^+$ gemeinsamer Teiler von b und m, so gilt wegen Satz 1(x) auch $d \mid a$, d.h. d ist gemeinsamer Teiler von a und m und daher $d = 1$. Wegen Korollar 40(ii) ist $bx \equiv ax \equiv 1 \ (m)$.

(ii) Wegen Korollar 40(ii) ist $ay \equiv ax \equiv 1 \ (m)$.

(iii) Aus $ay \equiv 1 \equiv ax \ (m)$ folgt $m \mid a(y-x)$. Da $ggT(a,m) = 1$ folgt wegen Satz 12, dass $m \mid (y-x)$, d.h. $y \equiv x \ (m)$.

Definition: Es sei $m \in \mathbb{N}$, $m \geq 2$. Eine Restklasse modulo m wird prime Restklasse genannt, wenn jedes $a \in \mathbb{Z}$, das in ihr liegt, die Bedingung $ggT(a,m) = 1$ erfüllt.

Bemerkung: Satz 46 und Lemma 47 besagen, dass eine Restklasse $a + m\mathbb{Z}$ genau dann ein multiplikatives Inverses (nämlich die Restklasse $x + m\mathbb{Z}$) besitzt, wenn $ggT(a,m) = 1$ gilt.

Beispiele: 1) Für $m = 2$ ist nur die Restklasse von 1 prime Restklasse.
2) Für $m = 3$ sind die Restklassen von 1 und 2 prime Restklassen.
3) Für $m = 4$ sind die Restklassen von 1 und 3 prime Restklassen.
4) Für $m = 5$ sind die Restklassen von 1, 2, 3 und 4 prime Restklassen.
5) Für $m = 6$ sind die Restklassen von 1 und 5 prime Restklassen.
6) Für $m = 12$ sind die Restklassen von 1, 5, 7 und 11 prime Restklassen.
7) Ist m eine Primzahl, so sind die Restklassen von $1, 2, \ldots, m-1$ prime Restklassen.

Definition: Für $m \in \mathbb{N}^+$ wird die EULERsche φ-Funktion definiert als

$$\varphi(m) = |\{k \in \mathbb{N} \mid 1 \leq k \leq m, \ ggT(k,m) = 1\}|.$$

Bemerkung: Für $n \geq 2$ ist $\varphi(n) = |\{k \in \mathbb{N} \mid 1 \leq k < n, \text{ggT}(k,n) = 1\}|$ und $\varphi(n)$ ist die Anzahl der primen Restklassen modulo n. Die obige Definition beinhaltet auch $\varphi(1) = 1$.

Beispiel: $\varphi(2) = 1$, $\varphi(3) = \varphi(4) = \varphi(6) = 2$, $\varphi(5) = \varphi(12) = 4$. Ist p eine Primzahl, so ist $\varphi(p) = p - 1$.

Lemma 48 Ist p eine Primzahl und $\alpha \in \mathbb{N}^+$, so ist $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

Beweis: Ist $k \in \{1, 2, \dots, p^\alpha\}$, so gilt $\text{ggT}(k, p^\alpha) > 1 \iff p \mid k \iff k \in \{pd \mid 1 \leq d \leq p^{\alpha-1}\}$

Lemma 49 Es seien $\ell, m \in \mathbb{N}^+$ und $k \in \mathbb{Z}$. Äquivalent sind:

(i) $\text{ggT}(k, \ell) = \text{ggT}(k, m) = 1$,

(ii) $\text{ggT}(k, \ell m) = 1$.

Beweis: (i) $\Rightarrow$ (ii) Ist $\text{ggT}(k, \ell m) > 1$, so gibt es eine Primzahl p mit der Eigenschaft $p \mid k$ und $p \mid \ell m$. Wegen Satz 16 folgt, dass $p \mid \ell$ oder $p \mid m$. Also ist $\text{ggT}(k, \ell) > 1$ oder $\text{ggT}(k, m) > 1$.

(ii) $\Rightarrow$ (i) Ist $d \in \mathbb{N}^+$ gemeinsamer Teiler von k und ℓ, so ist d auch gemeinsamer Teiler von k und ℓm. Nach Voraussetzung folgt $d = 1$ und $\text{ggT}(k, \ell) = 1$. Völlig analog gilt auch $\text{ggT}(k, m) = 1$.

