2.4. Kongruenzklassen

Wikipedia:1707 wurde **Euler** als der älteste Sohn des Pfarrers Paul Euler geboren. Er besuchte das Gymnasium in Basel und nahm gleichzeitig Privatunterricht beim Mathematiker Johannes Burckhardt. Ab 1720 studierte er an der Universität Basel und hörte hier Vorlesungen von Johann Bernoulli. 1723 erlangte er durch einen Vergleich der Newtonschen und Kartesischen Philosophie in lateinischer Sprache die Magisterwürde. Seinen Plan, auch Theologie zu studieren, gab er 1725 auf. Am 17. Mai 1727 berief ihn Daniel Bernoulli an die Akademie St. Petersburg. Hier traf er auf Christian Goldbach. 1730 erhielt Euler die Professur für Physik und schließlich 1733 als Nachfolger von Daniel Bernoulli die Professur für Mathematik.
Er bekam in den folgenden Jahren immer stärkere Probleme mit seinem Augenlicht und ab 1740 war eines seiner Augen blind.
1741 holte ihn Friedrich der Große an die Berliner Akademie. Euler korrespondierte und verglich seine Theorien weiterhin mit Christian Goldbach. Nach 25 Jahren in Berlin kehrte er 1766 zurück nach St. Petersburg.

1771 erblindete er total. Trotz dessen entstand fast die Hälfte seines Lebenswerks in der zweiten Petersburger Zeit. Hilfe erhielt er dabei von seinen beiden Söhnen Johann Albrecht und Christoph. 1783 starb er an einer Hirnblutung.

DEFINITION 2.4.1. kongruent modulo

Sei n eine natürliche Zahl > 1 und seien a, b zwei ganze Zahlen. Man sagt: a ist ***kongruent*** b ***modulo*** n, falls a und b den gleichen Rest bei einer Division durch n haben. Dies wird geschrieben als

$$a \equiv b \mod n.$$

Genauso hätte man definieren können: n teilt die Differenz $(a - b)$.

EXAMPLE.

- Rechnen mit beschränkter Genauigkeit im Rechner
- Uhr
- Das $365 \equiv 1 \mod 7$ verschieben sich die Wochentage pro Jahr um einen Tag
- Parity Bit

Das kongruent Zeichen $\equiv$ hat ähnliche Eigenschaften wie das $=$ Zeichen in einer Gleichung. Man darf mit einer ganzen Zahl c addieren, subtrahieren und multiplizieren :

$$\begin{aligned} a + c &\equiv b + c \mod n \\ a - c &\equiv b - c \mod n \\ ac &\equiv bc \mod n \end{aligned}$$

sind dann ebenfalls gültige sog. ***Kongruenzen***. Dividieren geht aber nicht. Man betrachtet dann ähnlich wie bei Gleichungen auch Kongruenzen mit Unbekannten, und sucht nach Lösungen:

$$2x \equiv 0 \mod 4.$$

Gesucht sind ganze Zahlen x (das ist unser Definitionsbereich für Kongruenzen) mit der Eigenschaft, dass nach der Multiplikation mit 2 das Ergebnis durch 4 teilbar ist. Also die Lösung ist:

$$\mathbb{L} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

Betrachtet man die Lösung genauer so zerfällt die Lösungsmenge in zwei Teile

$$\begin{aligned} \mathbb{L}_1 &= \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\ \mathbb{L}_2 &= \{\ldots, -6, -2, 2, 6, 10, \ldots\} \end{aligned}$$

dies sind einmal die Zahlen mit Divisionrest 0 und Divisionsrest 2 bei der Division durch 4. Die Vorstellung ist dann, dass obige Gleichung genau 2 Lösungen hat, dazu folgende Definition:

DEFINITION 2.4.2. Kongruenzklassen

Sei a eine ganze Zahl und n eine natürliche Zahl > 1. Die ***Kongruenzklasse*** von a modulo n ist die Menge aller Zahlen, die bei Division durch n den gleichen Divisionsrest wie a haben. Sie wird mit $[a]_n$ bezeichnet.

$$[a]_n := \{b : b \equiv a \mod n\}$$

Die Menge aller Kongruenzklassen modulo n wird als die Menge der ganzen Zahlen modulo n bezeichnet. Dafür wird das Symbol $\mathbb{Z}_n$ verwendet.

