# Aflevering i uge 40

**Proposition.** *Lad $n \in \mathbb{N}\backslash\{1\}$, og antag, at $(n-1)! \equiv -1 \bmod n$. Da er $n$ et primtal.*

**Bevis.** Jeg vil føre en modstrid: Antag, at $n$ ikke er et primtal, da kan $n$ skrives på formen $n = ab$, hvor $a, b \in \mathbb{N}$ og $1 < a, b < n$. Der er nu to muligheder, nemlig 1) $a \neq b$ eller 2) $a = b$. Jeg ser på de to muligheder hver for sig:

1) Da $a \neq b$, har jeg $a, b \in \{2, 3, \ldots, n-2, n-1\}$,[1] så både $a$ og $b$ er faktorer i $(n-1)!$. Heraf følger det, at $(n-1)! \equiv 0 \bmod n$, som strider mod antagelsen.

2) Jeg har $a = b$.[2] Lad nu $s$ være givet, så $as = (n-1)!$. Af $(n-1)! \equiv -1 \bmod n$ har jeg dermed følgende:

$$as = -1 + a^2 t \Leftrightarrow a(at - s) = 1. \tag{1}$$

   Da $a > 1$, er $a(at - s) > 1$, hvilket strider mod (1).

Da jeg har vist, at både 1) og 2) fører til en modstrid, er beviset fuldført. □

[1] Jeg antager her, at $n \geq 4$, men stadig er $(2-1)! \equiv -1 \bmod 2$ og $(3-1)! \equiv -1 \bmod 3$.

[2] Her antages, at $a$ og $b$ er primtal, ellers har jeg jo med $a = cd$, at $n = a^2 = c^2 d^2$, som i 1).