Lemma 50 Es seien $\ell, m \in \mathbb{N}^+$, $\text{ggT}(\ell, m) = 1$ und $r \in \mathbb{Z}$. Dann enthalten die m Zahlen $r, \ell + r, 2\ell + r, \dots, (m-1)\ell + r$ genau eine Zahl aus jeder Restklasse modulo m. (Da sie bilden ein „vollständiges Repräsentantensystem modulo m.")

Beweis: Ist $k\ell + r \equiv h\ell + r \ (m)$ (wobei $0 \leq k, h \leq m-1$), so folgt $m \mid (k-h)\ell$ und daher (wegen Satz 12) $m \mid (k-h)$, also $k \equiv h \ (m)$. Da $0 \leq k, h \leq m-1$ folgt $k = h$.

Satz 51 Sind $\ell, m \in \mathbb{N}^+$ und $\text{ggT}(\ell, m) = 1$, so gilt $\varphi(\ell \cdot m) = \varphi(\ell) \cdot \varphi(m)$. 26.5.2025

Beweis: Zu bestimmen ist die Anzahl aller $k \in \{1, 2, \dots, \ell m\}$, die die Bedingung $\text{ggT}(k, \ell m) = 1$ erfüllen. Nach Lemma 49 sind das genau jene k, die die Eigenschaft $\text{ggT}(k, \ell) = \text{ggT}(k, m) = 1$ erfüllen. Wir schreiben die Zahlen $1, 2, \dots, \ell m$ in folgendem rechteckigen Schema auf:

1	2	$\cdots$	r	$\cdots$ ℓ
$\ell+1$	$\ell+2$	$\cdots$	$\ell+r$	$\cdots$ 2ℓ
$2\ell+1$	$2\ell+2$	$\cdots$	$2\ell+r$	$\cdots$ 3ℓ
$\vdots$	$\vdots$		$\vdots$	$\vdots$
$(m-1)\ell+1$	$(m-1)\ell+2$	$\cdots$	$(m-1)\ell+r$	$\cdots$ $m\ell$

Für $1 \leq r \leq \ell$ betrachten wir nun die Zahlen $r, \ell + r, 2\ell + r, \dots, (m-1)\ell + r$ in der r-ten Spalte.

Ist $ggT(r,l)=1$, so sind alle Zahlen $r, l+r, 2l+r, \dots, (m-1)l+r$ relativ prim zu l.
(Ist $d \in \mathbb{N}^+$ gemeinsamer Teiler von $kl+r$ und l, so ist d auch gemeinsamer Teiler von r und l und daher $ggT(kl+r, l) = 1$.)

Ist $ggT(r,l) > 1$, so ist keine der Zahlen $r, l+r, 2l+r, \dots, (m-1)l+r$ relativ prim zu l. (Ist $d > 1$ gemeinsamer Teiler von r und l, so ist d auch gemeinsamer Teiler von $kl+r$ und l und daher $ggT(kl+r, l) > 1$.)
Von den l Spalten des Schemas enthalten daher $\varphi(l)$ nur Zahlen, die relativ prim zu l sind und die übrigen Spalten enthalten keine Zahlen, die relativ prim zu l sind. Wir betrachten nun die Zahlen $r, l+r, 2l+r, \dots, (m-1)l+r$ in einer der Spalten mit $ggT(r,l) = 1$. Nach Lemma 50 enthalten sie aus jeder Restklasse modulo m genau eine Zahl und daher $\varphi(m)$ Zahlen, die relativ prim zu m sind. Insgesamt enthält das Schema daher $\varphi(l)\varphi(m)$ Zahlen, die relativ prim zu lm sind.

Bemerkung: Ohne die Voraussetzung $ggT(l,m)=1$ ist Satz 51 und 4 korrekt.
z.B. ist $\varphi(4) = 2$ aber $\varphi(2)^2 = 1^2 = 1$.

Korollar 52 Es sei $m \in \mathbb{N}$, $m \geq 2$.

(i) Ist $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ die Primfaktorzerlegung von m, so ist

$$\varphi(m) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) = p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_k^{\alpha_k-1}(p_k-1),$$

(ii) $\varphi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$ (wobei das Produkt über alle Primzahlen p läuft, die m teilen).

