

Kürzungsregel für Kongruenzen



Erinnere dich an die folgende Rechenregel für Kongruenzen:

$$a \cdot c \equiv b \cdot c \pmod m \iff a \equiv b \pmod{\frac{m}{\text{ggT}(c,m)}}$$

Eine Erklärung für die Rechenregel findest du am [Arbeitsblatt – Kongruenz und Restklassen](#).

Wenn  $c$  und  $m$  teilerfremd sind, dann gilt also:

$$a \cdot c \equiv b \cdot c \pmod m \iff a \equiv b \pmod m$$

Kleiner Satz von Fermat (1640)



Für jede ganze Zahl  $a$  und jede Primzahl  $p$  gilt der **Kleine Satz von Fermat**:

$$a^p \equiv a \pmod p$$

Zum Beispiel:  $4^5 \equiv 4 \pmod 5$   
=1024

Wenn  $a$  kein Vielfaches von  $p$  ist, dann gilt  $\text{ggT}(a,p) = 1$  und damit:

$$a^{p-1} \equiv 1 \pmod p$$

Pascalsches Dreieck & Primzahlen



$p$  ist eine Primzahl. Rechts siehst du die obersten 12 Reihen vom **Pascalschen Dreieck**:

In jeder „Primzahlreihe“ sind alle **Zahlen im Inneren** jeweils Vielfache dieser Primzahl.

Zum Beispiel: Die Zahlen

$$7, 21, 35, 35, 21, 7$$

sind alle durch  $7$  teilbar.

Das ist kein Zufall.

				1																						
				1		1																				
		$p = 2$		1		2		1																		
		$p = 3$		1		3		3		1																
				1		4		6		4		1														
		$p = 5$		1		5		10		10		5		1												
				1		6		15		20		15		6		1										
		$p = 7$		1		7		21		35		35		21		7		1								
				1		8		28		56		70		56		28		8		1						
				1		9		36		84		126		126		84		36		9		1				
				1		10		45		120		210		252		210		120		45		10		1		
		$p = 11$		1		11		55		165		330		462		462		330		165		55		11		1

Die Zahlen in Reihe  $p$  sind die folgenden **Binomialkoeffizienten**:

$$\binom{p}{0}, \binom{p}{1}, \binom{p}{2}, \binom{p}{3}, \dots, \binom{p}{p-1}, \binom{p}{p} \quad \text{mit} \quad \binom{p}{k} = \frac{\overbrace{p \cdot (p-1) \cdot (p-2) \cdot \dots \cdot (p-k+1)}^{k \text{ Faktoren}}}{k!}$$

Erkläre, warum die Primzahl  $p$  den Binomialkoeffizienten  $\binom{p}{k}$  für alle  $k$  mit  $1 \leq k \leq p-1$  teilt.

Im Zähler von  $\binom{p}{k}$  kommt der Faktor  $p$  vor, weil  $k \geq 1$ .

Der Nenner  $k!$  und  $p$  sind teilerfremd, weil  $p$  eine Primzahl ist und  $k \leq p-1$ .

Das Ergebnis  $\binom{p}{k}$  der Division ist eine ganze Zahl, deren Primfaktorzerlegung also  $p$  enthalten muss.



Wir beweisen jetzt  $a^p \equiv a \pmod p$  für alle Primzahlen  $p$  mit **vollständiger Induktion** nach  $a \geq 0$ .  
Dabei verwenden wir die beiden folgenden Aussagen:

- **Binomischer Lehrsatz:**  $(x + y)^n = \sum_{k=0}^n \binom{n}{k} \cdot x^k \cdot y^{n-k}$
- $\binom{p}{k} \equiv 0 \pmod p$  für alle Primzahlen  $p$  und  $1 \leq k \leq p - 1$ .

1) Überprüfe den **Induktionsanfang** für  $a = 0$ :

$$0^p \equiv 0 \pmod p \checkmark$$

2) Überprüfe den **Induktionsschritt**  $a \rightarrow a + 1$ :

Du darfst also verwenden, dass  $a^p \equiv a \pmod p$  gilt.

Daraus musst du folgern, dass auch  $(a + 1)^p \equiv a + 1 \pmod p$  gilt.

$$(a+1)^p = \sum_{k=0}^p \binom{p}{k} \cdot a^k \cdot 1^{p-k} = \underbrace{\binom{p}{p} \cdot a^p \cdot 1^0}_{=a^p \ (k=p)} + \underbrace{\binom{p}{0} \cdot a^0 \cdot 1^p}_{=1 \ (k=0)} + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k} \cdot a^k \cdot 1^{p-k}}_{\equiv 0 \pmod p} \equiv a^p + 1 \pmod p$$

$$\implies (a + 1)^p \equiv a^p + 1 \equiv a + 1 \pmod p \checkmark$$

□



1) Für die gerade Primzahl  $p = 2$  können wir  $a^2 \equiv a \pmod 2$  für alle ganzen Zahlen  $a$  direkt beweisen:

- Wenn  $a$  gerade ist, dann ist  $a^2$  eine **gerade / ungerade** Zahl. Streiche jeweils durch.
- Wenn  $a$  ungerade ist, dann ist  $a^2$  eine **gerade / ungerade** Zahl.

