zeige: $ggT(m,n) = ggT(m, n+l\cdot m)$ für alle $m,n,l \in \mathbb{N}$.

Bew.: (i) $ggT(m,n) \mid ggT(m, n+l\cdot m)$

Seien $m,n,l \in \mathbb{N}$.

Dazu: $ggT(m,n) \mid m$

$ggT(m,n) \mid n$, d.h. es ex. $k_1, k_2 \in \mathbb{N}$ mit

$$m = k_1 \cdot ggT(m,n)$$
$$n = k_2 \cdot ggT(m,n)$$

Es ist: $n + l\cdot m = k_2 \cdot ggT(m,n) + l \cdot k_1 \cdot ggT(m,n)$

$$= \underbrace{(k_2 + l\cdot k_1)}_{\in \mathbb{N}} \cdot ggT(m,n)$$

$\Rightarrow ggT(m,n) \mid n + l\cdot m$

da ebenso auch $ggT(m,n) \mid m$,

folgt $ggT(m,n) \mid ggT(m, n+l\cdot m)$.

(ii) $ggT(m,n) = ggT(m, n+l\cdot m)$:

$\rightsquigarrow ggT(k_1,k_2) = 1$.

Von oben $m = k_1 \cdot ggT(m,n)$

$n + l\cdot m = (k_2 + l\cdot k_1) \cdot ggT(m,n)$

$\longrightarrow$ d.h. noch zz ist $\boxed{ggT(k_1, k_2 + l\cdot k_1) = 1.}$

Angenommen, $ggT(k_1, k_2 + l\cdot k_1) > 1$,

$\| \cdot g$

dann: $\boxed{g \mid k_1}$ $g \mid k_2 + l\cdot k_1$

d.h. $k_1 = g_1 \cdot g$, $k_2 + l\cdot k_1 = g_2 \cdot g$ mit $g_1, g_2 \in \mathbb{N}$

$\Rightarrow k_2 = g_2 \cdot g - l\cdot k_1$

$= g_2 \cdot g - l \cdot g_1 \cdot g$

$= (g_2 - l \cdot g_1) \cdot g$

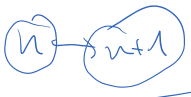
$\in \mathbb{Z}$ $(\in \mathbb{N})$

$\Rightarrow g \mid k_2$

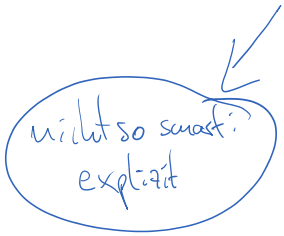
$\Rightarrow g \mid ggT(k_1, k_2) = 1$

$\Rightarrow g \leq 1$ bzw. $g = 1$. ↯ zu oben

d.h. $ggT(k_1, k_2 + l \cdot k_1) = 1$. □



$17^{2047} \mod 79$.



smart: 79 ist eine Primzahl.

↳ $(\mathbb{Z}/79\mathbb{Z})^*$ ist eine Gruppe mit 78 Elementen.

↳ für endliche Gruppen gilt:

> Sei G eine Gruppe mit n Elementen und $g \in G$ beliebig.
> Dann gilt $g^n = 1$.

↳ $17^{78} \equiv 1 \mod 79$

↳ $17^{k \cdot 78} \equiv (17^{78})^k \equiv 1^k \equiv 1 \mod 79$ ↳ für alle $k \in \mathbb{N}$

Es gilt: $2047 = 26 \cdot 78 + 19$

Also: $17^{2047} \equiv 17^{19+26 \cdot 78} \equiv 17^{19} \cdot 17^{26 \cdot 78}$

$\equiv 17^{19} \mod 79$

$\equiv 17 \cdot (17^2)^9$

$\equiv 17 \cdot 289^9$

$\equiv 17 \cdot 17^9$

M.i.TR zur Verfügung: $17^1, 17^2, 17^3, 17^4, 17^5$ ///

Betrachte kleine Potenzen modulo 79

↳ ziehe aus 17^{19} möglichst

Betrachte kleine Potenzen modulo 79

& ziehe aus 17^{19} möglichst viele kl. Potenzen heraus, die mod 79 betragsmäßig klein sind.