Die erste einfache Eigenschaft ist

$$[a]_n = [a + kn]_n$$

da sich ja der Rest bei der Division durch n nicht ändert wenn man vielfache von n addiert.

In $\mathbb{Z}_2$ gibt es zwei Kongruenzklassen, dies sind die geraden und ungeraden ganzen Zahlen. Verwendet man als Repräsentant einer Klasse die kleinste nicht negative Zahl, so nennen wir das die *Standarddarstellung*, bzw den *Standardrepräsentanten*.

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

Ist klar, modulo welchem n gerechnet wird, lässt man gerne das n in der Notation weg. Es wird häufig auch die folgende Notation verwendet:

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

LEMMA 2.4.3. *kongruent sein ist eine Äquivalenzrelation*

BEWEIS. langweiliges Nachrechnen, der Bedingungen an eine Äquivalenzrelation □

Die Notation der Kongruenzklasse stammt von Euler (1750), was aber erst posthum im Jahr 1830 veröffentlicht wurde. Da war es aber schon von Gauß durch sein Werk von 1801 bekannt. Die Kongruenzklassen sind wichtig, da man mit ihnen rechnen kann.

DEFINITION 2.4.4. Addition und Multiplikation von Kongruenzklassen

Seien a, b ganze Zahlen und n eine natürliche Zahl > 1. Dann definiert man Summe und Produkt von Kongruenzklassen:

$$\begin{array}{lcll} [a]_n & + & [b]_n & := & [a + b]_n \\ [a]_n & \times & [b]_n & := & [a \times b]_n \end{array}$$

Diese Definition hat ein mögliches Problem: was ist wenn eine Klasse durch verschiedene Repräsentanten dargestellt wird. Wir haben zu überprüfen, ob z.B.

$$[5]_7 \times [2]_7 = [47]_7 \times [-5]_7$$

Dies ist die Frage, ob Summe und Produkt von Kongruenzklassen ***wohldefiniert*** ist.

THEOREM 2.4.5. *Wohldefiniertheit von Summe und Produkt bei Kongruenzklassen. (Teil 1)*

Sei n eine natürliche Zahl > 1 und seien a, b, c ganze Zahlen. Sei dabei $[a]_n = [c]_n$. Dann gilt:

$$\begin{array}{lcl} [a + b]_n & = & [c + b]_n \\ [a \times b]_n & = & [c \times b]_n \end{array}$$

BEWEIS. Da a und c in der gleichen Kongruenzklasse sind, teilt n die Differenz, also

$$c - a = kn.$$

Was gleich bedeutend ist mit

$$c = a + kn.$$

Dann hat man für die Summe

$$[c+b]_n = [a+b+kn]_n = [a+b]_n$$

und für das Produkt

$$[cb]_n = [ab+nkb]_n = [ab]_n.$$

Wobei die jeweils letzte Gleichheit direkt aus der Definition der Kongruenzklasse folgt. □

Für das endgültige Ergebnis benötigt man nur das zweimalige Anwenden von obigem Theorem:

COROLLARY 2.4.6. *Wohldefiniertheit von Summe und Produkt bei Kongruenzklassen.*
Sei n eine natürliche Zahl > 1 und seien a, b, c, d ganze Zahlen. Seien dabei $[a]_n = [c]_n$ und $[b]_n = [d]_n$. Dann gilt:

$$\begin{aligned} [a+b]_n &= [c+d]_n \\ [a \times b]_n &= [c \times d]_n \end{aligned}$$

Die Rechenregeln für Multiplikation und Addition wird üblicherweise in Tabellenform festgehalten.

EXAMPLE 2.4.7. Multiplikation und Addition in $\mathbb{Z}_8$
Zur besseren Übersicht schreibt man statt $[a]_8$ nur a und verwendet die Standarddarstellung mit den Repräsentanten $0, \ldots, 7$

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3				
1	1	2	3					0
2							0	1
3						0	1	2
4					0	1	2	3
5				0	1	2	3	
6			0	1	2	3		
7		0	1	2	3			

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Der Eintrag in der $5-$Zeile und in der $6-$Spalte in der Tabelle $\times$ (er ist = 6) bedeutet:

$$[5]_8 \times [6]_8 = [6]_8$$

Damit können wir mit Kongruenzklassen genauso rechnen wie mit den natürlichen Zahlen (Addieren und Multiplizieren), sie sind also auch so etwas ähnliches wie Zahlen. Es gibt eine 'Null' bezüglich der Addition und eine 'Eins' bezüglich der Multiplikation. Man kann sogar mehr als mit natürlichen Zahlen, es gibt ein additiv Inverses, denn:

$$[a]_n + [-a]_n = [0]_n.$$

Diesbezüglich sind die Kongruenzklassen wie die ganzen Zahlen. Im weiteren untersuchen wir die multiplikativ Inversen, d.h. die Frage ob man dividieren kann.