Die ganzen Zahlen  $a$  und  $a^2$  liegen also in der gleichen Restklasse modulo 2.

2) Für jede ungerade Primzahl  $p$  und *negative* ganze Zahl  $a$  haben wir  $(-a)^p \equiv (-a) \pmod p$  gezeigt.  
Folgere daraus, dass auch  $a^p \equiv a \pmod p$  gilt.

$(-a)^p = -a^p$ , weil  $p$  ungerade ist.

$$(-a)^p \equiv (-a) \pmod p \implies -a^p \equiv (-a) \pmod p \xrightarrow{\cdot(-1)} a^p \equiv a \pmod p$$

Also gilt  $a^p \equiv a \pmod p$  auch für alle negativen ganzen Zahlen  $a$ .

Leonhard Euler (1707-1783) bewies, dass eine Verallgemeinerung von  $a^{p-1} \equiv 1 \pmod p$  nicht nur für Primzahlen  $p$  stimmt, sondern für beliebige natürliche Zahlen.

Als Nächstes sehen wir uns diesen **Satz von Euler** und einen eleganten Beweis dafür an.

Der Satz von Euler spielt eine wichtige Rolle in der modernen Verschlüsselung.

Mehr dazu erfährst du am [Arbeitsblatt – RSA-Verfahren](#).

Eulersche Phi-Funktion



MATHEMATIK  
macht  
FREU(N)DE

Die **Eulersche Phi-Funktion**  $\varphi$  ist für jede natürliche Zahl  $n \geq 1$  definiert.  
 $\varphi(n)$  ist die Anzahl natürlicher Zahlen  $a$ , für die  $1 \leq a \leq n$  und  $\text{ggT}(a, n) = 1$  gilt. Kurz:

$$\varphi(n) = |\{a \in \mathbb{N} \mid 1 \leq a \leq n \wedge \text{ggT}(a, n) = 1\}|$$

Eulersche Phi-Funktion

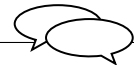


MATHEMATIK  
macht  
FREU(N)DE

Ermittle die folgenden Funktionswerte der Eulerschen Phi-Funktion.

- |                     |                     |                     |                        |
|---------------------|---------------------|---------------------|------------------------|
| 1) $\varphi(1) = 1$ | 4) $\varphi(4) = 2$ | 7) $\varphi(7) = 6$ | 10) $\varphi(10) = 4$  |
| 2) $\varphi(2) = 1$ | 5) $\varphi(5) = 4$ | 8) $\varphi(8) = 4$ | 11) $\varphi(11) = 10$ |
| 3) $\varphi(3) = 2$ | 6) $\varphi(6) = 2$ | 9) $\varphi(9) = 6$ | 12) $\varphi(12) = 4$  |

Eulersche Phi-Funktion



MATHEMATIK  
macht  
FREU(N)DE

$p$  und  $q$  sind verschiedene Primzahlen.

- 1) Für welche natürlichen Zahlen  $a$  mit  $1 \leq a \leq p$  gilt  $\text{ggT}(a, p) = 1$ ?

$$1, 2, 3, \dots, p-1 \implies \varphi(p) = p-1$$

- 2) Für welche natürlichen Zahlen  $a$  mit  $1 \leq a \leq p^k$  gilt *nicht*  $\text{ggT}(a, p^k) = 1$ ?

$$1 \cdot p, 2 \cdot p, 3 \cdot p, \dots, p^{k-1} \cdot p \implies \varphi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$$

- 3) Für welche natürlichen Zahlen  $a$  mit  $1 \leq a \leq p \cdot q$  gilt *nicht*  $\text{ggT}(a, p \cdot q) = 1$ ?

Vielfache von  $p$ , die  $\leq p \cdot q$  sind:

$$\underbrace{1 \cdot p, 2 \cdot p, 3 \cdot p, \dots, (q-1) \cdot p, q \cdot p}_{q \text{ Zahlen}}$$

Vielfache von  $q$ , die  $\leq p \cdot q$  sind:

$$\underbrace{1 \cdot q, 2 \cdot q, 3 \cdot q, \dots, (p-1) \cdot q, p \cdot q}_{p \text{ Zahlen}}$$

$$\implies \varphi(p \cdot q) = p \cdot q - (p + q - 1) = (p-1) \cdot (q-1) = \varphi(p) \cdot \varphi(q)$$

Multiplikativität der Eulerschen Phi-Funktion



MATHEMATIK  
macht  
FREU(N)DE

Tatsächlich ist die Eulersche Phi-Funktion für alle *teilerfremden* Zahlen  $m$  und  $n$  multiplikativ.

