

The exponent of 3 in the prime factorisation of N

Given G defined by

$$G.n = 0 \quad \text{if } n < 3 \vee n \bmod 3 \neq 0$$

$$G.n = 1 + G.(n \operatorname{div} 3) \quad \text{if } n \bmod 3 = 0$$

we are asked to derive, for positive integer N , a program to compute $G.N$.

* * *

As invariant we choose P given by

$$Py: \quad 1 \leq n$$

$$Pr: \quad G.N = r + G.n$$

which we initially establish with $r, n := 0, N$.

The postcondition is

$$R: \quad r = G.N$$

* * *

The repetition can terminate whenever $LHS.R = RHS.Pr$:

$$\begin{aligned} r &= r + G.n \\ &= \{ \text{arithmetic} \} \\ 0 &= G.n \\ \Leftrightarrow & \{ \text{properties of } G \} \\ n &< 3 \vee n \bmod 3 \neq 0 \end{aligned}$$

and therefore $3 \leq n \wedge n \bmod 3 = 0$ is an acceptable guard. Hence we are heading for a program of the form

```
r, n := 0, N .
; do 3 ≤ n ∧ n mod 3 = 0 →
    "Decrease n under invariance of P"
od
```

* * *

We observe

$$\begin{aligned} & \llbracket \textit{Context: } P \wedge 3 \leq n \wedge n \bmod 3 = 0 \\ & \quad r + G.n \\ & = \quad \{ \textit{property of } G \} \\ & \quad r + 1 + G.(n \mathbf{div} 3) \\ & \rrbracket \end{aligned}$$

and the resulting program is

```
 $r, n := 0, N$   
; do  $3 \leq n \wedge n \bmod 3 = 0 \rightarrow$   
    $r, n := r + 1, n \mathbf{div} 3$   
od
```

The proofs of termination and maintenance of Pn under $n := n \mathbf{div} 3$ are standard and we thus omit them.

E. Emmanuel Macaulay
eric@mathmeth.com

23 January 2007