DEFINITION 2.4.8. invertierbar, Nullteiler
Sei n eine natürliche Zahl > 1, und sei a eine ganze Zahl. Die Kongruenzklasse $[a]_n$ heißt ***invertierbar*** (oder invertierbar modulo n) falls es ein b gibt mit

$$[a]_n[b]_n = [1]_n.$$

$[b]_n$ ist dann das (mulitplikativ) Inverse von $[a]_n$, es wird auch mit $[a]_n^{-1}$ bezeichnet. Eine von $[0]_n$verschiedene Kongruenzklasse $[a]_n$ ist ein ***Nullteiler***, falls es ein $[b]_n \neq [0]_n$ gibt mit

$$[a]_n[b]_n = [0]_n.$$

Dann ist natürlich auch $[b]_n$ ein Nullteiler.

Zum Beispiel kann man aus der Multiplikationstabelle die Nullteiler heraussuchen. Im obigen Beispiel von $\mathbb{Z}_8$ sind dies $2, 4, 6$. Um heraus zu finden, welche Kongruenzklassen invertierbar sind kann man auch die Tabelle bemühen, man muss hier 1 suchen, im Falle der $\mathbb{Z}_8$ sind dies $1, 3, 5, 7$. Die allgemeine Methode ist dies:

THEOREM 2.4.9. *invertierbare Klassen in $\mathbb{Z}_n$*
Sei n eine natürliche Zahl > 1, und sei a eine ganze Zahl. Die Kongruenzklasse $[a]_n$ ist invertierbar genau dann wenn

$$ggT(a, n) = 1.$$

Aus der Linearkombination

$$1 = ar + ns$$

erhält man dann $[a]_n^{-1} = [r]_n^{-1}$.

BEWEIS. Wir bezeichnen die Klassen mit $\overline{a}$. Es sind zwei Teile zu zeigen.
Teil 1: zu zeigen ist hier : invertierbar $\Rightarrow ggt = 1$.
Sie $\overline{a}$ invertierbar, dann gibt es ein $\overline{k}$ mit $\overline{ak} = \overline{1}$. Also wissen wir

$$ak \equiv 1 \mod n.$$

Also teilt n die Zahl $ak - 1$, also $nt = ak - 1$ oder aber $ak - nt = 1$, was nach der ggT-Beschreibung als Linearkombination (siehe 2.1.7) bedeutet

$$ggT(a, n) = 1.$$

Teil 2: zu zeigen ist jetzt: $ggT = 1 \Rightarrow$ invertierbar.
Es existiert (wieder wegen der Beschreibung des ggT als Linearkombination) eine Linearkombination

$$1 = ar + ns.$$

Also ist $ar - 1$ durch n teilbar, somit:

$$ar \equiv 1 \mod n.$$

Das bedeutet $\overline{ar} = \overline{1}$, also ist $\overline{a}$ invertierbar und das Inverse ist $\overline{r}$. □

Die Verknüpfung mit dem ggT erlaubt nun, die schon bekannte Methode mit dem erweiterten ggT zu verwenden, um die multiplikativ Inversen zu bestimmen.

EXAMPLE 2.4.10. inverse Klasse mit erweitertem ggT
Wir wollen berechnen ob $[23]_{73}$ invertierbar ist, und wie die inverse Klasse aussieht. Dazu verwenden wir den erweiterten ggT in der Matrixversion

$$\left(\begin{array}{cc|c} 1 & 0 & 23 \\ 0 & 1 & 73 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 23 \\ -3 & 1 & 4 \end{array}\right) \to \left(\begin{array}{cc|c} 16 & -5 & 3 \\ -3 & 1 & 4 \end{array}\right) \to \left(\begin{array}{cc|c} 16 & -5 & 3 \\ -19 & 6 & 1 \end{array}\right)$$

Damit hat man die Linerakombination der 1 :

$$1 = 6 \times 73 - 19 \times 23$$

Das bedeutet, der ggT ist 1, also ist $[23]_{73}$ invertierbar und die inverse Klasse ist $[-19]_{73} = [54]_{73}$.

