Frank Klinker

Zahlentheorie

Teil 2: Der Zahlenraum $\mathbb{Z}_N$, die φ-Funktion und der Satz von Euler

1 Der Zahlenraum $\mathbb{Z}_N$

1.1 Die Menge $\mathbb{Z}_N$

Teilt man eine ganze Zahl durch eine feste Zahl N, dann hat der Quotient einen Rest der zwischen 0 und $N-1$ liegt.

Ist z. B. $N = 7$, so hat jede Zahle beim Teilen durch 7 den Rest $0, 1, 2, 3, 4, 5$ oder 6.

Die Menge der Reste beim Teilen durch N nennen wir die **Restklassenmenge** $\mathbb{Z}_N$. Wir schreiben dafür

$$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}\,.$$

Beispiel 1. Für $N = 7$ haben wir

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}\,.$$

1.2 Rechnen in $\mathbb{Z}_N$

In der Menge $\mathbb{Z}_N$ können wir addieren, subtrahieren und multiplizieren wie mit ganzen Zahlen.

Wir müssen nach einer Rechnung das Ergebnis lediglich so "korrigieren", dass es tatsächlich in der Menge $\mathbb{Z}_N$ liegt. Das heißt, wir berechnen den Rest beim Teilen durch N.

Unsere Schreibweise dafür ist

$$9 \equiv 2 \bmod 7\,, \quad 123 \equiv 21 \bmod 51\,, \quad 859 \equiv 3 \bmod 8\,, \quad -18 \equiv 2 \bmod 5$$

Für die Zahlen $N = 7$ und $N = 10$ wollen wir die Addition und Multiplikation hier beispielhaft durchführen:

Adresse: Eduard-Spranger-Berufskolleg, 59067 Hamm
E-Mail: mail@frank-klinker.de
Version: 10. April 2025

Beispiel 2 (Addieren in $\mathbb{Z}_7$ und $\mathbb{Z}_10$)**.**

$$\begin{aligned}
1+5 &\equiv 6 \bmod 7\\
3+4 &\equiv 7 \equiv 0 \bmod 7\\
6+8 &\equiv 14 \equiv 4 \bmod 10\\
7+3 &\equiv 10 \equiv 0 \bmod 10
\end{aligned}$$

Das liefert für $N = 7$ und $N = 10$ die folgenden zwei **Additionstabellen**

$\mathbb{Z}_7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\mathbb{Z}_{10}$

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Beispiel 3 (Multiplizieren in $\mathbb{Z}_7$ und $\mathbb{Z}_10$)**.** Für die Multiplikation haben wir z. B.

$$\begin{aligned}
1\cdot 5 &\equiv 5 \bmod 7\\
3\cdot 4 &\equiv 12 \equiv 5 \bmod 7\\
6\cdot 8 &\equiv 48 \equiv 8 \bmod 10\\
7\cdot 3 &\equiv 21 \equiv 1 \bmod 10
\end{aligned}$$

Das liefert für $N = 7$ und $N = 10$ die folgenden zwei **Multiplikationstabellen**:[1]

$\mathbb{Z}_7$

·	1	2	3	4	5	6
∗1	1	2	3	4	5	6
∗2	2	4	6	1	3	5
∗3	3	6	2	5	1	4
∗4	4	1	5	2	6	3
∗5	5	3	1	6	4	2
∗6	6	5	4	3	2	1

$\mathbb{Z}_{10}$

·	1	2	3	4	5	6	7	8	9
∗1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	0	2	4	6	8
∗3	3	6	9	2	5	8	1	4	7
4	4	8	2	6	0	4	8	2	6
5	5	0	5	0	5	0	5	0	5
6	6	2	8	4	0	6	2	8	4
∗7	7	4	1	8	5	2	9	6	3
8	8	6	4	2	0	8	6	4	2
∗9	9	8	7	6	5	4	3	2	1

Die Zeile und Spalte zu 0 wird in der Multiplikationstabelle weggelassen, weil die Ergebnisse immer 0 ergeben.

[1] Warum man in der Tabelle an manchen Stellen ein $*$ findet, wird ab Bemerkung 6 erklärt.

2 Teilerfremdheit und die Eulersche φ-Funktion

Um die Multiplikationstabellen weiter untersuchen zu können , wiederholen wir:

Zwei Zahlen $a, b \in \mathbb{Z}$ mit $a, b \neq 0$ heißen **teilerfremd**, wenn sie als gemeinsamen Teiler lediglich die 1 haben. Wir schreiben dafür

$$\mathrm{ggT}(a, b) = 1$$

und sagen auch **der größte gemeinsame Teiler** ist 1.

