

## 2000 Paper 1 Question 8

### Discrete Mathematics

The following fragment of ML implements Stein's algorithm for evaluating the Greatest Common Divisor,  $(a, b)$ , of two natural numbers,  $a$  and  $b$ :

```
fun stein a b c =
  if a = b then a * c
  else
    if (a mod 2) = 0 then
      if (b mod 2) = 0 then stein (a div 2) (b div 2) (c * 2)
      else stein (a div 2) b c
    else
      if (b mod 2) = 0 then stein a (b div 2) c
      else
        if a > b then stein (a - b) b c
        else stein (b - a) a c;

fun gcd a b = stein a b 1;
```

Prove that, at each iteration within the Stein algorithm, the product  $(a, b) \times c$  remains invariant. [8 marks]

Observing that the procedure starts with  $c = 1$  and concludes by returning  $a \times c$  when  $a = b$ , deduce that the algorithm correctly calculates the Greatest Common Divisor. [2 marks]

Show also that after two iterations the product  $a \times b$  is reduced by at least a factor of 2. [6 marks]

Deduce that Stein's algorithm is at least as efficient as Euclid's algorithm. [4 marks]