Im Falle kleiner n ist es eventuell geschickter, einfach die Multiplikation auszuprobieren und zu testen wann 1 modulo n herauskommt. So z.B. für $n = 11$, hier sieht man $7 \times 8 = 56 \equiv 1 \mod 11$.

COROLLARY 2.4.11. *Nullteiler oder invertierbar*
Sei $n > 1$, dann ist jede von $[0]_n$ verschiedene Klasse in $\mathbb{Z}_n$ entweder Nullteiler oder invertierbar, aber nie beides.

BEWEIS. Der Beweis hat zwei Teile.
Teil 1: wir zeigen: nicht invertierbar ⇒Nullteiler
Sei $[a]_n$nicht invertierbar, dann ist nach obigen Satz2.4.9 $ggT(a,n) =: d > 1$ und man hat $n = td$ mit einem $t < n$ (also $[t]_n \neq [0]_n$) und auch $a = kd$. Dann ist aber $[a]_n[t]_n = [at]_n = [kdt]_n = [kn]_n = [0]_n$ und somit ist $[a]_n$ ein Nullteiler.
Teil 2: wir zeigen: invertierbar ⇒nicht Nullteiler
Sei $[a]_n$invertierbar. Betrachte nun eine eventuelle Nullteilergleichung $[a]_n[b]_n = [0]_n$, diese Gleichung wird mit $[a]_n^{-1}$ multipliziert und bekommt dann die Form $[b]_n = [0]_n$, und damit ist $[a]_n$ kein Nullteiler, denn da muss ja nach Definition das $[b]_n \neq [0]_n$ sein. □

Wir wissen also, dass die Menge der Kongruenzklassen in $\mathbb{Z}_n$ in genau drei Teile zerfällt, die Nullklasse $[0]_n$, die Menge der invertierbaren Klassen und die Nullteiler. Die Nullteiler bereiten 'Probleme' es kann passieren, dass bei einer 'normalen' Multiplikation plötzlich das Ergebnis Null ist. Dies ist etwas, was man aus den bisherigen Zahlen nicht kennt. Das folgende Ergebnis (Euler) zeigt wann wir 'schöne' Kongruenzklassen haben.

COROLLARY 2.4.12.
Sei p eine Primzahl, dann sind alle von $[0]_p$ verschiedenen Kongruenzklassen in $\mathbb{Z}_p$ invertierbar.

BEWEIS. Das ist klar, denn aus 2.4.9 wissen wir, dass a invertierbar, falls $ggt(a,p) = 1$, was ja bei Primzahlen für alle $a \neq 0$ gilt. □

Die Menge der invertierbaren Elemente von $\mathbb{Z}_n$ wird mit $\mathbb{Z}_n^*$ bezeichnet, sie hat eine weitere interessante Eigenschaft:

THEOREM 2.4.13. *Abgeschlossenheit von $\mathbb{Z}_n^*$ unter Multiplikation*
Sei $n > 1$. Das Produkt von zwei Elementen (Kongruenzklassen) aus $\mathbb{Z}_n^*$ liegt wieder in $\mathbb{Z}_n^*$.

BEWEIS. Sind zwei Elemente $[a]$ und $[b]$ invertierbar, so bedeutet dies, sie sind teilerfremd zu n, aber dann ist auch das Produkt $[ab]$ teilerfremd, und somit ist auch das Produkt $[ab]$ invertierbar. □

EXAMPLE 2.4.14. Multiplikationstabelle von $\mathbb{Z}_{20}^*$
Die invertierbaren Elemente sind die teilerfremden, also $1, 3, 7, 9, 11, 13, 17, 19$. Die Multiplikationstabelle sieht dann so aus:

