# 1
# *While a*

Loop invariants is the topic of the problem [1] in this note.

[1] Problem 4 on page 9 from A. Engel. *Problem-Solving Strategies.* Problem Books in Mathematics. Springer New York, 2013. ISBN 9781475789546. URL https://books.google.com/books?id=aUofswEACAAJ

**Problem**

We start with the state $(a, b)$ where $a$, $b$ are positive integers. To this initial state we apply the following algorithm:

```
while a > 0:
    if a < b:
        (a,b) = (2a, b - a)
    else:
        (a,b) = (a - b, 2b)
```

For which starting positions does the algorithm stop? In how many steps does it stop, if it stops? What can you tell about periods and tails?

We start with $a > 0$ and $b > 0$. We adopt the following notation: $a_i$, $b_i$ are the values after $i \in \mathbb{N}_{\geq 0}$ times through the loop. Before the first time through the loop $a_0 = a$, $b_0 = b$. Let $n = a + b$.

Let's collect some invariants. We will prove all of them by induction on $i \in \mathbb{N}_{\geq 0}$.

*Invariant* 1.1.

$$\forall i \geq 0 : a_i + b_i = n$$

*Proof.* Base case $a_0 + b_0 = a + b = n$ holds by definition of $n$ and $(a_0, b_0)$. Assume $a_i + b_i = n$. For $a_{i+1} + b_{i+1}$ we have two cases:

Case $a_i < b_i$: Here we have $a_{i+1} = 2a_i$ and $b_{i+1} = b_i - a_i$. So

$$a_{i+1} + b_{i+1} = 2a_i + b_i - a_i = a_i + b_i = n$$

Case $a_i \geq b_i$: In this case we have $a_{i+1} = a_i - b_i$ and $b_{i+1} = 2b_i$. It follows

$$a_{i+1} + b_{i+1} = a_i - b_i + 2b_i = a_i + b_i = n$$

□

*Invariant* 1.2.

$$\forall i \geq 0 : b_i > 0$$

*Proof.* This follows almost immediately from definitions [2]. □

[2] Base case $b_0 = b > 0$ holds by definition of $b$. Assume $b_i > 0$. Again we have two cases. If $a_i < b_i$ then $b_{i+1} = b_i - a_i > 0$. If $a_i \geq b_i$ then $b_{i+1} = 2b_i > 0$.

*Invariant* 1.3.

$$\forall i \geq 0 : a_i \geq 0$$

*Proof.* This also follows from definitions [3]. □

[3] Base case $a_0 = a > 0$ holds by definition of $a$. Assume $a_i \geq 0$. Again we have two cases. If $a_i < b_i$ then $a_{i+1} = 2a_i \geq 0$. If $a_i \geq b_i$ then $a_{i+1} = a_i - b_i \geq 0$.

*Invariant* 1.4.

$$\forall i \geq 0 : a_i \equiv 2^i a \mod n$$

*Proof.* Base case $a_0 = a = 2^0 a$ trivially holds. Assume $a_i \equiv 2^i a \mod n$. For $a_{i+1}$ we have two cases:

Case $a_i < b_i$: Here we have $a_{i+1} = 2a_i$. So

$$\begin{aligned} a_{i+1} &= 2a_i \\ &\equiv 2 \cdot 2^i a \mod n \\ &\equiv 2^{i+1} a \mod n \end{aligned}$$

Case $a_i \geq b_i$: In this case we have $a_{i+1} = a_i - b_i$. It follows

$$\begin{aligned} a_{i+1} &= a_i - b_i \\ &\equiv a_i + n - b_i \mod n \\ &\equiv a_i + a_i + b_i - b_i \mod n \\ &\equiv 2a_i \mod n \\ &\equiv 2 \cdot 2^i a \mod n \\ &\equiv 2^{i+1} a \mod n \end{aligned}$$

□

We will use these 4 invariants ($a_i \geq 0$, $b_i > 0$, $a_i + b_i = n$ and $a_i \equiv 2^i a \mod n$) to determine for which initial values $a$ and $b$ the loop terminates. To do so we consider $\frac{a}{n}$. Because $0 < a < n$ we know that $\frac{a}{n} \in (0, 1)$. We look at the expansion of $\frac{a}{n}$ in base 2.