Beispiel 4.
- Die Zahlen 10 und 4 sind nicht teilerfremd, denn sie haben neben 1 noch den gemeinsamen Teiler 2, sodass $\mathrm{ggT}(4, 10) = 2$.
- Die Zahlen 10 und 9 sind teilerfremd, denn es ist $\mathrm{ggT}(9, 10) = 1$.
- Die Zahl 7 ist teilerfremd zu jeder Zahl außer zu ihren Vielfachen: Das gilt für <u>jede Primzahl</u> p:
$$\mathrm{ggT}(p, a) = 1, \text{ für } a \neq kp, k \in \mathbb{Z}$$

Bemerkung 5. Addieren, Subtrahieren und Multiplizieren macht in $\mathbb{Z}_N$ keine großen Probleme. Größere Probleme gibt es da beim Dividieren. Das sollte uns nicht wundern, denn das klappt ja schon nicht in $\mathbb{Z}$.

Allerdings sehen wir in z. B. $\mathbb{Z}_{10}$ das folgende Phänomen: Es gelten die Gleichungen

$$5 \cdot 3 \equiv 5 \cdot 17 \bmod 10 \qquad \text{und} \qquad 7 \cdot 3 = 7 \cdot 13 \bmod 10\,.$$

Hier kann man in der rechten Gleichung die 7 kürzen aber in der linken Gleichung darf man die 5 nicht kürzen.

Der Unterschied besteht darin, dass $\mathrm{ggT}(7, 10) = 1$ (dann durften wir kürzen), aber $\mathrm{ggT}(5, 20) \neq 1$ (dann durften wir nicht kürzen). Das können wir so zusammenfassen:

1. $\boxed{\text{Ist } m \cdot a \equiv m \cdot b \bmod N \text{ und } \mathrm{ggT}(m, N) = g, \text{ dann ist } a \equiv b \bmod \frac{N}{g}}$

Besonders interessant ist das in dem Fall, wo m und N teilerfremd sind, also $\mathrm{ggT}(m, N) = 1$:

2. $\boxed{\text{Ist } m \cdot a \equiv m \cdot b \bmod N \text{ und } \mathrm{ggT}(m, N) = 1, \text{ dann ist } a \equiv b \bmod N}$

Wir sehen uns die zwei Multiplikationstabellen zu $N = 10$ und $N = 7$ nochmal genauer an:

Bemerkung 6.
- In den Multiplikationstabellen ist auffällig, dass in einigen Zeilen und analogen Spalten jede mögliche Zahl auch als Ergebnis vorkommt (das sind die Zeilen mit $*$).
- In $\mathbb{Z}_7$ trifft dies für jede Zeile zu, in $\mathbb{Z}_{10}$ aber nur für die Zeilen zu 1,3,7 und 9.

- In den anderen Zeilen fehlen nicht nur einige Zahlen, sondern es tritt auch die Zahl 0 als Ergebnis einer Multiplikation auf. Das ist ein enormer Unterschied zu den reellen Zahlen $\mathbb{R}$, wo das nicht passieren kann.

Fakt 7. 1. In der Multiplikationstabelle von $\mathbb{Z}_N$ kommen in der Zeile zur Zahl a <u>alle</u> Zahlen von 0 bis $N-1$ vor, wenn N und a teilerfremd sind, also wenn $\mathrm{ggT}(N,a)=1$.

2. In der Multiplikationstabelle von $\mathbb{Z}_N$ kommen in den Zeilen zur Zahl a <u>nicht alle</u> Zahlen von 0 bis $N-1$ vor, wenn N und a nicht teilerfremd sind, also wenn $\mathrm{ggT}(N,a)=g>1$.
   Genauer: Es tauchen als Reste nur die Vielfachen von g auf. Insbesondere kommt die 1 nicht vor, aber die 0 kommt mindestens ein einmal vor.

Die Eigenschaften des modularen Rechnens in $\mathbb{Z}_N$ und Fakt 7 lassen sich so zusammenfassen:

Folgerung 8. 1. $\mathbb{Z}_N$ ist mit der modularen Addition eine kommutative Gruppe.

