

*Proposition.* Given  $n \in \mathbb{N} \cap [2, \infty)$ .  $\forall$  prime  $p \in [2, \sqrt{n}]$ ,  $p \nmid n$ . Show that  $n$  is prime.

*Proof :*

Suppose  $n$  is composite,  $\exists$  prime  $a$  s.t.  $a|n \Rightarrow a \notin [2, \sqrt{n}]$  by hypothesis; otherwise, prime  $a \in [2, \sqrt{n}]$ ,  $a \nmid n$ , C!  
 $\therefore n - 1 \geq a > \sqrt{n}$ ,  $2 \leq b := \frac{n}{a} < \sqrt{n}$ , where  $a|n \Rightarrow b \in \mathbb{N}$ .

That is,  $b \in [2, \sqrt{n}] \wedge b|n$ , accordingly  $b$  is composite by hypothesis again.

Hence,  $\exists$  prime  $q \in \mathbb{N}$  s.t.  $q|b$ , then  $2 \leq q < b$ ,  $\therefore q \in [2, \sqrt{n}]$ , thus  $q \nmid n$  by hypothesis.

Nonetheless,  $q|b \wedge b|n \Rightarrow q|n$ , C!

*Proposition.*  $\forall m, n \in \mathbb{Z}$ ,  $\gcd(m, n) = 1 \Rightarrow \gcd(m^i n^j, m^k \pm n^l) = 1$  for all  $i, j, k, l \in \mathbb{N}$ .

*Proof :*

(i)

If  $d := \gcd(m^i n^j, m^k \pm n^l) \neq 1$ .  $\exists$  prime  $p \in \mathbb{N}$  s.t.  $p|d$ ,  $\therefore p|m^i n^j$ ,

$p|m \vee p|n$  by Arithmetic Fundamental Thm.; w.l.o.g. let  $p|m$ .

(ii)

$\therefore p|d$ ,  $\therefore p|m^k \pm n^l$ , thus  $p|n$  by (i) and Arithmetic Fundamental Thm.,  $\therefore p|\gcd(m, n) = 1$ , C!