**Theorem 1.1.** *If the expansion of $\frac{a}{n}$ is finite with $k$ digits $d_i \in \{0,1\}$*

$$\frac{a}{n} = \sum_{i=1}^{k} d_i 2^{-i}$$

*then $a_k = 0$ and the loop terminates after $k$ steps.*

*Proof.* From

$$\frac{a}{n} = \sum_{i=1}^{k} d_i 2^{-i}$$

we get by multiplying both sides with $2^k n$:

$$2^k a = \sum_{i=1}^{k} n d_i 2^{k-i} \equiv 0 \mod n$$

Together with invariant 1.4 we get

$$a_k \equiv 2^k a \equiv 0 \mod n$$

and because $a_k \geq 0$, $b_k > 0$, $a_k + b_k = n$ we know that $0 \leq a_k < n$, so it must be that $a_k = 0$ and the loop terminates after at most $k$ steps. To show that the loop terminates after exactly $k$ steps, we need to show that $a_j > 0$ for $0 \leq j < k$. We will do this by finding a contradiction. Assume there exists a $j < k$ such that $a_j = 0$. Then it also holds that $2^j a \equiv 0 \mod n$.

From

$$\frac{a}{n} = \sum_{i=1}^{k} d_i 2^{-i}$$

we get by multiplying both sides with $2^j n$:

$$2^j a = \sum_{i=1}^{k} n d_i 2^{j-i} = \sum_{i=1}^{j} n d_i 2^{j-i} + \sum_{i=j+1}^{k} n d_i 2^{j-i} \equiv 0 \mod n$$

$2^j a \equiv 0 \mod n$, so $2^j a = nq$ for some $q \in \mathbb{Z}$. Then

$$q = \sum_{i=1}^{j} d_i 2^{j-i} + \sum_{i=j+1}^{k} d_i 2^{j-i}$$

We have $q \in \mathbb{Z}$, $\sum_{i=1}^{j} d_i 2^{j-i} \in \mathbb{Z}$, but $\sum_{i=j+1}^{k} d_i 2^{j-i} \notin \mathbb{Z}$, because $d_i \in \{0,1\}$. This is a contradiction.

$\square$

We arrived at a neat result: if the binary expansion of $\frac{a}{a+b}$ is finite with $k$ digits, then the loop terminates after $k$ steps.

What can we say if the expansion is not finite but instead has a repeating pattern with a prefix and a period (the only other option [4]) ? For starters, we can use a contradiction similar to the earlier one to prove that the loop does not terminate. Consider the infinite binary expansion:

[4] That is because $\frac{a}{a+b} \in \mathbb{Q}$.

$$\frac{a}{n} = \sum_{i=1}^{\infty} d_i 2^{-i}$$

Assume there is a $k$ for which $a_k = 0$. Then by multiplying the expansion with $2^k n$ we get:

$$2^k a = \sum_{i=1}^{k} n d_i 2^{k-i} + \sum_{i=k+1}^{\infty} n d_i 2^{k-i} \equiv 0 \mod n$$

So for some $q \in \mathbb{Z}$ such that $2^k a = nq$ we have

$$q = \sum_{i=1}^{k} d_i 2^{k-i} + \sum_{i=k+1}^{\infty} d_i 2^{k-i}$$

The left side and the first sum on the right both belong to $\mathbb{Z}$ but the second sum does not, which is a contradiction. This means, that $\forall k : a_k > 0$ and the loop does not terminate.

# *Bibliography*

A. Engel. *Problem-Solving Strategies*. Problem Books in Mathematics. Springer New York, 2013. ISBN 9781475789546. URL https://books.google.com/books?id=aUofswEACAAJ.