Contrôle express (gpe 8)

Voici une démonstration d'un célèbre théorème d'Euclide (300 a.J.-C.):

Il existe un nombre premier plus grand que tout nombre entier donné.

Démonstration. Soit n un entier au moins égal à 2, et soit $\mathbb{P}_n$ l'ensemble des nombres premiers inférieurs à n. Nous devons trouver un nombre premier qui n'appartient pas à $\mathbb{P}_n$. On sait que tout entier au moins égal à 2 admet un diviseur premier; il nous suffit alors de construire un entier $A > 2$ qui n'est divisible par aucun des éléments de $\mathbb{P}_n$. En effet, un tel entier A admettra un diviseur premier q, qui ne peut appartenir à $\mathbb{P}_n$ puisqu'aucun des éléments de $\mathbb{P}_n$ ne divise A. Il ne reste plus qu'à trouver A : il suffit de poser $A = 1 + \prod_{p \in \mathbb{P}_n} p$. Pour tout p dans $\mathbb{P}_n$, le reste de la division de A par p est 1, donc p ne divise pas A.

1. Identifier les ressources mises en jeu dans l'énoncé en précisant leur type.
2. Formaliser l'énoncé.
3. Identifier les tactiques de la démonstration.

Solution:

1. L'énoncé parle de l'ensemble $\mathbf{N}$: Ens, de la relation $>$: $\mathbf{N} \times \mathbf{N} \to \mathcal{B}$, et de la propriété $premier$: $\mathbf{N} \to \mathcal{B}$.
2. $\forall n \in \mathbf{N}, \exists p \in \mathbf{N}, p > n$ et $premier(p)$.
3. **Soit n un entier au moins égal à 2**:
   Introduire n; Distinguer selon $n \geq 2$;
   on ne traite que le premier cas;

   et soit $\mathbb{P}_n$ l'ensemble des nombres premiers inférieurs à n:
   ce n'est pas une tactique mais une définition;

   Nous devons trouver un nombre premier qui n'appartient pas à $\mathbb{P}_n$:
   Observer $\exists p \in \mathbf{N}, premier(p)$ et $p \notin P_n$;
   ceci génère deux buts dont le second est considéré comme évident;

   On sait que tout entier au moins égal à 2 admet un diviseur premier:
   Rappel de la ressource R_1:
   $\forall x \in \mathbf{N}, x \geq 2 \Longrightarrow \exists q \in \mathbf{N}, premier(q)$ et $q|x$.

   il nous suffit alors de construire un entier $A > 2$ qui n'est divisible par aucun des éléments de $\mathbb{P}_n$:
   Observer $\exists A \in \mathbf{N}, A > 2$ et $\forall x \in P_n, \forall m \in \mathbf{N}, mx \neq A$;
   cette tactique génère deux buts, et on commence par le deuxième;

   En effet, un tel entier A admettra un diviseur premier q:
   Eliminer $\exists$ (cette tactique introduit A); Appliquer $R1$ à $x := A$; Eliminer $\exists$ (cette tactique introduit q);

qui ne peut appartenir à $\mathbb{P}_n$:
Observer $q \notin P_n$;

puisqu'aucun des éléments de $\mathbb{P}_n$ ne divise A:
Appliquer la ressource qui dit: $\forall E \in Ens, \forall P \in \mathcal{P}(E), \forall x \in E, (\forall y \in P, y \neq x) \Longrightarrow x \notin P$
à $E := \mathbf{N}, P := P_n$, et $x := q$; Introduire y; Appliquer la ressource qui dit:
$\forall E \in Ens, \forall u, v \in E, \forall P \in E \to \mathcal{B}, P(u) \neq P(v) \Longrightarrow u \neq v$
à $E := \mathbf{N}, u := q, v := y, P := z \mapsto z|A$;

Il ne reste plus qu'à trouver A :
Rappel du but restant;

il suffit de poser $A = 1 + \prod_{p \in \mathbb{P}_n} p$:
Exhiber; on ne traite pas $A > 2$;

Pour tout p dans $\mathbb{P}_n$:
Introduire p;

le reste de la division de A par p est 1:
Observer $A \mod p = 1$;

donc p ne divise pas A.
Appliquer la contraposée de $\forall u \in \mathbf{N}, \forall v \in \mathbf{N}, v|u \Longrightarrow u \mod v = 0$ à $u := A, v := p$.