Correctness

Last updated: April 3rd 2017, at 10.57am

1 The Basic Algorithm

This handout contains information on an algorithm, due to Euclid[1], for caclulating the greatest common divisor of two numbers.

1.1 Implementation

```
public int gcd(int p,int q) {
   int n = p, m = q;
   while (n != m) {
      if (n > m) {
         n = n-m;
      } else {
         m = m-n;
      }
   }
   return n;
}
```

2 The Annotated Algorithm

Section 2.1 contains the same algorithm as in section 1.1, but now partially annotated with assertions that could form part of a potential proof aiming to show that the method has the correct semantics — i.e. that the return value is the greatest common divisor of the two parameters.

If you are unsure of how to read the assertions in the code in section 2.1 please see section 2.2. This contains explanations of the assertions which should make their meaning clearer.

The assertions in section 2.1 are presented with no in-text explanation of their derivation. See section 2.3 for justifications for the assertions' derivations.

[1] *Elements*, circa 300BC

2.1 Assertions

In the code below, the values of the parameters `p` and `q` are copied into new variables `n` and `m`, at line 4, in order to leave the values of `p` and `q` unchanged during execution of the algorithm. This makes the construction of the assertions easier. Our aim is to prove assertion $\boxed{32}$. Also, the symbol "γ" is used to represent the greatest common divisor of `p` and `q`, in order to make the assertions more compact. This use is made explicit is "assertion" $\boxed{1}$.

```
1  public int gcd(int p,int q) {
2      $\boxed{1}\{\text{let } \gamma = \mathrm{gcd}(p, q)\}$
3      $\boxed{2}\{\exists a_0, b_0 \mid p = a_0\gamma, q = b_0\gamma\}$
4      int n = p, m = q;
5      $\boxed{3}\{p = n, q = m\}$
6      $\boxed{4}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$
7      $\boxed{5}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$
8      while (n != m) {
9          $\boxed{6}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$
10         $\boxed{7}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$
11         if (n > m) {
12             $\boxed{8}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$
13             $\boxed{9}\{n > m\}$
14             $\boxed{10}\{a_0 > b_0\}$
15             $\boxed{11}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$
16             n = n - m;
17             $\boxed{12}\{\exists a_0', b_0 \mid n = a_0'\gamma, m = b_0\gamma\}$
18             $\boxed{13}\{\exists a_1, a_2, b_1', b_2' \mid p = a_1 n + b_1' m, q = a_2 n + b_2' m\}$
19             $\boxed{14}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$
20             $\boxed{15}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$
21         } else {
22             $\boxed{16}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$
23             $\boxed{17}\{n < m\}$
24             $\boxed{18}\{a_0 < b_0\}$
25             $\boxed{19}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$
26             m = m - n;
27             $\boxed{20}\{\exists a_0, b_0' \mid n = a_0\gamma, m = b_0'\gamma\}$
28             $\boxed{21}\{\exists a_1', a_2', b_1, b_2 \mid p = a_1' n + b_1 m, q = a_2' n + b_2 m\}$
29             $\boxed{22}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$
30             $\boxed{23}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$
31         }
32         $\boxed{24}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$
33         $\boxed{25}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$
34     }
```

$\boxed{26}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$

$\boxed{27}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$

$\boxed{28}\{n = m\}$

$\boxed{29}\{\exists a_1, a_2, b_1, b_2 \mid p = (a_1 + b_1)n, q = (a_2 + b_2)n\}$

$\boxed{30}\{\exists a_1, a_2, b_1, b_2 \mid p = (a_1 + b_1)a_0\gamma, q = (a_2 + b_2)a_0\gamma\}$

$\boxed{31}\{a_0 = 1\}$

$\boxed{32}\{n = \gamma\}$

```
    return n;
}
```

2.2 Elucidations

Assertion $\boxed{1}$: A convention to make the remaining assertions more compact. We are using "γ" to represent the greatest common divisor of p and q.

