Il y a une infinité de nombres premiers

Énoncé 1 (à montrer) : Il y a une infinité de nombres premiers.

Énoncé 2 (équivalent à 1 mais ne parlant pas d'infini) : Aucun ensemble fini de nombres premiers contient tous les nombres premiers.

Clairement les énoncés 1 et 2 disent la même chose. L'énoncé 2 est plus intéressant car il ne parle pas d'infini. Mais pour montrer qu'aucun ensemble n'a une certaine propriété il faut normalement faire une preuve indirecte. On suppose qu'il y en a un et on montre que c'est absurde. Essayons une formulation plus directe menant à une preuve directe :

Énoncé 3 (équivalent aux énoncés 1 et 2) : Soit P un ensemble fini de nombres premiers. Alors, on peut trouver un nombre premier qui ne soit pas dans P

Preuve de l'énoncé 3 : Soit $P = \{p_1, p_2, \ldots, p_n\}$ un ensemble fini de nombres premiers (pour chaque i, i = 1, 2, …, n, p_i est un nombre premier). On veut construire un nombre premier qui ne soit pas dans P.

Soit $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$

Soit N est premier ou N n'est pas premier.

Si N est premier, clairement N n'appartient pas à P, on a trouvé un nouveau nombre premier N hors de P.

Si N n'est pas premier, alors N se décompose en facteurs premiers. Si q est un de ses facteurs, alors q est premier et q divise N alors clairement q ne divise pas N – 1. Mais pour chaque p_i, i = 1, 2, …, n, p_i divise $N - 1 = p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Donc q n'est pas un des p_i, q n'appartient pas à P. On a trouvé un nouveau nombre premier hors de P.

La preuve est complète. Étant donné un ensemble fini quelconque de nombres premiers P, on a montré comment construire un nombre premier n'appartenant pas à P.