DM #4 — Correction de l'algorithme du PGCD binaire d'automne

Dans tout cet exercice, bien que ce ne soit pas vraiment nécessaire, on pourra supposer si l'on veut que les calculs arithmétiques ont lieu en précision arbitraire (« dans $\mathbb{N}$ »).

On souhaite prouver la correction totale d'un algorithme de *PGCD binaire*. On commence par analyser un type de boucle apparaissant dans l'algorithme, **où l'on suppose que la valeur initiale de la variable `a` est strictement positive** :

```
while (a % 2 == 0)
{
    a = a / 2;
}
```

où `a` est de type `unsigned`.
On note a et a' les valeurs prises par la variable `a` en début et en fin d'une itération de la boucle ci-dessus.

1. Prouvez l'invariant de boucle $\mathcal{I}_1 : a > 0$.
2. Montrez que a est un variant de cette boucle.

On définit la *valuation 2-adique* d'un entier naturel non nul n, notée $v_2(n)$, comme le nombre d'occurrences du facteur 2 dans la décomposition de n en facteurs premiers. Autrement dit, $v_2(n)$ est l'entier naturel k (éventuellement nul) le plus grand tel que 2^k divise n.
Soit α, α' les valeurs de `a` avant et après l'exécution de la boucle ci-dessus, on veut montrer que $\alpha' = \alpha \div 2^{v_2(\alpha)}$. Autrement dit, α' est égal à α dont on a « supprimé » tous les éventuels facteurs 2.
Pour montrer cela avec un invariant, on introduit une variable « fantôme » `i` (dont on note i et i' les valeurs en début et fin d'itération) dont le but est de compter le nombre d'itérations dans la boucle. Cette boucle modifiée est alors :

```
unsigned i = 0;
while (a % 2 == 0)
{
    a = a / 2;
    i = i + 1;
}
```

3. Prouvez l'invariant $\mathcal{I}_3$ suivant : $a \times 2^i = \alpha$
4. Conclure.

L'algorithme du PGCD binaire que l'on souhaite analyser utilise en réalité la suite de trois boucles suivantes,

```
while ((a % 2 == 0) && (b % 2 == 0))
{
    r = r * 2;
    a = a / 2;
    b = b / 2;
}
while (a % 2 == 0)
{
    a = a / 2;
}
while (b % 2 == 0)
{
    b = b / 2;
}
```

où l'on suppose les variables `a`, `b` et `r` préalablement déclarées, **et `a` et `b` de valeurs strictement positives**.
On note α, β, ρ les valeurs initiales de ces variables avant la première boucle, α', β', ρ' leur valeur à la fin de celle-ci, α'', β'', ρ'' à la fin de la seconde, et α''', β''', ρ''' à la fin de la troisième.
L'objectif va être de montrer que :

— $\alpha''' = \alpha \div 2^{v_2(\alpha)}$
— $\beta''' = \beta \div 2^{v_2(\beta)}$
— $\rho''' = \rho \times 2^{\min(v_2(\alpha), v_2(\beta))}$

On commence par la dernière égalité, en constatant que $\rho''' = \rho'$ et qu'il suffit donc d'analyser la première boucle.

5. Montrez cette égalité, en suivant la même approche qu'aux questions 1 à 4.
6. On note i le nombre d'itérations effectuées par la première boucle. Montrez que $\alpha' \times 2^i = \alpha$ et $\beta' \times 2^i = \beta$.
7. Montrez que la seconde boucle termine.
8. On note j le nombre d'itérations effectuées par la seconde boucle. Montrez que $\alpha'' \times 2^j = \alpha'$.
9. Montrez qu'on a alors $\alpha'' = \alpha \div 2^{v_2(\alpha)}$.
10. Conclure.

On considère maintenant la boucle principale de l'algorithme du PGCD binaire :

```
unsigned r = 1;
while (a > 0 && b > 0)
{
    while ((a % 2 == 0) && (b % 2 == 0))
    {
        r = r * 2;
        a = a / 2;
```

```
8           b = b / 2;
9       }
10      while (a % 2 == 0)
11      {
12          a = a / 2;
13      }
14      while (b % 2 == 0)
15      {
16          b = b / 2;
17      }
18
19      if (a < b)
20      {
21          b = b - a;
22      }
23      else
24      {
25          unsigned t = b;
26          b = a - b;
27          a = t;
28      }
29  }
```

où l'on suppose les variables `a` et `b` préalablement déclarées.
On renouvelle nos notations, et utilise a, a', a'' et b, b', b'' pour dénoter les valeurs des variables `a` et `b` au début d'une itération de la boucle, à la ligne 19, et à la fin de l'itération respectivement, ainsi que r et r' pour dénoter les valeurs de la variable `r` en début et fin d'itération.

11. Montrez que $a + b$ est un variant de la boucle principale.
12. Conclure sur la terminaison de cette boucle.

Soit x, y deux entiers naturels, on utilise ci-dessous la notation $x \wedge y$ pour désigner le PGCD de x et y (défini comme le plus grand entier naturel k divisant x et y).

13. Montrez que $r \times a \wedge b = r' \times a' \wedge b'$.
14. Montrez que $a' \wedge b' = a'' \wedge b''$.

On considère enfin l'algorithme du PGCD binaire au complet :

```
1   unsigned bgcd(unsigned a, unsigned b)
2   {
3       unsigned r = 1;
4       while (a > 0 && b > 0)
5       {
6           while ((a % 2 == 0) && (b % 2) == 0)
7           {
```

```
8               r *= 2;
9               a /= 2;
10              b /= 2;
11          }
12          while (a % 2 == 0)
13          {
14              a /= 2;
15          }
16          while (b % 2 == 0)
17          {
18              b /= 2;
19          }
20
21          if (a < b)
22          {
23              b = b - a;
24          }
25          else
26          {
27              unsigned t = b;
28              b = a - b;
29              a = t;
30          }
31      }
32
33      if (a > 0)
34      {
35          return a * r;
36      }
37      else
38      {
39          return b * r:
40      }
41  }
```

15. Prouvez la correction totale de cet algorithme.