×	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

Die Anzahl der Elemente in $\mathbb{Z}_n^*$ wird mit $\phi(n)$ bezeichnet. Diese Funktion heisst auch *Eulersche - Phi - Funktion*. Nach obigen Ergebnis kann sie wie folgt definiert werden:

$$\phi(n) := |\{i \in N : 1 \leq i \leq n \text{ und } ggT(i,n) = 1\}|$$

THEOREM 2.4.15. *einfache Eigenschaften von $\phi(n)$*
Sei p eine Primzahl und $n \in \mathbb{N}$ positiv. Dann ist

$$\phi(p^n) = p^n - p^{n-1}.$$

BEWEIS. Welche Zahlen zwischen 1 und p^n haben einen Teiler mit p^n gemeinsam? Dies sind gerade die Vielfachen von p, davon gibt es genau p^n/p viele. Das Komplement davon sind gerade die teilerfremden Zahlen, die ja von ϕ gezählt werden. Also $\phi(p^n) = p^n - p^{n-1}$. □

THEOREM 2.4.16. *Berechnung von $\phi(n)$*
Sei $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ die eindeutige Primexponentendarstellung von n.Dann ist

$$\phi(n) = n \prod_{i=1\dots s} (1 - \frac{1}{p_i})$$

BEWEIS. (Inklusion-Exklusion)
Um die Anzahl der teilerfremden Zahlen $\leq n$ zu bestimmen beginnt man mit allen Zahlen, dies sind n Stück. Davon müssen die Vielfachen der verschiedenen Primzahlen abgezogen werden:

$$n - \frac{n}{p_1} - \dots - \frac{n}{p_s} = n - \sum_{i=1\dots s} \frac{n}{p_i}$$

Dabei wurden zuviel abgezogen, nämlich gerade die Zahlen die Vielfaches eines Produkts zweier Primzahlen waren, also muss korrigiert werden.

$$n - \sum_{i=1\dots s} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j}$$

Auch das muss korrigiert werden, nämlich wurde zuviel addiert, gerade um die Produkte von drei Primzahlen, dies geht bis zu den Produkten aus den s verschiedenen Primzahlen, insgesamt hat man:

$$\phi(n) = n - \sum_{i=1\dots s} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \dots (-1)^s \frac{n}{p_1 p_2 \dots p_s}.$$

Klammert man nun n aus und multipliziert die rechte Seite aus (direkte Multiplikation der Differenzen), dann sieht man

$$n - \sum_{i=1\dots s} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \dots (-1)^s \frac{n}{p_1 p_2 \dots p_s} = n \prod_{i=1\dots s} (1 - \frac{1}{p_i}).$$

□

COROLLARY 2.4.17. *ϕ ist eine multiplikative Funktion*
Seien a, b teilerfremd, dann gilt

$$\phi(ab) = \phi(a)\phi(b).$$

BEWEIS. Direkt aus obigen Theorem zur Berechnung der ϕ Funktion. □

2.4.1. Ordnung von Elementen in $\mathbb{Z}_n$. Dazu betrachtet man was, beim Bilden von Potenzen der Kongruenzklassen passiert. Dies ist auch die Operation, die später im RSA Verschlüsselungsverfahren verwendet wird.

EXAMPLE 2.4.18. Potenzen von Kongruenzklassen.
Betrachte in $\mathbb{Z}_{20}$ die Potenzen von $[3]$:

Exponent	1	2	3	4	5	...	
Ergebnis	[3]	[9]	[27] = [7]	[21] = [1]	[3]	...	

Betrachtet man die Potenzen von $[4]$:

Exponent	1	2	3	4	5	...	
Ergebnis	[4]	[16]	[64] = [4]	[16]	[4]	...	

Betrachtet man die Potenzen von $[10]$:

Exponent	1	2	3	4	5	...	
Ergebnis	$[10]$	$[100] = [0]$	$[0]$	$[0]$	$[0]$	...	

Es ist klar, dass sich die Werte wiederholen (es gibt unendlich viele Potenzen, und nur endlich viele Elemente). Eine spezielle Situation, sind die Startwerte wo man wieder zur $[1]_n$, und damit zum Ausgangswert zurück kommt. Das motiviert die folgende Definition:

DEFINITION 2.4.19. multiplikative Ordnung

Sei $n > 1$ eine natürliche Zahl. $a \in \mathbb{N}$ hat eine *endliche (multiplikative) Ordnung modulo* n falls ein $k > 0$ gibt mit:

$$([a]_n)^k = [1]_n.$$

Die kleinste solche Zahl k heisst dann die *Ordnung* von a modulo n, oder auch die *Ordnung* von $[a]_n$.