2. $\mathbb{Z}_N$ ist mit der modularen Addition und Multiplikation ein kommutativer Ring mit Eins.
3. $\mathbb{Z}_N^*$ enthält alle Elemente aus $\mathbb{Z}_N$, die teilerfremd zu N sind.
4. Sind $a \in \mathbb{Z}_N$ und N nicht teilerfremd, so gibt es eine Zahl $b \in \mathbb{Z}_N$, sodass $a \cdot b = 0 \bmod N$. Das heißt, ZZ_N ist nur nullteilerfrei, wenn N eine Primzahl ist
5. $\mathbb{Z}_N$ ist nur dann ein Körper, wenn N eine Primzahl ist.
6. **Beispiele:** $\mathbb{Z}_{10}$ ist ein kommutativer Ring mit Eins, der nicht nullteilerfrei ist. $\mathbb{Z}_7$ ist ein Körper.

Da zu einem vorgegebenen Modus N die hierzu teilerfremden Zahlen eine besondere Rolle spielen, ist es auch interessant, ihre Anzahl zu kennen:

Die Eulersche φ-Funktion

Es sei N eine positive natürliche Zahl, dann bezeichnet

$$\varphi(N)$$

die Anzahl der zu N teilerfremden Zahlen in der Menge $\{1,2,\ldots,N-1\}$.

φ heißt die **Eulersche φ-Funktion**.

Beispiel 9.

1,2,3,4,5,6 sind teilerfremd zu 7,	$\varphi(7) = 6$
1,3,7,9 sind teilerfremd zu 10	$\varphi(10) = 4$
1,3,5,7 sind teilerfremd zu 8	$\varphi(8) = 4$
1,7,11,13,17,19,23,29 sind teilerfremd zu 30	$\varphi(30) = 8$
1,2,4,7,8,11,13,14 sind teilerfremd zu 15	$\varphi(15) = 8$
1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 91, 97, 101, 103, 107, 109, 113, 119 sind teilerfremd zu 120	$\varphi(120) = 32$

Fakt 10. Für eine Primzahl p ist die Berechnung von $\varphi(p)$ recht einfach. Da alle Zahlen $1, 2, \ldots, p-1$ teilerfremd zu p sind, gilt:

$$\boxed{\text{Ist } p \text{ eine Primzahl, dann ist } \ \varphi(p) = p - 1}$$

Fakt 11 (Multiplikationsregel für die φ-Funktion)**.**

Lässt sich die Zahl N in das Produkt von zwei <u>teilerfremden</u> Zahlen N_1 und N_2 zerlegen, also $N = N_1 \cdot N_2$, dann gilt

$$\varphi(N) = \varphi(N_1) \cdot \varphi(N_2)\,.$$

Beispiel 12.

- Es ist $120 = 8 \cdot 15$ und $\mathrm{ggT}(8, 15) = 1$. Weiter ist $\varphi(8) = 4$ und $\varphi(15) = 8$. Damit ist $\varphi(8) \cdot \varphi(15) = 4 \cdot 8 = 32$ und das stimmt mit $\varphi(120) = 32$ überein.
- Anderseits ist aber auch $120 = 4 \cdot 30$ aber mit $\mathrm{ggT}(4, 30) = 2 > 1$. Es ist $\varphi(4) = 2$ und $\varphi(30) = 8$ und deshalb $\varphi(4) \cdot \varphi(30) = 2 \cdot 8 = 16$. Das stimmt <u>nicht</u> mit $\varphi(120) = 32$ überein.

Bemerkung 13.

- Die Multiplikationsregel ist leider nur bedingt nützlich, weil es ist in der Regel schwierig ist, eine Zahl in ein Produkt teilerfremder Zahlen zu zerlegen.
- Damit ist auch die Berechnung von $\varphi(N)$ in der Regel kompliziert, insbesondere für große N.

In speziellen Fällen lässt sich $\varphi(n)$ jedoch berechnen:

Bemerkung 14. 1. Die folgende Verallgemeinerung von Fakt 10 ist gültig:

$$\boxed{\text{Ist } p \text{ eine Primzahl, dann ist } \ \varphi(p^k) = p^{k-1} \cdot (p-1)}$$

2. Hat N die Primkatorzerlegung $N = p_1^{k_1} \cdot_2^{k_2} \cdot \ldots p_r^{k_r}$, dann ist

$$\begin{aligned}\varphi(N) &= p_1^{k_1-1}(p_1-1) \cdot_2^{k_2-1} (p_2-1) \cdot \ldots p_r^{k_r-1}(p_r-1) \\ &= N \cdot \left(1 - \tfrac{1}{p_1}\right) \cdot \left(1 - \tfrac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \tfrac{1}{p_r}\right).\end{aligned}$$

Insbesondere ist $\varphi(N)$ für alle Zahlen $N > 2$ stets gerade.

