p1 q8
PR

Discrete Mathematics – Question 8 2000

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;
```

The following fragment implements the same algorithm in Java:

```
static int stein (int a, int b, int c) {
      while (a != b)
            switch (((a & 1) << 1) + (b & 1)) {
            case 0:
                  a >>= 1; b >>= 1; c <<= 1;
                  break;
            case 1:
                  a >>= 1;
                  break;
            case 2:
                  b >>= 1;
                  break;
            case 3:
                  if (a > b) a -= b;
                  else {a = b-a; b -= a;};
            };
      return a * c;
}

static int gcd (int a, int b) {
      return stein (a, b, 1);
}
```

Prove that, at each iteration within the Stein algorithm, the product (a,b).c remains invariant. [8 marks]
Observing that the procedure starts with c=1 and concludes by returning a.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.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]

Answer

(2u,2v) = 2.(u,v), (2u,2v+1) = (u, 2v+1), (2u+1,2v) = (2u+1,v), (u,v) = (u-v,u) = (u-v,v).
Invariant starts as (a,b).1 and ends as (a,a).c = a.c which is the final value returned.
$u.v \le 2u.2v/2$, $u.(2v+1) \le 2u.(2v+1)/2$, $(2u+1).v \le (2u+1).2v/2$, $(u-v)(2v+1) = (2u-2v)(2v+1)/2 \le (2u+1)(2v+1)/2$.
If $a < 2^n$ and $b < 2^n$ then $a.b < 2^{2n}$ and the algorithm concludes in at most 4n steps. Hence O(log a).

6 cases: a=b, a & b even, a even & b odd, a odd & b even, a & b odd a>b, a&b odd b<a.