Assertion $\boxed{2}$: p and q are both multiples of γ — i.e. there are numbers a_0 and b_0 that we can multiply γ by to get, respectively, p and q.

Assertion $\boxed{3}$: Trivial — p and n are equal, and so are q and m.

Assertion $\boxed{4}$: n and m are both multiples of γ.

Assertion $\boxed{5}$: p and q can both be written as sums of multiples of n and m — i.e. there are numbers a_1 and b_1, such that p is equal to a_1 times n plus b_1 times m, and similarly there are numbers a_2 and b_2 such that $q = a_2 m + b_2 m$.

Assertion $\boxed{6}$: n and m are both multiples of γ.

Assertion $\boxed{7}$: p and q can both be written as sums of multiples of n and m.

Assertion $\boxed{8}$: n and m are both multiples of γ.

Assertion $\boxed{9}$: n is greater than m

Assertion $\boxed{10}$: a_0 is greater than b_0

Assertion $\boxed{11}$: p and q can both be written as sums of multiples of n and m.

Assertion $\boxed{12}$: n and m are both multiples of γ.

Assertion $\boxed{13}$: p and q can both be written as sums of multiples of n and m.

Assertion $\boxed{14}$: n and m are both multiples of γ.

Assertion $\boxed{15}$: p and q can both be written as sums of multiples of n and m.

Assertion $\boxed{\mathbf{16}}$: n and m are both multiples of γ.

Assertion $\boxed{\mathbf{17}}$: n is less than m

Assertion $\boxed{\mathbf{18}}$: a_0 is less than b_0

Assertion $\boxed{\mathbf{19}}$: p and q can both be written as sums of multiples of n and m.

Assertion $\boxed{\mathbf{20}}$: n and m are both multiples of γ.

Assertion $\boxed{\mathbf{21}}$: p and q can both be written as sums of multiples of n and m.

Assertion $\boxed{\mathbf{22}}$: n and m are both multiples of γ.

Assertion $\boxed{\mathbf{23}}$: p and q can both be written as sums of multiples of n and m.

Assertion $\boxed{\mathbf{24}}$: n and m are both multiples of γ.

Assertion $\boxed{\mathbf{25}}$: p and q can both be written as sums of multiples of n and m.

Assertion $\boxed{\mathbf{26}}$: n and m are both multiples of γ.

Assertion $\boxed{\mathbf{27}}$: p and q can both be written as sums of multiples of n and m.

Assertion $\boxed{\mathbf{29}}$: p and q can both be written as sums of multiples of n.

Assertion $\boxed{\mathbf{29}}$: p and q can both be written as sums of multiples of $a_0\gamma$.

Assertion $\boxed{\mathbf{31}}$: a_0 is one.

Assertion $\boxed{\mathbf{32}}$: n is the greatest common divisor of p and q.

2.3 Justifications

Assertion $\boxed{\mathbf{1}}$: Just a notational convention — does not require a justification.

Assertion $\boxed{\mathbf{2}}$: From the properties of a (greatest common) divisor. If γ is a divisor of p, then p must be a multiple of γ, and similarly for q.

Assertion $\boxed{\mathbf{3}}$: From the assignment on line 4.

Assertion $\boxed{\mathbf{4}}$: From assertion $\boxed{3}$, and substituting n for p and m for q in assertion $\boxed{2}$.

Assertion $\boxed{\mathbf{5}}$: From assertion $\boxed{3}$ $p = n$. So taking $a_1 = 1$ and $b_1 = 0$ gives $p = a_1 n + b_1 m$. Similarly for $q = a_2 n + b_2 m$.

Assertion $\boxed{\mathbf{6}}$: From assertions $\boxed{4}$ and $\boxed{24}$, the only points from which we can reach this point.

Assertion $\boxed{7}$: From assertions $\boxed{5}$ and $\boxed{25}$, the only points from which we can reach this point.

Assertion $\boxed{8}$: From assertion $\boxed{6}$, the only point from which we can reach this point.

Assertion $\boxed{9}$: From the success of the **if** test on line `11`.

