レポート問題 1.1
修正された Euclidean Algorithm の反復回数を評価せよ
担当：今井浩 先生

司馬博文 J4-190549
hirofumi-shiba48@g.ecc.u-tokyo.ac.jp

2020 年 5 月 12 日

1 Euclidean Algorithm とは何か

Euclidean Algorithm とは，与えられた 2 つの自然数の組 (M, N) $(M \leqslant N)$ について，$q, r \in \mathbb{N}$ として

$$M = qN + r \quad (0 \leqslant r < N)$$

を満たす (q, r) を計算し，次に $(M, N) = (N, r)$ として同じ計算を $r = 0$ を満たす計算結果 (q, r) を得るまで（停止条件）繰り返し，停止時に直前の演算で得た q の値を $\gcd(M, N)$ の値であるとして返す数論的な algorithm である．

1.1 Euclidean Algorithm の反復回数

Euclidean algorithm では 1 回の計算で

$$\begin{cases} (0 \leqslant) r < N \leqslant \dfrac{M}{2} & (N \leqslant \dfrac{M}{2}) \\ (0 \leqslant) r = M - 1 \cdot N & (\dfrac{M}{2} < N \leqslant M) \end{cases}$$

という条件を満たすため，いずれの場合でも $(0 \leqslant) r \leqslant \dfrac{M}{2}$ を満たす．従って，各反復後の演算結果の推移 $(M, N) \mapsto (N, r) \mapsto (r, r') \mapsto \cdots$ を考えた時，反復回数 2 回で第一要素は必ず半分以下になる．

これより，Euclidean algorithm は，入力値 (M, N) の M の大きさに対して，$\log_2 M$ の値に比例した回数以下の反復回数で停止条件に至ることが出来ることがわかった．

> Euclidean algorithm は入力値 (M, N) に対して，$O(\log_2 M)$ の反復回数で答えを返すことが出来る．

2 修正された Euclid Algorithm の問題設定

初期値を (M_0, M_1) $(M_0 \leqslant M_1)$ と置き，各 $i = 0, 1, 2, \cdots$ について，$q = 1, 2, \cdots$ として

$$M_i = qM_{i+1} + M_{i+2} \quad (-\frac{M_{i+1}}{2} < M_{i+2} \leqslant \frac{M_{i+1}}{2}) \tag{1}$$

を満たす (M_{i+1}, M_{i+2})（と q）を計算し，停止条件 $M_{i+2} = 0$ を満たさない限り，次は (M_{i+1}, M_{i+2}) について再び式 1 を計算する，という algorithm を考える．

2.1 隣項比 a_i の考察

数列 $(M_i)_{i \in \mathbb{N}}$ に対して，停止条件 $M_i = 0$ を満たさない限り

$$a_i := \frac{M_{i+1}}{M_i} \quad (-1 < a_i < 1)$$

と置く．これを用いて式 1 を書き換える．$a_{i+1}=\dfrac{M_{i+2}}{M_{i+1}}=\dfrac{M_{i+2}}{M_i\cdot a_i}$ に注意して，式 1 の両辺を

$$M_i = qM_{i+1}+M_{i+2} \tag{2}$$
$$M_{i+2} = -q(M_i a_i)+M_i \tag{3}$$
$$\frac{M_{i+2}}{M_i a_i}(=a_{i+1}) = -q+\frac{1}{a_i} \tag{4}$$

