Defining the greatest common divisor

In this note, all variables are of type natural number; "d divides n" is denoted by $d \sqsubseteq n$ and defined by

(0) $$d \sqsubseteq n \;\equiv\; \langle \exists q :: d \cdot q = n \rangle \quad ,$$

from which we deduce

(1) $$\langle \forall d :: d \sqsubseteq 0 \rangle \quad .$$

Proof We observe for arbitrary d

$$\begin{array}{ll}
 & d \sqsubseteq 0 \\
\equiv & \quad \{ (0) \text{ with } n := 0 \} \\
 & \langle \exists q :: d \cdot q = 0 \rangle \\
\Leftarrow & \quad \{ \text{instantiation: } q := 0 \} \\
 & d \cdot 0 = 0 \\
\equiv & \quad \{ \text{zero property} \} \\
 & \text{true.}
\end{array}$$

(End of Proof.)

I would like to stress that (0) is "only" a choice, but by far the wisest one. Someone who is not attracted by its consequence that zero has an unbounded number of divisors, might, for instance, consider the alternative definition for $d \sqsubseteq n$:

$$\langle \exists q : q \geq 1 : d \cdot q = n \rangle \quad ,$$

something some people may have had in mind when the natural numbers still started at 1 . But the consequences would be unattractive, for laws like

$$1 \sqsubseteq n$$

$$d \sqsubseteq m \wedge d \sqsubseteq n \Rightarrow d \sqsubseteq (m-n)$$

would no longer hold.

In the rest of this note we shall denote the greatest common divisor of x and y by $x \downarrow y$ (and their least common multiple, if we need it, by $x \uparrow y$). Historically, the "greatest common divisor" is not only the name of that function but also its <u>verbal definition</u>: if you are interested, say, in $12 \downarrow 21$, you observe:

- the divisors of 12 are $\{1,2,3,4,6,12\}$
- the divisors of 21 are $\{1,3,7,21\}$
- their common divisors are $\{1,3\}$
- their greatest common divisor is 3 .

The most attractive <u>formal definition</u> of $x \downarrow y$ is as the (only!) solution for w of the equation

(2) w: $\langle \forall z :: z \sqsubseteq w \equiv z \sqsubseteq x \wedge z \sqsubseteq y \rangle$

Because we have $- A \equiv A \wedge A -$

$$\langle \forall z :: z \sqsubseteq x \equiv z \sqsubseteq x \wedge z \sqsubseteq x \rangle$$

and —not proved here— the solution of (2) is unique, we have derived

(3) $x \downarrow x = x$ for any x .

But now we have to make up our minds about $0 \downarrow 0$! According to the verbal definition, $0 \downarrow 0$ is, on account of (1), the greatest natural number, i.e.
(i) $0 \downarrow 0$ is undefined , or, perhaps,
(ii) $0 \downarrow 0 = +\infty$.
According to the formal definition, which gives rise to (3), we conclude
(iii) $0 \downarrow 0 = 0$.

I propose to choose (iii), i.e. to let the formal definition prevail, thus ensuring the general validity of the laws about $\downarrow$ (such as

$$x \uparrow y = x \uparrow (y - x)$$
$$x \uparrow 0 = x \quad , \text{etc.})$$

<u>Remark</u> $0{\downarrow}0$ is the only case where verbal and formal definition disagree. For $x{\uparrow}y$, the least common multiple of x and y, the most attractive formal definition is as the (only!) solution for w of the equation

$$w: \langle \forall z :: w \sqsubseteq z \equiv x \sqsubseteq z \wedge y \sqsubseteq z \rangle \quad ,$$

from which $x{\uparrow}x = x$ —and $0{\uparrow}0 = 0$ in particular— follows. Note that, when we read $d \sqsubseteq n$ also as "n is a multiple of d", $0{\uparrow}0$ is the <u>only</u> case where verbal and formal definition agree! (End of Remark.)

Austin, 7 February 1997

prof. dr Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA