Copyright Notice

The following manuscript

EWD 582: A proof of a theorem communicated to us by S.Ghosh (with C.S.Scholten)

is held in copyright by Springer-Verlag New York.

The manuscript was published as pages 233–234 of

Edsger W. Dijkstra, Selected Writings on Computing: A Personal Perspective,

Reproduced with permission from Springer-Verlag New York.
Any further reproduction is strictly prohibited.
A proof of a theorem communicated to us by S.Ghosh.

by Edsger W.Dijkstra and C.S.Scholten

In a letter of 19 August 1976, S.Ghosh (currently c/o Lehrstuhl Informatik I, Universität Dortmund, Western Germany) communicated without proof the following theorem in natural numbers — here chosen to mean "nonnegative integers"—:

Given a set of $k$ linear equations of the form

$$L_i = b_i \quad (0 \leq i < k) \quad (1)$$

in which the $L_i$ are homogeneous linear expressions in the unknowns with natural coefficients and the $b_i$ are natural numbers, there exists a single equation

$$M = c \quad (2)$$

in which $M$ is a homogeneous linear expression in the unknowns with natural coefficients and $c$ is a natural number, such that (2) has the same natural solutions as (1).

Because the natural solutions of (1) are the common natural solutions of (3) and (4), as given by

$$L_0 = b_0 \quad L_1 = b_1 \quad (3)$$

and

$$L_i = b_i \quad \text{for} \quad 2 \leq i < k \quad (4)$$

it suffices to prove that (3) can be replaced by a single equation with the same natural solutions as (3).

Consider for natural $p_0$ and $p_1$, to be chosen later, the equation

$$p_0 \cdot L_0 + p_1 \cdot L_1 = p_0 \cdot b_0 + p_1 \cdot b_1 \quad (5)$$

All solutions of (3) are solutions of (5). We shall show that $p_0$ and $p_1$ can be chosen in such a way, that, conversely, all natural solutions of (5) are solutions of (3). We shall do so by choosing $p_0$ and $p_1$ in such a way that (5), considered as an equation in $L_0$ and $L_1$, has (3) as its only natural solution; because all natural choices for the original unknowns will
give rise to natural $L_0$ and $L_1$, this is sufficient.

Considered as an equation in $L_0$ and $L_1$, the general parametric solution of (5) is given by

$$L_0 = b_0 + t \cdot p_1$$
$$L_1 = b_1 - t \cdot p_0$$

(where, to start with, $t$ need not be a natural number). We shall choose a natural $p_0$ and $p_1$ in such a way that from natural $L_0$ and $L_1$, viz.

$$b_0 + t \cdot p_1 \geq 0$$
$$b_1 - t \cdot p_0 \geq 0$$

left-hand sides of (6) and (7) integer

we can conclude $t = 0$.

Choosing $p_1 > b_0$, we derive from (6)

$$t > -1$$

Choosing $p_0 > b_1$, we derive from (7)

$$t < 1$$

Choosing $p_0$ and $p_1$ furthermore such that $\gcd(p_0, p_1) = 1$, we derive from (8) that $t$ must be integer; in view of (9) and (10) we conclude that $t = 0$ holds. Summarizing: (5) can replace (3) provided

$$p_0 > b_1, \quad p_1 > b_0, \quad \gcd(p_0, p_1) = 1$$

Example. Let the given set be $x = 1, y = 1, z = 1$. The first two equations can be combined by choosing $p_0 = 2$ and $p_1 = 3$, yielding:

$$2x + 3y = 5, \quad z = 1$$

These two can be combined by choosing $p_0 = 2$ and $p_1 = 7$, yielding

$$4x + 6y + 7z = 17$$

for which $(1,1,1)$ is, indeed, the only natural solution. (End of example.)

3 August 1976
Plataanstraat 5
NL-4565 NUNEN
The Netherlands