

## Fermats lilla sats

Om  $a$  är ett heltal,  $p$  ett primtal, och  $p \nmid a$ , då är

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

Bevis då  $p=7$

Ta talet  $a$  och titta på de 6 talen

$$a, 2a, 3a, 4a, 5a, 6a$$

Desse, när reducerade mod  $p$ , är precis

$$1, 2, 3, 4, 5, 6 \quad (\text{ev i omvänd ordning})$$

$a, 2a, \dots, 6a$  annorlunda mod 7?

$$\text{då: } 0 \text{ om } 3a \equiv 5a \pmod{7}$$

$$\text{då är } 2a \equiv 0 \pmod{7}$$

$$\text{så } a \equiv 0 \pmod{7}$$

men det stämmer inte

$$a \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv a \cdot (2a) \cdot (3a) \cdot (4a) \cdot (5a) \cdot (6a) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}$$

$$a^6 \equiv 1 \pmod{7}$$

Låt  $n \geq 1$

Oavsett hur man tar bort en ruta från ett  $2^n \times 2^n$ -bräde, så går det att täcka brädet med  $\text{L}$ -brickor ('triominoes')

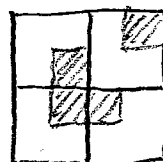
Basfall  $n=1$   $2 \times 2$ -bräde med 1 ruta borttagen



Oavsett ruta går denna att täcka med L-brickor

Induktionssteget Anta att jag kan täcka alla  $2^{n-1} \times 2^{n-1}$ -bräden med en ruta borttagen.

Då kan jag göra det för  $2^n \times 2^n$  enligt bilden



Slutsats Eftersom  $n=1$  fallet håller och fallet  $n \leq k$  innebär fallet  $n=k+1$  så håller påståendet för alla  $n=1, 2, 3, \dots$   $\square$