

### Kleiner Satz von Fermat

Ist  $a \in \mathbb{N}$  kein Vielfaches der Primzahl  $p$ , so ist  $a^{p-1} \equiv 1 \pmod{p}$ .

Beispiel:  $p = 7$

a	a Vielfaches von 7?	$a^6$	Rest von $a^6$ bei Division durch 7	$a^{7-1} \equiv 1 \pmod{7}$ ?
1	nein	$1^6 = 1$	$= 0 \cdot 7 + \underline{1}$	ja
2	nein	$2^6 = 64$	$= 9 \cdot 7 + \underline{1}$	ja
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

Der kleine Satz von Fermat gilt nicht für zusammengesetzte Zahlen  $p$ , selbst dann nicht, wenn man die Voraussetzung „ $a$  kein Vielfaches von  $p$ “ in „ $\text{ggT}(a, p) = 1$ “ ändert.

Beispiel:  $p = 8$

a	a Vielfaches von 8?	$\text{ggT}(a, 8)$	$a^7$	Rest von $a^7$ bei Division durch 8	$a^{8-1} \equiv 1 \pmod{8}$ ?
1	nein	1	1	$= 0 \cdot 8 + \underline{1}$	ja
2					
3					
4					
5					
6					
7					
8					
9					
10					

Obwohl  $\text{ggT}(\_, 8) = \_$ , ist  $\_$  modulo  $\_$ .

### Kleiner Satz von Fermat

Ist  $a \in \mathbb{N}$  kein Vielfaches der Primzahl  $p$ , so ist  $a^{p-1} \equiv 1 \pmod{p}$ .

Beispiel:  $p = 7$

a	a Vielfaches von 7?	$a^6$	Rest von $a^6$ bei Division durch 7	$a^{7-1} \equiv 1 \pmod{7}$ ?
1	nein	$1^6 = 1$	$= 0 \cdot 7 + \underline{1}$	ja
2	nein	$2^6 = 64$	$= 9 \cdot 7 + \underline{1}$	ja
3	nein	$3^6 = 729$	$= 104 \cdot 7 + \underline{1}$	ja
4	nein	$4^6 = 4096$	$= 585 \cdot 7 + \underline{1}$	ja
5	nein	15625	$= 2232 \cdot 7 + \underline{1}$	ja
6	nein	46656	$= 6665 \cdot 7 + \underline{1}$	ja
7	ja	117649	$= 16807 \cdot 7 + \underline{0}$	nein
8	nein	262144	$= 37449 \cdot 7 + \underline{1}$	ja
9	nein	531441	$= 57920 \cdot 7 + \underline{1}$	ja
10	nein	1000000	$= 142857 \cdot 7 + \underline{1}$	ja
11	nein	1771561	$= 253080 \cdot 7 + \underline{1}$	ja
12	nein	2985984	$= 426569 \cdot 7 + \underline{1}$	ja
13	nein	4826809	$= 689544 \cdot 7 + \underline{1}$	ja
14	ja	7529536	$= 1075648 \cdot 7 + \underline{0}$	nein
15	nein	11390625	$= 1627232 \cdot 7 + \underline{1}$	ja
16	nein	16777216	$= 2396745 \cdot 7 + \underline{1}$	ja
17	nein	24137569	$= 3448224 \cdot 7 + \underline{1}$	ja
18	nein	34012224	$= 4858889 \cdot 7 + \underline{1}$	ja
19	nein	47045881	$= 6720840 \cdot 7 + \underline{1}$	ja
20	nein	64000000	$= 9142857 \cdot 7 + \underline{1}$	ja
21	ja	85766121	$= 12252303 \cdot 7 + \underline{0}$	nein
22	nein	113379904	$= 16197129 \cdot 7 + \underline{1}$	ja
23	nein	148035889	$= 21147984 \cdot 7 + \underline{1}$	ja
24	nein	191102976	$= 27300425 \cdot 7 + \underline{1}$	ja
25	nein	244140625	$= 34877232 \cdot 7 + \underline{1}$	ja

Der kleine Satz von Fermat gilt **nicht** für zusammengesetzte Zahlen  $p$ , selbst dann nicht, wenn man die Voraussetzung „a kein Vielfaches von p“ in „ $\text{ggT}(a, p) = 1$ “ ändert.

Beispiel:  $p = 8$

a	a Vielfaches von 8?	$\text{ggT}(a, 8)$	$a^7$	Rest von $a^7$ bei Division durch 8	$a^{8-1} \equiv 1 \pmod{8}$ ?
1	nein	1	1	$= 0 \cdot 8 + \underline{1}$	ja
2	nein	2	128	$= 16 \cdot 8 + \underline{0}$	nein
3	nein	1	2187	$= 273 \cdot 8 + \underline{3}$	nein
4	nein	4	16384	$= 2048 \cdot 8 + \underline{0}$	nein
5	nein	1	78125	$= 9765 \cdot 8 + \underline{5}$	nein
6	nein	2	279936	$= 34992 \cdot 8 + \underline{0}$	nein
7	nein	1	823543	$= 102942 \cdot 8 + \underline{7}$	nein
8	ja	8	2097152	$= 262144 \cdot 8 + \underline{0}$	nein
9	nein	1	4782969	$= 597871 \cdot 8 + \underline{1}$	ja
10	nein	2	10000000	$= 1250000 \cdot 8 + \underline{0}$	nein

Obwohl  $\text{ggT}(3, 8) = 1$ , ist  $3^{8-1}$  nicht kongruent zu 1 modulo 8.