Aus  $\text{ggT}(m, n) = 1$  folgt also  $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ .

Primfaktorzerlegung von  $n \sim \varphi(n)$



MATHEMATIK  
macht  
FREU(N)DE

Zerlege  $n$  in Primfaktoren und berechne  $\varphi(n)$ .

- a)  $n = 42$

$$42 = 2 \cdot 3 \cdot 7$$

$$\implies \varphi(42) = \varphi(2) \cdot \varphi(3) \cdot \varphi(7) \\ = 1 \cdot 2 \cdot 6 = 12$$

- b)  $n = 360$

$$360 = 2^3 \cdot 3^2 \cdot 5$$

$$\implies \varphi(360) = \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(5) \\ = 4 \cdot 6 \cdot 4 = 96$$



Wenn  $\text{ggT}(a, n) = 1$  ist, dann gilt der **Satz von Euler**:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Wenn  $n$  eine Primzahl ist, dann ist das der Satz von Fermat.

mod 100



Ermittle mit dem Satz von Euler die letzten beiden Dezimalstellen von  $23^{42}$ .

$$n = 100 = 2^2 \cdot 5^2 \implies \varphi(100) = \varphi(2^2) \cdot \varphi(5^2) = 2 \cdot 20 = 40$$

Der Satz von Euler garantiert also  $a^{40} \equiv 1 \pmod{100}$  für alle Zahlen  $a$  mit  $\text{ggT}(a, 100) = 1$ .

$$\text{ggT}(23, 100) = 1 \implies 23^{42} = \underbrace{23^2}_{=529} \cdot \underbrace{23^{40}}_{\equiv 1 \pmod{100}} \equiv 529 \pmod{100}$$

Die beiden letzten Stellen von  $23^{42}$  sind also 29.

Kongruenz & ggT



Für den Beweis vom Satz von Euler verwenden wir zwei Eigenschaften:

1)  $a \equiv b \pmod{n} \implies \text{ggT}(a, n) = \text{ggT}(b, n)$

Alle Zahlen, die in der gleichen Restklasse modulo  $n$  sind, haben mit  $n$  den gleichen größten gemeinsamen Teiler.

Begründe die Aussage:

Hinweis:  $\text{ggT}(a + k \cdot n, n) = \text{ggT}(a, n)$

$$\begin{aligned} a \equiv b \pmod{n} &\implies b = a + k \cdot n \text{ mit einer ganzen Zahl } k \\ &\implies \text{ggT}(b, n) = \text{ggT}(a + k \cdot n, n) = \text{ggT}(a, n) \end{aligned}$$

2) Wenn  $\text{ggT}(a, n) = 1$ , dann gilt:  $x \cdot a \equiv y \cdot a \pmod{n} \iff x \equiv y \pmod{n}$

Satz von Euler – Beweis



Damit beweisen wir jetzt  $a^{\varphi(n)} \equiv 1 \pmod{n}$  für alle Zahlen  $a$  mit  $\text{ggT}(a, n) = 1$ .

Unter den Zahlen  $\{1, 2, 3, \dots, n\}$  gibt es  $\varphi(n)$  verschiedene Zahlen, die zu  $n$  teilerfremd sind.

Wir geben diesen  $\varphi(n)$  verschiedenen Zahlen jeweils einen Namen:  $\{a_1, a_2, a_3, \dots, a_{\varphi(n)}\}$

Aus  $\text{ggT}(a_i, n) = 1$  und  $\text{ggT}(a, n) = 1$  folgt  $\text{ggT}(a_i \cdot a, n) = 1$ .

Wegen 1) muss  $a_i \cdot a$  in der gleichen Restklasse modulo  $n$  wie eine der Zahlen  $\{a_1, a_2, \dots, a_{\varphi(n)}\}$  sein.

Wegen 2) sind die Zahlen  $a_1 \cdot a, a_2 \cdot a, \dots, a_{\varphi(n)} \cdot a$  alle in verschiedenen Restklassen modulo  $n$ , denn:

$$a_i \cdot a \equiv a_j \cdot a \pmod{n} \xrightarrow{2)} a_i \equiv a_j \pmod{n} \implies a_i = a_j \quad \text{„Indirekter Beweis“}$$

Die Multiplikation mit  $a$  vertauscht also nur die Reihenfolge der  $\varphi(n)$  verschiedenen Restklassen.

$$\implies a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(n)} \equiv (a_1 \cdot a) \cdot (a_2 \cdot a) \cdot \dots \cdot (a_{\varphi(n)} \cdot a) \pmod{n}$$

$$\implies a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(n)} \equiv a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(n)} \cdot a^{\varphi(n)} \pmod{n}$$

$$\xrightarrow{2)} 1 \equiv a^{\varphi(n)} \pmod{n} \quad \square$$