$\equiv 17 \cdot 289^9$

$\equiv 17 \cdot 52^9$

$\equiv 17 \cdot (-27)^9$

$\equiv 17 \cdot ((-27)^3)^3$

$\equiv 17 \cdot (-19683)^3$

$\equiv 17 \cdot (-12)^3$

$\equiv -17 \cdot 144 \cdot 12$

$\equiv -17 \cdot (-14) \cdot 12$

$\equiv 238 \cdot 12$

$\equiv 12 \mod 79$

Gesucht: $17^{-1} \mod 19$.

1.) 19 ist eine Primzahl, d.h. $17^{18} \equiv 1 \mod 19$ (s.o. für Begr.)

$\Rightarrow 17^{-1} \equiv 17^{17} \mod 19$ (**)

$\rightsquigarrow$ berechne $17^{17} \mod 19$,

z.B.: $17^{17} \equiv (-2)^{17} \equiv -2 \cdot (2^8)^2$

$\equiv 256^2 \cdot (-2)$

$\equiv 9^2 \cdot (-2)$

$\equiv 81 \cdot (-2)$

$\equiv 5 \cdot (-2)$

$\equiv -10 \equiv 9 \mod 19$.

$17^{-1} \equiv 9 \mod 19$ (Probe: $9 \cdot 17 = 153$
$= 8 \cdot 19 + 1$
$\equiv 1 \mod 19$)

2.) mit erweitertem eukl. Algor.:

$19 = 1 \cdot 17 + 2 \rightsquigarrow 2 = 19 - 1 \cdot 17$

$17 = 8 \cdot 2 + 1 \rightsquigarrow 1 = 17 - 8 \cdot 2 = 17 - 8 \cdot (19 - 1 \cdot 17)$

$2 = 2 \cdot 1 + 0$

$= -8 \cdot 19 + 9 \cdot 17$

$\text{ggT}(17, 19)$

$\overset{\text{mod } 19}{\Rightarrow} 1 \equiv 9 \cdot 17 \mod 19$

$\Rightarrow 9 \equiv 17^{-1} \mod 19$.

$\Rightarrow 9 \equiv 17^{-1} \mod 19$.

gesucht: "$\frac{3}{4} \in \mathbb{F}_{19}$", d.h. $3 \cdot 4^{-1} \in \mathbb{F}_{19}$.

$\rightsquigarrow$ Berechne zuerst 4^{-1}, danach $3 \cdot 4^{-1}$

Dazu: (mit 2.1):

$19 = 4 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$

ggT(4,19)

$3 = 19 - 4 \cdot 4$

$1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (19 - 4 \cdot 4)$

$= -1 \cdot 19 + 5 \cdot 4$

$\Rightarrow 1 \equiv 5 \cdot 4 \mod 19$

$\Rightarrow 4^{-1} \equiv 5 \mod 19$

$\Rightarrow 3 \cdot 4^{-1} \equiv 3 \cdot 5 \equiv 15 \mod 19$.

$\frac{3}{4} = 3 \cdot \frac{1}{4} = 3 \cdot 4^{-1}$

$= \frac{1}{4} \cdot 3 = 4^{-1} \cdot 3$

$\rightsquigarrow$ in Körpern (wie z.B. $\mathbb{F}_{19}$) spielt die Reihenfolge der Multiplikation keine Rolle

$\rightsquigarrow$ in Ringen aber muss die Multiplikation nicht unbedingt kommutativ sein, d.h. $a \cdot b \neq b \cdot a$ (Bsp.: Matrizenringe).

$\rightsquigarrow$ Körper können auch als Ringe aufgefasst werden; wenn man mit Körpern (aufgefasst als Ringe) und nicht-kommutativen Ringen gleichzeitig arbeitet, ist die Notation mit Brüchen "gefährlich".