

gcd and Euclid's algorithm for integers

1

Euclid's algorithm relies on the idea

$$\begin{aligned} \gcd(a, 0) &= a && \text{for } a \neq 0 \\ \gcd(a, b) &= \gcd(b, a - q \cdot b) && \text{for any } q \in \mathbb{Z} \end{aligned}$$

input: a, b integers, not both = 0

output: $\gcd(a, b)$

$\alpha := a, \beta := b$

while $\beta \neq 0$ **do**

$(\alpha, \beta) := (\beta, \alpha \text{ rem } \beta)$ **od**

end while

return(α)

2

schematic execution (standard form) of Euclid's algorithm

$$\begin{aligned} a_0 &:= a \\ a_1 &:= b \\ a_0 &= a_1 \cdot q_0 + a_2 && (q_0 \in \mathbb{Z}, 0 < a_2 < a_1) \\ a_1 &= a_2 \cdot q_1 + a_3 && (q_1 \in \mathbb{N}_+, 0 < a_3 < a_2) \\ &\vdots \\ a_{n-2} &= a_{n-1} \cdot q_{n-2} + a_n && (q_{n-2} \in \mathbb{N}_+, 0 < a_n < a_{n-1}) \\ a_{n-1} &= a_n \cdot q_{n-1} && (q_{n-1} \geq 2, a_{n+1} = 0) \end{aligned}$$

$(q_0, q_1, q_2, \dots, q_{n-1})$: *sequence of quotients*

$(a_0, a_1, a_2, \dots, a_n, 0)$: *sequence of remainders*

3

- termination

$$a_0 \geq a_1 > a_2 > \dots > a_n > a_{n+1} = 0 \text{ for some } n \geq 1$$

- correctness

$$\begin{aligned} \gcd(a, b) &= \gcd(a_0, a_1) \\ &= \gcd(a_1, a_2) \\ &= \gcd(a_2, a_3) \\ &= \dots = \gcd(a_n, a_{n+1}) = a_n \end{aligned}$$

4

- The “cost” of Euclid’s algorithm

The following is perhaps the first nontrivial result in history about the complexity of an algorithm

Theorem(Lamé, 1845)

Let $a, b \in \mathbb{N}_+$ and let the Euclidean algorithm for (a, b) perform n division steps. Then

$$a \geq F_{n+1}, b \geq F_n$$

where the F_i are the Fibonacci numbers.

The proof is by an easy induction for the assertion $a_{n-i} \geq F_i$

$$i = 0 : a_n \geq 1 = F_0$$

$$i = 1 : a_{n-1} - a_n q_n \geq 1 = F_1$$

$$i \geq 2 : a_{n-i} = a_{n-i+1} q_{n-i+1} + a_{n-i+2} \geq F_{i-1} + F_{i-2} = F_i$$

This gives as a consequence

Corollary: let $a, b \in \mathbb{N}$ and $a \geq b$, then the number of steps in the Euclidean algorithm for a, b is $\leq 4.8 \cdot \log_{10}(a) + 2$

This follows from the known asymptotic behaviour of the sequence of Fibonacci numbers

$$F_n = \frac{\phi^{n+1} - \hat{\phi}^{n+1}}{\sqrt{5}}$$

where

$$\phi = \frac{1 + \sqrt{5}}{2} (\sim 1.61803\dots) \quad \hat{\phi} = \frac{1 - \sqrt{5}}{2} (\sim -0.61803\dots)$$

$\phi =$ the *golden ratio*

A variant proof

Euclid’s algorithm with input $(a, b) = (a_0, b_0)$ gives us corresponding to the sequence

$$a_i = a_{i+1} \cdot q_i + a_{i+2} \quad (0 \leq i \leq n)$$

of division steps a quotient sequence q_0, q_1, \dots, q_n with

$$q_i \geq 1 \quad (0 \leq i < n) \quad \text{and} \quad q_n \geq 2$$

We have

$$a_{i+2} \cdot (q_i + 1) < a_{i+1} \cdot q_i + a_{i+2} = a_i \quad (0 \leq i < n)$$

and thus

$$q_i + 1 < a_i/a_{i+2} \quad (0 \leq i < n) \quad \text{and} \quad q_n = a_n/a_{n+1} .$$