3 Potenzieren in $\mathbb{Z}_N$ und der Satz von Euler

3.1 Potenzieren in $\mathbb{Z}_N$

Das Potenzieren mit natürlichen Zahlen im Restklassenraum $\mathbb{Z}_N$ ist eigentlich kein Problem, denn es ist ja "lediglich" Multiplikationen durchzuführen.

Dabei lohnt es sich Potenzgesetze zu verwenden und sich im Wesentlichen auf kleine Potenzen zurückzuziehen:

Beispiel 15.

$$\begin{aligned}
2^7 &\equiv 128 \equiv 9 \bmod 17 \\
2^7 &\equiv 2^4 \cdot 2^3 \equiv 16 \cdot 8 \equiv (-1) \cdot 8 \equiv -8 \equiv 9 \bmod 17 \\
2^{66} &\equiv (2^4)^{16} \cdot 2^2 \equiv (-1)^{16} \cdot 4 \equiv 4 \bmod 17 \\
8^{10} &\equiv ((-3)^2)^5 \equiv (9)^5 \equiv (-2)^5 \equiv -32 \equiv 1 \bmod 11 \\
8^{21} &\equiv 8 \cdot (((-3)^2)^2)^5 \equiv 8 \cdot ((-2)^2)^5 \equiv 8 \cdot (4)^5 \equiv 8 \cdot 4 \cdot (4^2)^2 \\
&\equiv 8 \cdot 4 \cdot 5^2 \equiv 8 \cdot 4 \cdot 3 \equiv 8 \cdot 12 \equiv 8 \cdot 1 \equiv 8 \bmod 11
\end{aligned}$$

Fakt 16. Wenn wir bereits wissen, dass es eine Potenz gibt, sodass $a^K \equiv 1 \bmod N$ gilt, dann können wir und das Berechnen sehr vereinfachen.

Wir können das nämlich nutzen, um einen beliebigen Exponenten zu verkleinern.

Es ist etwa in dem obigen Beispiel $8^{10} \equiv 1 \bmod 11$, sodass

$$8^{21} = 8^{10 \cdot 2 + 1} \equiv (8^{10})^2 \cdot 8 \equiv 1^2 \cdot 8 \equiv 8 \bmod 11\,.$$

Etwas formaler lautet das:

$$\boxed{\text{Gilt } \; a^K \equiv 1 \bmod N \; \text{ und } \; \ell = m \bmod K, \; \text{ dann ist } \; a^\ell \equiv a^m \bmod N\,.}$$

Wir brauchen dann nur noch die Potenzen $a^1, a^2, \ldots, a^{K-1}$ berechnen und kennen danach bereits alle!

3.2 Der Satz von Euler

Das Problem in Bemerkung 16 besteht nun darin: Wie finden wir zu vorgegebener Basis a einen solchen Exponenten K?

Da hilft uns der folgende Satz von Euler (daher hat die Funktion φ ihren Namen):

Satz 17 (Satz von Euler)**.**

Ist N eine positive, natürliche Zahl und a teilerfremd zu N, d. h. $\mathrm{ggT}(a, N) = 1$ so gilt

$$a^{\varphi(N)} = 1 \bmod N\,.$$

Bemerkung 18. 1. Das Ergebnis des Satzes ist erstaunlich, da es besagt, dass es einen Exponenten mit der in Bemerkung 16 gewünschten Eigenschaft gibt, der für alle (interessanten) Basen der gleiche ist!

2. Ist p eine Primzahl, dann ist $\varphi(p) = p - 1$. Damit gilt für alle Zahlen $a = 1, 2, \ldots, p-1$:
$$a^{p-1} = 1 \bmod p\,.$$
Schreiben wir das etwas anders, so gibt das den Satz von Euler für Primzahlen

Für alle Primzahlen p gilt $a^p \equiv a \bmod p$

4 Die Begründungen für einige der Aussagen

4.1 Die Begründung für Fakt 7

1. Wir befinden uns in $\mathbb{Z}_N$ und sehen uns dort die Zahl a an. Es gilt

Ist $\mathrm{ggT}(a, N) = 1$, dann haben die Werte $k \cdot a$ mit $k = 0, 1, \ldots, (N-1)$ alle verschiedene Rest modulo N. D. h. durchlaufen alle Reste $0, 1, \ldots, N-1$ und decken ganz $\mathbb{Z}_N$ ab.