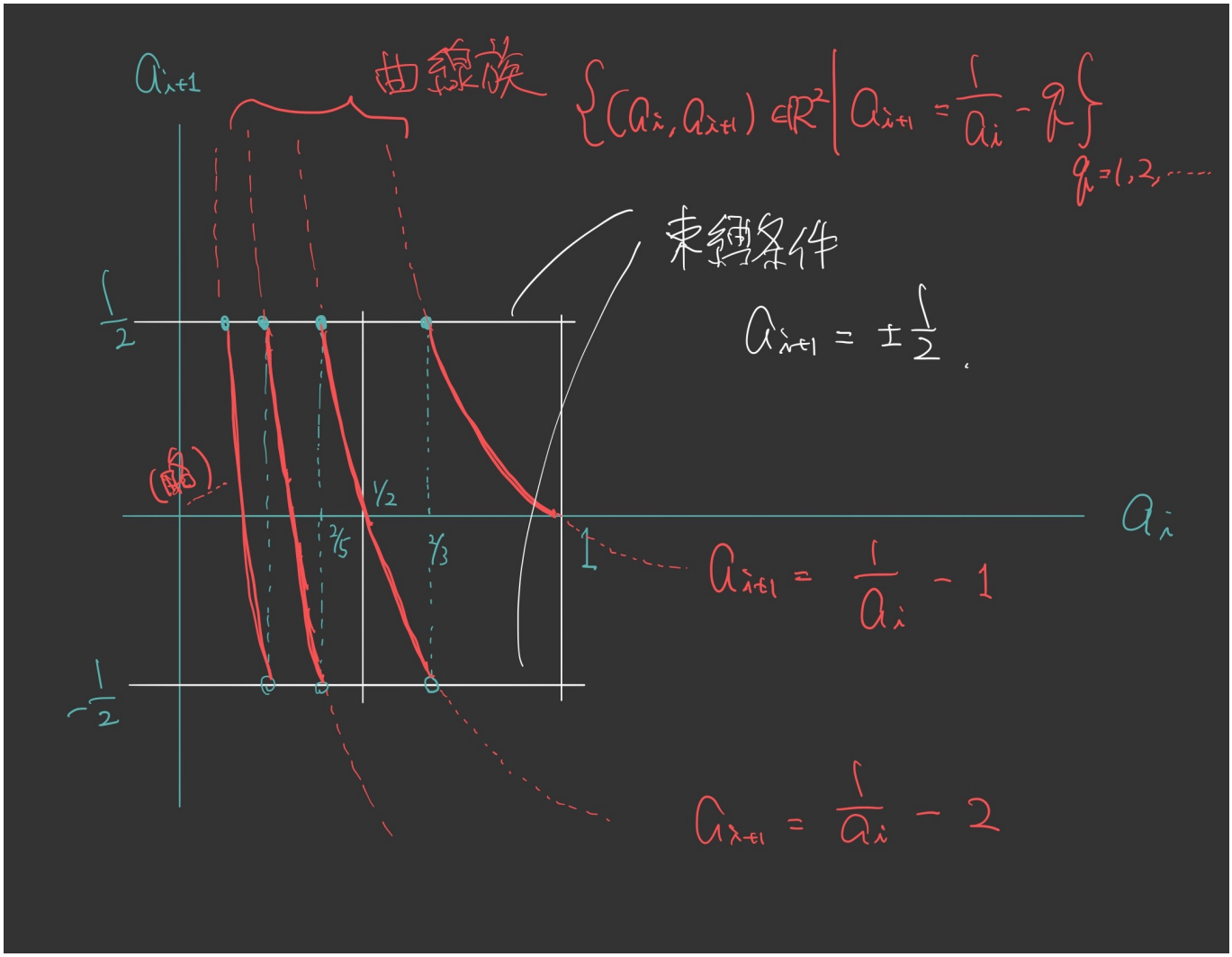
となり，束縛条件は

$$-\frac{1}{2} < a_{i+1}=\frac{M_{i+2}}{M_i a_i} \leqslant \frac{1}{2} \tag{5}$$

と書き換えられる．

式 4,5 を図示すると，次のようになる．

図 1　赤色の太線が式 4 の曲線族，白色の 2 本の水平線が式 5 の直線をそれぞれ図示したものである．



2.2　隣項比 a_i による反復回数の評価

これより分かることは，初期値 a_0（や一般の入力値 a_i）に関わらず，以降の隣項比は $\dfrac{1}{2}$ になるということである．即ち，演算結果の推移 $(M_0,M_1)\mapsto(M_1,M_2)\mapsto(M_2,M_3)\mapsto\cdots$ に於て，

$$|a_{i+1}|=\left|\frac{M_i}{M_{i+1}}\right| \leqslant \frac{1}{2} \quad (i=1,2,\cdots) \tag{6}$$

が成立する（注）．よって，初回の演算を除き，少なくとも確実に値を半減以下にさせることが出来る．

結論

修正された Euclidean algorithm により，値を必ず半分以下にすることが保証される反復回数を，最低 2 回から 1 回に減らすことができた．
一方で，そのオーダーとしては，入力値 (M, N) に対して，$O(\log_2 M)$ の反復回数が必要となり，これは通常の Euclidean algorithm と変わらない．

注． あまり本筋に関係のない議論であるが，$a_{i+1} = \frac{1}{2}$ となる式 6 の等号が成立する場合は，図 1 からも分かる通り，次の試行において $a_{i+2} = 0$ となる，即ち割り切れてしまい，停止条件に引っかかる．即ち，$a_{i+1} = \frac{1}{2}$ は準停止条件とも言えるもので，この場合は式 6 での議論から省いてしまっても問題がないが，省かなくても問題がないので，こうして注釈を述べるだけに留めた．

3 考察

本来，図 1 を作った際には，さらに直線 $y = x$ を補助線として引いて，隣項比の推移を詳細に追う腹づもりであったが，手書きの図では不可能に近いことに気づき，かといって即座に計算機を活用方法するのもあまりに不慣れであったから，このレポートを間に合わせるにあたってはその本来の考察は出来なかった．

本来ならば，例えば前述の注での振る舞いのように，最悪の場合 (worst case) は，見かけ上は図 1 から $a_i = \frac{1}{2}$ の場合であると思われるが，実はその場合は次の反復で必ず停止してしまうように，この修正された Euclidean algorithm の性能は，結論に書いた「1 回の反復で値が半分以下になる」よりはもう少し精度が良く，私の今回のレポートでの評価は（一般の場合を相手にしているとはいえ），まだ評価が粗いであろうことは容易に想像される．

4 参考文献・共同執筆者

参考文献，共同執筆者など，今回は特にありません．