Starting with $a = a_0 \geq a_1 = b$ we get

$$\begin{aligned} 2^{n+1} &\leq q_n \prod_{i=0}^{n-1} (q_i + 1) < \frac{a_n}{a_{n+1}} \prod_{i=0}^{n-1} \frac{a_i}{a_{i+2}} \leq \frac{a_0 \cdots a_n}{a_2 \cdots a_{n+1} a_{n+1}} \\ &= \frac{a_0 a_1}{a_{n+1} a_{n+1}} \leq \left(\frac{a}{\gcd(a, b)} \right)^2 \end{aligned}$$

- **Theorem :** For $a, b \in \mathbb{N}$ the computation of $\gcd(a, b)$ needs at most

$$\lceil 2 \cdot \log_2 \max(a, b) \rceil + 1 \quad \text{mod operations}$$

(this is linear in problem size!)

A closer look reveals: let $L_\beta(a)$ denote the size (length) of a in base- β -representation, then each division step $a_i = a_{i+1} \cdot q_i + a_{i+2}$ needs $L_\beta(a_{i+1}) \cdot L_\beta(q_i)$ operations in β -arithmetic.

The total amount of work measured in β -operations for Euclid's algorithms executed on input (a, b) is

$$\sum_{i=0}^n L_\beta(a_{i+1}) \cdot L_\beta(q_i)$$

and this is (again assume $a \geq b$) less than

$$\begin{aligned} & L_\beta(a_1) \cdot \left(\sum_{i=0}^{n-1} L_\beta(q_i + 1) + L_\beta(q_n) \right) \\ & \sim L_\beta(b) \cdot L_\beta(q_n) \cdot \prod_{i=0}^{n-1} (q_i + 1) \\ & \leq 2 L_\beta(b) \cdot (L_\beta(a) - L_\beta(\gcd(a, b)) + 1) \end{aligned}$$

9

the extended algorithm

let $a \geq b > 0$

for $i = 0, 1, 2, \dots$ define $\alpha^{(i)} = \langle s_i, t_i, a_i \rangle \in \mathbb{Z}^3$ and $q_i \in \mathbb{N}_+$ by

$$\alpha^{(0)} := \langle 1, 0, a \rangle$$

$$\alpha^{(1)} := \langle 0, 1, b \rangle$$

$i := 1$

while $a_i \neq 0$ **do**

$$q_{i-1} := \lfloor a_{i-1} / a_i \rfloor$$

$$\alpha^{(i+1)} := \alpha^{(i-1)} - q_{i-1} \cdot \alpha^{(i)}$$

$i := i + 1$

end while

10

To verify properties of the extended Euclidean algorithm write it as

$$\alpha = \langle \alpha_1, \alpha_2, \alpha_3 \rangle := \langle 1, 0, a \rangle$$

$$\beta = \langle \beta_1, \beta_2, \beta_3 \rangle := \langle 0, 1, b \rangle$$

while $\beta_3 \neq 0$ **do**

$$q := \alpha_3 \text{ div } \beta_3$$

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} := \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

end while

$$\langle s, t, d \rangle := \langle \alpha_1, \alpha_2, \alpha_3 \rangle$$

11

note that

$$\begin{pmatrix} \alpha^{(i)} \\ \alpha^{(i+1)} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}$$

for $0 \leq i < n$; hence

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} a \\ b \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

is a loop invariant. Writing again: $\alpha^{(i)} = \langle s_i, t_i, a_i \rangle$

$$s_i \cdot a + t_i \cdot b = a_i \quad \text{for } 0 \leq i \leq n + 1$$

Hence the Bézout relation

$$s_n \cdot a + t_n \cdot b = a_n = \gcd(a, b)$$

12

Euclid's algorithm is intimately related to a computational technique that goes back to antiquity (Aristarch and Archimedes apparently have used it) - the technique of *continued fraction expansion* of real numbers.

