1. Euclid via Knuth. The very first algorithm we encounter in *The Art of Computer Programming* is Euclid's formula for the greatest common divisor. Euclid's algorithm is actually a family of algorithms, one of which Knuth describes below.

Algorithm E (*Euclid's algorithm*). Given two positive integers m and n, find their *greatest common divisor*, that is, the largest positive integer that evenly divides both m and n.

E1 [Find remainder.] Divide m by n and let r be the remainder. (We will have $0 \leq r < n$)

E2 [Is it zero?] If $r = 0$, the algorithm terminates: n is the answer.

E3 [Reduce.] Set $m \leftarrow n$, $n \leftarrow r$, and go back to step E1.

Knuth's presentation is somewhat unfortunate, as the algorithm above has something of the status of a rabbit pulled from a hat. In his preface to volume one Knuth writes '... I am not trying to teach the reader how to use somebody else's software. I am concerned rather with teaching people how to write better software themselves.' In that spirit, let us see how we might produce *this* algorithm ourselves.

2. A formal specification for our problem is

$|[$ **con** M, N : int $\{M \geq 0 \ \wedge \ N \geq 0\}$;

var x : int;

gcd

$\{x \ = \ M \downarrow N\}$

$]|$

3. One of the nice properties of $\downarrow$ is that it has a number of tail recursive definitions. One of them is

(0) $\quad x \downarrow 0 \ = \ x$

(1) $\quad x \downarrow y \ = \ y \downarrow (x \ \mathbf{mod} \ y)$

4. This invites us to introduce the fresh variable y and choose as invariant

P0: $x \downarrow y \quad = \quad M \downarrow N$

P1: $0 \leq y \leq N$

which we establish by $x, y := M, N$.

We observe that $P0 \ \wedge \ y = 0 \quad \Rightarrow \quad x \ = \ M \downarrow N$ and so the guard of our repetition will be $y \neq 0$.

5. From the recurrence relation for $\downarrow$ we infer

$$y \neq 0 \;\Rightarrow\; (P0 \equiv P0.(x, y \;:=\; y \;,\; x \;\mathbf{mod}\; y))$$

and we have the following solution to *gcd*

|[**var** y :int;
$x, y := M, N$
{invariant: $x \downarrow y \;=\; M \downarrow N \quad \wedge \quad 0 \leq y \leq N$, bound: y}
;**do** $y \neq 0 \rightarrow x, y \;:=\; y \;,\; x$ **mod** y **od**
$\{x \downarrow y \;=\; M \downarrow N \quad \wedge \quad y = 0$, hence, $x \;=\; M \downarrow N\}$
]|

EUCLID