Denn ist $k \cdot a \equiv \ell \cdot a \bmod N$, also $(k - \ell) \cdot a \equiv 0 \bmod N$, dann wäre wegen Bemerkung 5.2 auch $k - \ell \equiv 0 \bmod N$, also $k = \ell \bmod N$. Das passiert aber in der aufgeführten Menge nicht.

2. Ist aber $\mathrm{ggT}(a, N) = g$, dann ist $\mathrm{ggT}(\frac{a}{g}, \frac{N}{g}) = 1$.

Damit durchlaufen die Zahlen $k \cdot \frac{a}{g}$ mit $k = 0, \ldots\ m-1$ alle Reste $0, 1, \ldots, m-1$ modulo $\frac{N}{g}$, wobei $m = \frac{N}{g}$ ist.

Multiplizieren wir das mit g, dann sehen wir, dass $k \cdot a = k \cdot \frac{a}{g} \cdot g$ die Reste $0, g, 2 \cdot g, \ldots (m-1)g$ modulo N durchläuft.

Ist nun $\ell \geq m$ dann gibt es ein $0 \leq r < m$ und eine Zahl j, sodass $\ell = j \cdot m + r$. Dann ist $\ell \cdot a = (j \cdot m + r) \cdot a = j \cdot m \cdot a + r \cdot a = j \cdot \frac{N}{g} \cdot a + r \cdot a = r \cdot a + j \cdot \frac{a}{g} \cdot N$, also $\ell \cdot a \equiv r \cdot a \bmod N$ und wir erhalten einen Rest, der bereits vorhanden war.

Wir fassen zusammen:

Ist $\mathrm{ggT}(a, N) = g$, dann nehmen die Werte $k \cdot a$ mit $k = 0, 1, \ldots, N-1$ nur die Reste $0, g, 2 \cdot g, \ldots, N-g$ modulo N an. Insbesondere ist 1 nicht darunter und alle Werte wiederholen sich genau g mal.

4.2 Die Begründung für Fakt 11

Für die Begründung von Fakt 11 werden wir die folgenden natürlichen eigenschaften ganzer Zahlen benötigen:

- Ist $a \equiv b \bmod N$ und teilt q die Zahl N, dann gilt auch $a \equiv b \bmod q$.
- Ist $\mathrm{ggT}(a, m) = g$, dann ist auch $\mathrm{ggT}(a + k \cdot m, m) = g$.
- Ist $\mathrm{ggT}(a, m) = 1$ und $\mathrm{ggT}(a, n) = 1$, dann ist auch $\mathrm{ggT}(a, m \cdot n) = 1$.

Wir gehen in drei Schritten vor, um Fakt 11 zu begründen. Dabei gilt immer die Voraussetzung, dass N_1 und N_2 teilerfremd sind, also $\mathrm{ggT}(N_1, N_2) = 1$.

1. $\boxed{\text{Durchläuft } k \text{ alle Reste modulo } N_2 \text{ und } \ell \text{ alle Reste modulo } N_1\text{, dann durchläuft } k \cdot N_1 + \ell \cdot N_2 \text{ alle Reste modulo } N_1 \cdot N_2.}$

   Da die Anzahl der berechneten werte mit der Anzahl aller möglichen Reste übereinstimmt, müssen wir lediglich zeigen, dass ihre Reste unterschiedlich sind.

   Ist aber $k \cdot N_1 + \ell \cdot N_2 \equiv k' \cdot N_2 + \ell' \cdot N_2 \bmod N_1 \cdot N_2$, dann ist auch $k \cdot N_1 \equiv k' \cdot N_1 \bmod N_2$ und $\ell \cdot N_2 \equiv \ell' \cdot N_2 \bmod N_1$. Wegen $\mathrm{ggT}(N_1, N_2) = 1$ ist dann aber auch $k \equiv k' \bmod N_2$ und $\ell \equiv \ell' \bmod N_1$.

   Damit sind alle oben beschriebenen Reste modulo $N_1 \cdot N_2$ tatsächlich verschieden und geben tatsächlich alle möglichen Reste.

2. $\boxed{\text{Durchläuft } k \text{ alle teilerfremden Reste modulo } N_2 \text{ und } \ell \text{ alle teilerfremden Reste modulo } N_1\text{, dann durchläuft } k \cdot N_1 + \ell \cdot N_2 \text{ nur teilerfremde Reste modulo } N_1 \cdot N_2.}$

   Mit $\mathrm{ggT}(N_1, N_2) = 1$, $\mathrm{ggT}(k, N_2) = 1$ und $\mathrm{ggT}(\ell, N_1) = 1$ gilt auch $\mathrm{ggT}(k \cdot N_1 + \ell \cdot N_2, N_1) = 1$ und $\mathrm{ggT}(k \cdot N_1 + \ell \cdot N_2, N_2) = 1$. Die beiden letzten zusammen geben dann $\mathrm{ggT}(k \cdot N_1 + \ell \cdot N_2, N_1 \cdot N_2) = 1$.

3. $\boxed{\text{Ist } k \text{ nicht teilerfremd zu } N_2 \text{ oder } \ell \text{ nicht teilerfremd zu } N_1\text{, dann ist auch } k \cdot N_1 + \ell \cdot N_2 \text{ nicht teilerfremd zu } N_1 \cdot N_2.}$

   Hat z. B. der Rest k einen gemeinsamen Teiler d mit N_2, also $k = d \cdot k'$, $N_2 = d \cdot n$, dann hat auch $k \cdot N_1 + \ell \cdot N_2 = d \cdot k' \cdot N_1 + d \cdot \ell \cdot n$ einen gemeinsamen Teiler mit $N_1 \cdot N_2 = d \cdot N_1 \cdot n$.

1.-3. geben uns nun, dass in Punkt 2. <u>alle</u> teilerfremden Reste modulo $N_1 \cdot N_2$ durchlaufen werden. Da es genau $\varphi(N_1)$ viele teilerfremde Reste von N_1 gibt und $\varphi(N_2)$ viele teilerfremde Reste von N_2, haben wir nun gezeigt, dass es im Fall $\mathrm{ggT}(N_1, N_2) = 1$ genau $\varphi(N_1) \cdot \varphi(N_2)$ viele teilerfremde Reste von $N_1 \cdot N_2$ gibt, also:

$$\boxed{\varphi(N_1 \cdot N_2) = \varphi(N_1) \cdot \varphi(N_2) \quad \text{falls } \mathrm{ggT}(N_1, N_2) = 1}$$

4.3 Die Begründung für den Satz von Euler, Satz 17

$$\boxed{\begin{array}{c}\text{Ist } N \text{ eine positive, natürliche Zahl mit } \mathrm{ggT}(a, N) = 1 \text{ so gilt} \\ a^{\varphi(N)} = 1 \bmod N\,.\end{array}}$$

Wir nehmen zur Begründung der Aussage alle Zahlen zwischen 0 und N her, die teilerfremd zu N sind. Davon gibt es $\varphi(N)$ Stück, etwa $r_1 < r_2 < \ldots < r_{\varphi(N)}$.

- Wir multiplizieren jetzt diese Zahlen mit a, also $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(N)}$.

  Dann sind die Ergebnisse weiterhin teilerfremd zu N.

- Keine zwei dieser neuen Zahlen haben den gleichen Rest modulo N.

  Das liegt daran, dass aus $a \cdot r_i \equiv a \cdot r_j \bmod N$ die Gleichung $r_i \equiv r_j \bmod N$ folgt (wegen $\mathrm{ggT}(a, N) = 1$ dürfen wir durch a teilen). Weil aber $0 < r_i, r_j < N$ ist folgt schließlich $r_i = r_j$.

  Die Reste der Zahlen $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\varphi(N)}$ modulo N sind also die gleichen, wie die Zahlen $r_1, r_2, \ldots, r_{\varphi(N)}$.

- Deshalb ist

$$\begin{aligned}
&(a \cdot r_1) \cdot (a \cdot r_2) \cdot \ldots \cdot (a \cdot r_{\varphi(N)}) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(N)} \bmod N \\
\iff\ & a^{\varphi(N)} \cdot (r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(N)}) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(N)} \bmod N \\
\iff\ & a^{\varphi(N)} \equiv 1 \bmod N
\end{aligned}$$

  Den letzte Schritt durften wir wieder machen, weil $r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(N)}$, wie jeder der Faktoren, teilerfremd zu N ist.