LANGUAGE: 0, $s(x)$, $+$, $\cdot$, $\leq$

THEORY: $\boxed{\text{PEANO ARITHMETIC} \quad PA}$

ax's: • Robinson's arithmetic Q (will have Q^+)

• axiom scheme of induction:

$$(A(0) \wedge (\forall x, A(x) \to A(s(x)))) \to \forall x A(x)$$

for all L_{PA}-flas

Q^+ :

$$\left.\begin{array}{l}
s(x) \neq 0 \\
s(x) = s(y) \to x = y \\
x + 0 = x \\
x + s(y) = s(x+y) \\
x \cdot 0 = 0 \\
x \cdot s(y) = (x \cdot y) + x \\
x \leq y \iff \exists z,\ z + x = y
\end{array}\right\} \boxed{Q}$$

↳ extras to simplify things

$x \cdot y = y \cdot x$

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$

$x \neq 0 \to x \not\leq 0$

$x \cdot s(0) = x$

$\vdots$

PA^- := "non-negative part of discretely ordered commutative rings"

LNP (= least nb. principle)

$$\exists x\, B(x) \longrightarrow \exists z \left(B(z) \wedge \forall y \left((y \neq z \wedge y \leq z) \rightarrow \neg B(y) \right) \right)$$

("$\exists$ min x s.t. $B(x)$").

Easy fact : $PA \vdash LNP$

Prf: Assume $\exists x\, B(x)$ but $\underbrace{\neg \exists \text{ min } B}$.

Put : $A(y) :\equiv \forall z, z \leq y \rightarrow \neg B(z)$.

$\Rightarrow A(0)$

$\Rightarrow A(y) \rightarrow A(s(y))$

$\Leftarrow$ IND

$\forall y A(y)$: $\lightning$ with $\exists x\, B(x)$.

FO predicate calculus "enhancements"

- <u>abbreviations</u>: $x < y \rightleftharpoons (x \leq y \wedge x \neq y)$

$$1 := s(0)$$

$$2 := s(1)$$

$$x \mid y \rightleftharpoons \exists z,\ x \cdot z = y$$

$$\mathrm{Prime}(z) \rightleftharpoons z \geq 2 \wedge \forall y,\ y \mid z \rightarrow (y = 1 \vee y = z)$$

- <u>introducing hypotheses</u>: for proofs by contradiction
- <u>introducing constants</u>: names for witnesses

⋮

ΛΕΜΜΑ 1 : $u \mid v \rightarrow u \mid v \cdot w$.

Prf: $u \mid v \overset{}{\underset{\text{df.}}{\Longleftrightarrow}} u \cdot z = v \underset{\text{equal. ax.}}{\Longrightarrow} (u \cdot z) \cdot w = v \cdot w$

$$\Downarrow \text{ asso.}$$

$$u \cdot (z \cdot w) = v \cdot w$$

$$\Updownarrow \text{ df}$$

$$u \mid v \cdot w$$

$\square$

ΛΕΜΜΑ 2 : $(u \mid v \, , \, v \mid w) \rightarrow u \mid w$.

Prf:

$u \mid v \Leftrightarrow u \cdot z = v \underset{\text{eq. ax.}}{\longrightarrow} (u \cdot z) \cdot z' = v \cdot z' \underset{\text{assoc.}}{\longrightarrow} u \cdot (z \cdot z') = v \cdot z'$

$v \mid w \Leftrightarrow v \cdot z' = w \longrightarrow$ $\Big\downarrow$ eq. ax.

$$u \cdot (z \cdot z') = w$$

$$\|$$

$$u \mid w$$

$\square$

LEMMA 3: $2 \le x \longrightarrow \exists z\, (z \mid x \wedge \mathrm{Prime}(z))$.

Prf.:

$$B(z) :\equiv (2 \le z \wedge z \mid x).$$

1. $\left.\begin{array}{l} 2 \le x \\ x \cdot 1 = x \end{array}\right\} \to B(x)$

2. LNP applied to B:

$$\exists \min z : \quad z \ge 2 \wedge z \mid x.$$

3. If $\cancel{u \le z}$ $u \mid z \xrightarrow{L2 \checkmark} u \mid x \xrightarrow[\text{choice of } z]{} (u < z \to u = 1)$

$$\Downarrow$$

$$\mathrm{Prime}(z).$$

$\square$.

LEMMA 4 : $\forall x\, \underbrace{\exists y\, \forall z\, ((z \leq x,\ \mathrm{Prime}(z)) \to z \mid y)}_{A(x) :=}$.

Prf.:

1) $x = 0, 1$: OK

$x = 2 \Rightarrow y := 2$ witnesses $A(x)$.

2) $A(x) \to A(x+1)$

$A(x)$ ⟶ witness y :

- $x+1$ not prime: $y' := y$
- $x+1$ prime: $y' := y(x+1)$ ← witnesses $A(x+1)$ by L 1.

$\square$.

LEMMA 5 : $(x \mid y \wedge x \mid y+z) \longrightarrow x \mid z$

LEMMA 6 : $x \mid 1 \longrightarrow x = 1$.

LEMMA 7 : $(2 \leq x \wedge x \mid y) \longrightarrow \neg\, x \mid (y+1)$.

Pf. :

$$\left.\begin{array}{l} x \cdot u = y \\ x \cdot v = y+1 \end{array}\right\} \xrightarrow[L5]{} x \mid 1 \xrightarrow[L6]{} x = 1 \;\lightning\; \text{with } x \geq 2.$$

$\square$.

$\Phi := \forall x \exists z, x \leq z \wedge \mathrm{Prime}(z)$ ($\leftrightarrows \exists^\infty$ primes).

Thm: $PA \vdash \Phi$.

Prf: Take x. By L4 $\exists y : \forall z \leq x, \mathrm{Prime}(z) \to z \mid y)$

By L3: $\exists z, \underbrace{\mathrm{Prime}(z) \wedge z \mid y+1}_{\to \text{witness } z}$ $\Big\} \xrightarrow[L7]{} z \nmid y \xrightarrow[\text{choice of } y]{} z \nleq x$.

$\square$.