To see the connection, write the usual divisibility relation as

$$\frac{a}{b} = q + \frac{1}{\left(\frac{b}{r}\right)}$$

13

Euclid's algorithm means iterated long division, hence

$$a_k = a_{k+1} \cdot q_k + a_{k+2} \quad (0 \leq k < n)$$

leads to

$$\begin{aligned} \frac{a}{b} &= q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots}}} \\ &=: [q_0; q_1, q_2, \dots, q_{n-1}] \end{aligned}$$

14

the procedure for generating this *continued fraction* can be carried out (in principle) for any real number; this is the *continued fraction algorithm*

input: $x \in \mathbb{R}$

output: a finite or infinite sequence q_0, q_1, q_2, \dots of integers

where $q_0 \in \mathbb{Z}$ and $q_i \in \mathbb{N}_+$, ($i \geq 1$)

$i := 0$

$x_0 := x$

$q_0 := \lfloor x_0 \rfloor$

while $q_i \neq x_i$ **do**

$x_{i+1} := 1/(x_i - q_i)$

$i := i + 1$

$q_i := \lfloor x_i \rfloor$

end while

STOP

15

This algorithm produces a "simple continued fraction"

- if it terminates

$$x = [q_0; q_1, q_2, q_3, \dots, q_n] = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots}}} \\ q_{n-1} + \frac{1}{q_n}$$

where $q_i \geq 1$ ($1 \leq i \leq n$) and $q_n \geq 2$

16

- if it does not terminate

$$x = [q_0; q_1, q_2, q_3, \dots, q_n] = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_{n-1} + \frac{1}{\dots}}}}}$$

where $q_i \geq 1$ ($i \geq 1$)

17

basic facts

- each $x \in \mathbb{R}$ has a *unique* repr. as a simple continued fraction
- the algorithm terminates if and only if $x \in \mathbb{Q}$ —
precisely: if $x = a/b$ and if $(q_0, q_1, q_2, \dots, q_{n-1})$ is the sequence of quotients in Euclid's algorithm for (a, b) , then the algorithm produces $[q_0; q_1, q_2, \dots, q_{n-1}]$. for example

$$\frac{180}{146} = [1; 4, 3, 2, 2]$$

moreover: erasing the last element of this representation gives the continued fraction representation of the quotient of the Bézout coefficients

$$[1; 4, 3, 2] = \frac{37}{30} \text{ and } (-30) \cdot 180 + 37 \cdot 146 = 2 = \gcd(180, 146)$$

18

- the algorithm eventually runs into a periodic loop if and only if x satisfies a nontrivial quadratic equation $ax^2 + bx + c = 0$, for example,

$$\sqrt{3} = [1; 1, 2, 1, 2, 1, 2, 1, 2, \dots]$$

$$\frac{1 + \sqrt{5}}{2} = [1; 1, 1, 1, 1, 1, 1, \dots]$$

- if x is not rational and not a quadratic irrational, then there are (few) cases where the algorithm produces a nice pattern, like

$$e = 2.71828 \dots = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \dots]$$

and many cases where apparently no regular structure emerges, like

$$\pi = 3.14159 \dots = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 14, 2, 11, \dots]$$

19

To study properties of the continued fraction expansion in detail, write

$$[x_0; x_1, \dots, x_n] = x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{\dots + \frac{1}{x_{n-1} + \frac{1}{x_n}}}}}$$

where the x_i are now variables, as a fraction in the usual way, then

$$[x_0; x_1, x_2, \dots, x_n] = \frac{Q_{n+1}(x_0, \dots, x_n)}{Q_n(x_1, \dots, x_n)}$$

20

where the polynomials $Q_n(x_0, x_1, \dots, x_{n-1})$, called *continuants*, are defined by

$$Q_0() := 1$$

$$Q_1(x_0) := x_0$$

$$Q_2(x_0, x_1) := x_0 x_1 + 1$$

$$Q_{n+1}(x_0, x_1, \dots, x_n) := x_n Q_n(x_0, \dots, x_{n-1}) + Q_{n-1}(x_0, \dots, x_{n-2})$$

