

Fermats nedstegsmetod

- $A^2+B^2 = Mp$
- Bilda $u \equiv_M A$ och $v \equiv_M B$ $-M/2 \leq u, v \leq M/2$
- Då är $u^2+v^2=rM$ för $1 \leq r < M$ eftersom
 - $u^2+v^2 \equiv_M A^2+B^2 \equiv_M 0$ dvs $u^2+v^2=rM$ för något r
 - $r=(u^2+v^2)/M \leq ((M/2)^2+(M/2)^2)/M = M/2 < M$
 - om $r=0$ vore $u=v=0$, dvs $A \equiv_M B \equiv_M 0$ dvs $A^2+B^2 \equiv_M^2 0$ dvs $M|p$, men eftersom $M < p$ måste då $M=1$ och vi vore redan klara.
- Bilda $A_1=(uA+vB)/M$ och $B_1=(vA-uB)/M$.
 - Heltal ty $uA+vB \equiv_M A^2+B^2=Mp \equiv_M 0$ och $vA-uB \equiv_M BA-AB \equiv_M 0$
- $A_1^2+B_1^2=rp$, där $r < M$
 - $A_1^2+B_1^2=((uA+vB)/M)^2 + ((vA-uB)/M)^2 = (u^2+v^2)(A^2+B^2)/M^2 = (rM)(Mp)/M^2 = rp$
- Upprepa tills $r=1$.