Démonstration du lemme d'Euclide

Enoncé du théorème

$$\forall (b,c) \in \mathbb{Z}^2 : p \mid bc \Rightarrow p \mid b \ \vee p \mid c$$

Démonstration (par l'absurde)

On suppose l'existence d'un nombre entier p et d'entiers naturels a et b non divisibles par p tels que p divise ab.

La plus petite valeur de b possible est entre 1 et p exclus, on enlève 1 car p ne divise pas b et sinon on pourrait remplacer b par son reste modulo p ce qui reviendrait au même.

Soit r =/= 0 le reste de la DE de p par b. (non nul car p est premier et b est différent de 1)

On peut donc écrire p sous la forme : p = mb+r

On obtient donc après manipulation : ar = ap-mab. Vu que (par hypothèse) ab est un multiple de p alors ar aussi.

Sauf que 0 < r < b < p. b est bien plus petit que p mais positif donc ar ne peut pas être un multiple de p. La contradiction est là.

L'hypothèse a et b non divisibles par p est fausse et la propriété est donc vérifiée