Beweis: $\varphi(m) = \varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) \overset{\text{Satz 51}}{=} \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$

$$\overset{\text{Lemma 48}}{=} (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) = p_1^{\alpha_1-1}(p_1-1) \cdots p_k^{\alpha_k}(p_k-1)$$

$$= p_1^{\alpha_1} \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$

Beispiel Zu berechnen ist $\varphi(8712)$. Da $8712 = 2^3 \cdot 3^2 \cdot 11^2$, ist

$\varphi(8712) = (8-4) \cdot (9-3) \cdot (121-11) = 4 \cdot 6 \cdot 110 = 2640$ oder

$\varphi(8712) = 8712 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{11}\right) = 8712 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{10}{11} = 2640$

Lemma 53 Es sei $m \in \mathbb{N}$, $m \geq 2$ und $a \in \mathbb{Z}$, $ggT(a,m) = 1$. Enthält die Menge $\{x_1, \dots, x_{\varphi(m)}\}$ aus jeder primen Restklasse genau einen Repräsentanten, so enthält auch die Menge $\{ax_1, \dots, ax_{\varphi(m)}\}$ aus jeder primen Restklasse genau einen Repräsentanten.

Beweis: Aus $ggT(x_i, m) = ggT(a, m) = 1$ folgt $ggT(ax_i, m) = 1$ (für $1 \le i \le \varphi(m)$).
(Ist $ggT(ax_i, m) > 1$, so gibt es eine Primzahl p mit $p \mid (ax_i)$ und $p \mid m$. Daraus folgt wegen Satz 16), dass $p \mid a$ oder $p \mid x_i$ und daher $ggT(a, m) > 1$ oder $ggT(x_i, m) > 1$.)
Daher liegen $ax_1, \dots, ax_{\varphi(m)}$ alle in primen Restklassen. Aus $ax_i \equiv ax_j \ (m)$ (wobei $1 \le i, j \le \varphi(m)$) folgt $m \mid a(x_i - x_j)$. Da $ggT(a, m) = 1$ folgt wegen Satz 12 $m \mid (x_i - x_j)$ und daher $x_i \equiv x_j \ (m)$. Da $x_1, \dots, x_{\varphi(m)}$ in verschiedenen Restklassen liegen, folgt $x_i = x_j$ bzw $i = j$

Satz 54 (EULER) Es sei $m \in \mathbb{N}$, $m \ge 2$, $a \in \mathbb{Z}$ und $ggT(a, m) = 1$. Dann ist $a^{\varphi(m)} \equiv 1 \ (m)$.

Beweis: Die Menge $\{x_1, \dots, x_{\varphi(m)}\}$ enthielt aus jeder primen Restklasse modulo m genau einen Repräsentanten. Nach Lemma 53 gilt das dann auch für die Menge $\{ax_1, \dots, ax_{\varphi(m)}\}$. Anders gesagt: Für jedes $i \in \{1, \dots, \varphi(m)\}$ gibt es genau ein $j \in \{1, \dots, \varphi(m)\}$ sodass $x_i \equiv ax_j \ (m)$. Es folgt

$$x_1 \cdot x_2 \cdots x_{\varphi(m)} \equiv (ax_1)(ax_2) \cdots (ax_{\varphi(m)}) = a^{\varphi(m)} \cdot (x_1 x_2 \cdots x_{\varphi(m)}) \ (m).$$

Dabei ist $ggT(x_1 \cdots x_{\varphi(m)}, m) = 1$. (Wäre $ggT(x_1 \cdots x_{\varphi(m)}, m) > 1$, so würde es eine Primzahl p mit der Eigenschaft $p \mid (x_1 \cdots x_{\varphi(m)})$ und $p \mid m$ geben. Wegen Korollar 17 würde dann $p \mid x_i$ und daher $ggT(x_i, m) > 1$ für ein $i \in \{1, \dots, \varphi(m)\}$ gelten.)
Mit Hilfe von Korollar 40 (vii) erhält man $a^{\varphi(m)} \equiv 1 \ (m)$.