Obiges Beispiel zeigt: die Ordnung von $[3]_{20}$ ist 4. Man kann die Elemente endlicher Ordnung in Z_n charakterisieren:

THEOREM 2.4.20. *Beschreibung der Elemente endlicher Ordnung in* $\mathbb{Z}_n$

$a \in \mathbb{N}$ *hat endliche Ordnung modulo* n *genau dann wenn* $ggT(a, n) = 1$.

BEWEIS. Es sind zwei Dinge zu beweisen:
Teil 1: endliche Ordnung ⇒ggT=1
a habe endliche Ordnung, dann existiert ein $k > 0$ mit $[a^k] = [a][a^{k-1}] = [1]$. Dann ist aber $[a^{k-1}]$ das inverse Element, also ist $[a]$ invertierbar, und daher nach dem Satz 2.4.9 ist $ggT(a, n) = 1$.
Teil 2: ggt=1 ⇒endliche Ordnung
Sei $ggT(a, n) = 1$, dann ist nach dem gleichen Satz $[a]$ invertierbar, dann sind auch alle Potenzen von $[a]$ invertierbar (denn $[a^s]^{-1} = [a^{-1}]^s$). Betrachte nun die $n+1$ Kongruenzklassen $[a], [a]^2, \ldots, [a]^{n+1}$. Davon müssen zwei identisch sein (mit $1 \leq s < t \leq n-1$):

$$[a]^s = [a]^t.$$

Nun multipliziert man mit $[a]^{-s}$:

$$[1] = [a]^{t-s}.$$

Also hat $[a]$ endliche Ordnung. □

THEOREM 2.4.21. *Satz von Fermat*

Sei p *eine Primzahl, und* $a \in \mathbb{N}$ *mit* $ggT(a, p) = 1$ *dann gilt:*

$$[a]_p^{p-1} = [1]_p.$$

BEWEIS. Wir wissen:

$$\mathbb{Z}_p^* = \{[1], \ldots, [p-1]\}.$$

Betrachte nun die Vielfachen einer Kongruenzklasse $[a]$ in $\mathbb{Z}_p^*$:

$$[a]\mathbb{Z}_p^* = \{[a][b] : [b] \in \mathbb{Z}_p^*\}.$$

Diese Produkte $[a][b]$ liegen alle in $\mathbb{Z}_p^*$, und es sind genau $p-1$ verschiedene Produkt, denn durch Multiplikation mit $[a]^{-1}$ ($[a]$ ist invertierbar) sieht man:

$$[a][b] = [a][c] \iff [b] = [c].$$

Also wissen wir:

$$\mathbb{Z}_p^* = [a]\mathbb{Z}_p^*.$$

Multipliziert man alle Elemente auf beiden Seiten auf, so erhält man

$$[x] = [a]^{p-1}[x],$$

und da $[x]$ invertierbar ist, bekommt man so:

$$[1] = [a]^{p-1}.$$

□

Dieses Ergebnis von Fermat (angekündigt in einem Brief von 1640) wurde vor 1750 von Euler in obiger Art bewiesen, und um 1750 verallgemeinert:

THEOREM 2.4.22. *Satz von Euler*
Sei $n > 1$, *und* $a \in \mathbb{N}$ *mit* $ggT(a, n) = 1$ *dann gilt:*

$$[a]_n^{\phi(n)} = [1]_n.$$

BEWEIS. Wir gehen genauso vor wie beim Beweis des Satzes von Fermat. Wir bemerken zuerst

$$\mathbb{Z}_n^* = [a]\mathbb{Z}_n^*,$$

nach der Multiplikation erhalten wir

$$[x] = [a]^{\phi(n)}[x],$$

was bedeutet:

$$[1] = [a]^{\phi(n)}.$$

□

Will man zum Beispiel die letzten beiden Stellen von 3^{125} bestimmen, kann man wie folgt vorgehen: Die letzten beiden Stellen entsprechen dem Wert modulo 100. Man bestimmt

$$\phi(100) = \phi(2^2)\phi(5^2) = (4-2)(25-5) = 40,$$

und damit

$$3^{125} = (3^{40})^3 \times 3^5 \equiv 1 \times 243 \equiv 43 \mod 100.$$