Assertion $\boxed{10}$: From assertion $\boxed{8}$ we have $n = a_0\gamma$ and $m = b_0\gamma$. From assertion $\boxed{9}$ we have $n > m$. It follows that a_0 must be greater then b_0.

Assertion $\boxed{11}$: From assertion $\boxed{7}$, the only point from which we can reach this point.

Assertion $\boxed{12}$: This assertion uses a_0', rather than a_0 to make the reasoning clearer. Where a_0 is used int this justification it represents the value a_0 in assertion $\boxed{8}$. Similarly, in this justification, we will use n' to represent the new value of n (i.e., as if the assignment on line `16` were $\mathtt{n}' = \mathtt{n} - \mathtt{m}$.

Clearly, m is still equal to $b_0\gamma$, as the value of m hasn't changed. If we take $a' = a_0 - b_0$, then we have $n' = a_0'\gamma = (a_0 - b_0)\gamma = a_0\gamma - b_0\gamma = n - m$, which matches the effect of the assignment on line `16`. The step $a_0\gamma - b_0\gamma = n - m$ follows from the equalities in assignment $\boxed{8}$.

Assertion $\boxed{13}$: This assertion uses b_1' and b_2' for the same reason that the previous assertion used a_0', and n' will again be used for the new value of n.

Take $b_1' = b_1 + a_1$. Then the assertion states, making the new value of n explicit as n'. that $p = a_1n' + b_1'm = a_1(n - m) + (b_1 + a_1)m = a_1n - a_1m + b_1m + a_1m = a_1n + b_1m = p$. The last step follows from assertion $\boxed{11}$. A similar reasoning, taking $b'2 = b_2 + a_2$, can be followed to show that $q = a_2n' + b_2'm$ also holds.

Assertions $\boxed{14}$ and $\boxed{15}$: These are simply assertions $\boxed{12}$ and $\boxed{13}$, using a_0, b_1, and b_2, rather than a_0', b_1', and b_2'.

Assertions $\boxed{16}$ to $\boxed{23}$: These all follow a similar reasoning to the corresponding assertions, $\boxed{8}$ to $\boxed{15}$, in the then part of the **if** statement.

Assertion $\boxed{24}$: From assertions $\boxed{14}$ and $\boxed{22}$, the only points from which we can reach this point.

Assertion $\boxed{25}$: From assertions $\boxed{15}$ and $\boxed{23}$, the only points from which we can reach this point.

Assertion $\boxed{26}$: From assertions $\boxed{4}$ and $\boxed{24}$, the only points from which we can reach this point.

Assertion $\boxed{\mathbf{27}}$: From assertions $\boxed{5}$ and $\boxed{25}$, the only points from which we can reach this point.

Assertion $\boxed{\mathbf{28}}$: From the failure of the **while** test on line 8.

Assertion $\boxed{\mathbf{29}}$: From assertion $\boxed{27}$, $p = a_1 n + b_1 m$, and from assertion $\boxed{28}$, $n = m$, so, substituting n for m gives $p = a_1 n + b_1 n = (a_1 + b_1)n$. A similar reasoning can be followed to show that $q = (a_2 + b - 2)n$.

Assertion $\boxed{\mathbf{30}}$: From assertion $\boxed{26}$ $n = a_0\gamma$. Substituting $a_0\gamma$ for n in assertion $\boxed{29}$ gives $p = (a_1 + b_1)a_0\gamma$. Again, a similar reasoning shows that $q = (a_2 + b_2)a_0\gamma$.

Assertion $\boxed{\mathbf{31}}$: From assertion $\boxed{30}$, p and q are both multiples of $a_0\gamma$. It follows that $a_0\gamma$ is a common divisor of p and q. But γ is the greatest common divisor of p and q, so $a_0\gamma$ cannot be greater than γ. Therefore, a_0 must be one.

Assertion $\boxed{\mathbf{32}}$: Follows from assertion $\boxed{26}$, and substituting 1 for a_0 (from assertion $\boxed{31}$) in $n = a_0\gamma$.