Correctness: A longer example

Last updated: March 10$^{\text{th}}$ 2019, at 5.29pm

Contents

1 Introduction

This document provides a longer worked example of a proof of programme correctness by assertion. It shows a proof of the correctness of an algorithm, due to Euclid[1], for caclulating the greatest common divisor of two numbers. The basic algorithm is given in section 2, and an annotated version, with assertions, is in section 3. These assertions are presented without further explanation (in section 3). For explanations of the assertions, see section 4, which presents elucidations of the assertions, and section 5, which presents justifications for them.

2 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;
```

[1] *Elements*, circa 300BC

```
        }
    }
    return n;
}
```

The basic reasoning behind the algorithm is:

- There must be a greatest common divisor for p and q, even if this is just 1.
- This is also the greatest common divisor of the initial values of n and m
- Call this greatest common divisor γ.
- Then there must be values a and b, such that $n = a\gamma$ and $m = b\gamma$.
- At each step the larger of n and m is reduced by the smaller. Since the smaller value is subtracted from the larger, the result will, of course, be positive.
- The result will also be a multiple of γ (because we have subtratced one multiple of γ from another).
- Also, γ will still be the greatest common divisor of the new pair of values.
- The process will terminate when both values are γ.

3 Assertions

This section contains the same algorithm as in section 2, but now annotated with assertions that aim to prove that this is a correct implementation of a greatest common divisor algorithm — i.e. that the result is the greatest common divisor of the two parameters.

If you are unsure of how to read the assertions in the code in section 3 please see section 4. This contains explanations of the assertions which should make their meaning clearer.

The assertions in section 3 are presented with no in-text explanation of their derivation. See section 5 for justifications for the assertions' derivations.

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      [1] {let γ = gcd(p, q)}
```

$\boxed{2}\{\exists a_0, b_0 : p = a_0\gamma, q = b_0\gamma\}$

```
int n = p, m = q;
```

$\boxed{3}\{p = n, q = m\}$

$\boxed{4}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$

$\boxed{5}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$

```
while (n != m) {
```

$\boxed{6}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$

$\boxed{7}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$

```
    if (n > m) {
```

$\boxed{8}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$

$\boxed{9}\{n > m\}$

$\boxed{10}\{a_0 > b_0\}$

$\boxed{11}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$

```
        n = n - m;
```

$\boxed{12}\{\exists a_0', b_0 \mid n = a_0'\gamma, m = b_0\gamma\}$

$\boxed{13}\{\exists a_1, a_2, b_1', b_2' \mid p = a_1 n + b_1' m, q = a_2 n + b_2' m\}$

$\boxed{14}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$

$\boxed{15}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$

```
    } else {
```

$\boxed{16}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$

$\boxed{17}\{n < m\}$

$\boxed{18}\{a_0 < b_0\}$

$\boxed{19}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$

```
        m = m - n;
```

$\boxed{20}\{\exists a_0, b_0' \mid n = a_0\gamma, m = b_0'\gamma\}$

$\boxed{21}\{\exists a_1', a_2', b_1, b_2 \mid p = a_1' n + b_1 m, q = a_2' n + b_2 m\}$

$\boxed{22}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$

$\boxed{23}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$

```
    }
```

$\boxed{24}\{\exists a_0, b_0 \mid n = a_0\gamma, m = b_0\gamma\}$

$\boxed{25}\{\exists a_1, a_2, b_1, b_2 \mid p = a_1 n + b_1 m, q = a_2 n + b_2 m\}$

```
}
```

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

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

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

$\boxed{29}\{\exists a, b \mid p = an, q = bn\}$

$\boxed{30}\{\exists a, b \mid p = a \times a_0\gamma, q = b \times a_0\gamma\}$

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

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

```
return n;
}
```

4 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 $q = a_2m + b_2m$.

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

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

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

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

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

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

Assertion $\boxed{22}$: 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 multiples of n.

Assertion $\boxed{\mathbf{29}}$: n and m are both multiples of n

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

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

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

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

Assertion $\boxed{\mathbf{9}}$: Because the test in the **if** statement on line 11 succeeded.

Assertion $\boxed{\mathbf{10}}$: 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 $\boxed{\mathbf{11}}$: From assertion $\boxed{7}$, the only point from which we can reach this point.

Assertion $\boxed{\mathbf{12}}$: This assertion uses a_0', rather than a_0 to make the reasoning clearer. Where a_0 is used in 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 $\boxed{\mathbf{13}}$: Again we will use n' to represent the new value of n, after the assignment on line `16`.

Using n', the assertion requires us to find a_1, a_2, b_1' and b_2' such that $p = a_1 n' + b_1' m$ and $q = a_2 n' + b_2' m$. If we take a_1 and a_2 to be the same values as in assertion $\boxed{11}$ then, for example, $a_1 n' = a_1(n - m) = a_1 n - a_1 m$. I.e. we have "lost" $a_1 m$ from this part of the equation, and we need to add it back in in the m component. I.e. we take b_1' to be $b_1 + a_1$ (using the values from assertion $\boxed{11}$). Similarly, we take b_2' to be $b_2 + a_2$.

So the assertion claims (for p, the reasoning for q is similar):

$$\begin{aligned} p &= a_1 n' + b_1' m \\ &= a_1(n - m) + (b_1 + a_1)m \\ &= a_1 n - a_1 m + b_1 m + a_1 m \\ &= a_1 n + b_1 m \end{aligned}$$

We know the last equality to be true, from assertion $\boxed{11}$, so assertion $\boxed{13}$ is also true.

Assertions $\boxed{\mathbf{14}}$ and $\boxed{\mathbf{15}}$: 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 $\boxed{\mathbf{16}}$ to $\boxed{\mathbf{23}}$: These all follow a similar reasoning to the corresponding assertions, $\boxed{8}$ to $\boxed{15}$, in the then part of the **if** statement.

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

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

Assertion $\boxed{\mathbf{26}}$: 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 $\boxed{\textbf{29}}$**:** From assertions $\boxed{27}$ and $\boxed{28}$. Because of assertion $\boxed{28}$ we can replace m in assertion $\boxed{27}$ by n to give $p = a_1 n + b_1 n$ and $q = a_2 n + b_2 n$. For this assertion take $a = a_1 + b_1$, and $b = a_2 + b_2$.

Assertion $\boxed{\textbf{30}}$**:** From assertion $\boxed{26}$ $n = a_0\gamma$. Substituting $a_0\gamma$ for n in assertion $\boxed{29}$ gives $p = a \times a_0\gamma$. Again, a similar reasoning shows that $q = b \times a_0\gamma$.

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