Korollar 55 (Kleiner FERMAT'scher Satz) Es sei p eine Primzahl.
(i) Ist $a \in \mathbb{Z}$ und $ggT(a, p) = 1$, so ist $a^{p-1} \equiv 1 \ (p)$,
(ii) Für jedes $a \in \mathbb{Z}$ ist $a^p \equiv a \ (p)$.

Beweis: (i) Ist ein Spezialfall von Satz 54, da $a^{p-1} = a^{\varphi(p)} \equiv 1 \ (p)$.
(ii) Ist $ggT(a, p) = 1$, so ist $a^p = a \cdot a^{p-1} \equiv a \cdot 1 = a \ (p)$.
Ist $ggT(a, p) > 1$, so gilt $p \mid a$ (wegen Lemma 15) und $a^p \equiv 0 \equiv a \ (p)$.

Bemerkung: Man kann mit Hilfe von Korollar 55 (ii) untersuchen, ob eine Zahl $n \in \mathbb{N}$ eine Primzahl ist. Ist z.B. $2^n \not\equiv 2 \ (n)$, so kann n keine Primzahl sein.
Wir zeigen auf diese Weise, dass $91 \ (= 7 \cdot 13)$ keine Primzahl ist. Aus $2^{12} = 4096 = 45 \cdot 91 + 1$ folgt $2^{12} \equiv 1 \ (91) \Rightarrow 2^{91} = 2^{7 \cdot 12 + 7} = (2^{12})^7 2^7 \equiv 2^7 = 128 \equiv 37 \ (91)$ und daher $2^{91} \not\equiv 2 \ (91)$.
Aus $2^n \equiv 2 \ (n)$ folgt aber nicht, dass n eine Primzahl ist. Z.B. ist $2^{561} \equiv 2 \ (561)$ aber $561 = 3 \cdot 11 \cdot 17$ ist keine Primzahl.

Satz 56 (Satz von WILSON) Es sei $p \in \mathbb{N}$, $p > 1$. Äquivalent sind:

(i) p ist Primzahl,

(ii) $(p-1)! \equiv -1 \ (p)$

Beweis: (i) $\Rightarrow$ (ii) Die Behauptung ist erfüllt wenn $p \in \{2,3\}$ da $1! = 1 \equiv -1 \ (2)$ und $2! = 2 \equiv -1 \ (3)$. Es sei nun $p \geq 5$. Die Zahlen $1, 2, \dots, p-1$ bilden ein vollständiges Repräsentantensystem für die primen Restklassen modulo p. Nach Satz 46 und Lemma 47 gibt es für jedes $x \in \{1,2,\dots,p-1\}$ ein eindeutig bestimmtes $y \in \{1,2,\dots,p-1\}$ mit der Eigenschaft $xy \equiv 1 \ (p)$. Dabei ist $x = y \iff x \in \{1, p-1\}$, denn

$x^2 \equiv 1 \ (p) \Rightarrow p \mid (x^2-1) \Rightarrow p \mid (x-1)(x+1) \Rightarrow p \mid (x-1)$ oder $p \mid (x+1)$

$\Rightarrow x \equiv 1 \ (p)$ oder $x \equiv -1 \ (p) \rightarrow x = 1 \vee x = p-1$.

Daher sind die Zahlen $2, 3, \dots, p-2$ eine Vereinigung von $\frac{p-3}{2}$ Paaren x, y mit der Eigenschaft $xy \equiv 1 \ (p)$ und daher $2 \cdot 3 \cdot \dots \cdot (p-2) \equiv 1^{\frac{p-3}{2}} = 1 \ (p)$. Daraus folgt

$(p-1)! = 2 \cdot 3 \cdot \dots \cdot (p-2) \cdot (p-1) \equiv p-1 \equiv -1 \ (p)$.

2.6.2025

(ii) $\Rightarrow$ (i) Angenommen, es gilt $(p-1)! \equiv -1 \ (p)$ und p ist keine Primzahl. Dann $\exists a \in \mathbb{N}, 2 \leq a \leq p-1 : a \mid p$. Dann würde einerseits $a \mid (p-1)!$ und daher $(p-1)! \equiv 0 \ (a)$ gelten und andererseits $(p-1)! \equiv -1 \ (a)$ wegen Satz 39 (iii). Daraus würde $0 \equiv -1 \ (a)$ folgen, ein Widerspruch.