Note that

$$Q_n(\underbrace{1, 1, \dots, 1}_n) = F_n$$

(the n -th FIBONACCI number)

21

After executing k division steps in Euclid's algorithm one has

$$\alpha_1 = (-1)^k Q_{k-2}(q_1, \dots, q_{k-2}) \quad \alpha_2 = (-1)^{k-1} Q_{k-1}(q_0, \dots, q_{k-2})$$

$$\beta_1 = (-1)^{k-1} Q_{k-1}(q_1, \dots, q_{k-1}) \quad \beta_2 = (-1)^k Q_k(q_0, \dots, q_{k-1})$$

and in particular the Bézout coefficients are given by

$$s = (-1)^{n+1} Q_{n-1}(q_1, \dots, q_{n-1}) \quad , \quad t = (-1)^n Q_n(q_0, \dots, q_{n-1})$$

wheras

$$\frac{a}{b} = \frac{Q_{n+1}(q_0, q_1, \dots, q_n)}{Q_n(q_1, \dots, q_n)}$$

is the reduced representation of the rational number a/b .

22

The major interest for continued fraction expansions comes from their extremely good approximation properties

Intuitively: if $x \in \mathbb{R}$ and if

$$x = [q_0; q_1, q_2, q_3, \dots]$$

is the (finite or infinite) continued fraction expansion, then one can expect the chopping the expansion by setting

$$x^{(n)} = [q_0; q_1, q_2, q_3, \dots, q_n]$$

gives a (rational) number $x^{(n)}$ that is "close" to x .

23

conversely: if x and y are real numbers that are "close", then one may hope that their continued fraction expansion agrees in many "digits"

attention: this statement is NOT true in general (of course!)

but something similar IS true:

if $x < y < z$ are real numbers such that the "digits" of the continued fraction expansion for x and for z agree in the first n positions, then those of y also agree with these in the first n positions — this observation leads to D. LEHMER's "fast" Euclidean algorithm

24

If $[q_0; q_1, q_2, q_3, \dots]$ is the continued fraction expansion of some $x \in \mathbb{R}$, then the rational numbers

$$x^{(N)} = [q_0; q_1, q_2, q_3, \dots, q_N] = \frac{P_N}{Q_N} \quad (N \geq 0)$$

where

$$P_N = Q_{N+1}(q_0, q_1, \dots, q_N) \quad Q_N = Q_N(q_1, q_2, \dots, q_N)$$

are the *convergents* of x .

One expects

$$\lim_{N \rightarrow \infty} x^{(N)} = x$$

so that the notation

$$x = [q_0; q_1, q_2, q_3, \dots]$$

would be justified

25

examples

- Aristarch uses

$$\frac{43}{37} = [1, 6, 6] = 1.162162162\dots$$

as an approximation for

$$\frac{71\,755\,875}{61\,735\,500} = [1, 6, 6, 4, 1, 2, 1, 2, 1, 6] = 1.162311393\dots$$

- Archimedes uses

$$3 + \frac{10}{71} = [3, 7, 10] = 3.14085070\dots$$

as an approximation for

$$\pi = [3, 7, 15, 1, 292, 1, 1, 2, 1, 3, \dots] = 3.1415926535\dots$$

26

- the convergents of the “golden ratio”

$$\phi = \frac{1+\sqrt{5}}{2} = [1; 1, 1, 1, 1, 1, 1, \dots] = 1.618033989\dots \text{ are}$$

$$\phi^{(0)} = [1] = 1$$

$$\phi^{(1)} = [1; 1] = 2/1 = 2$$

$$\phi^{(2)} = [1; 1, 1] = 3/2 = 1.5$$

$$\phi^{(3)} = [1; 1, 1, 1] = 5/3 = 1.666\dots$$

$$\phi^{(4)} = [1; 1, 1, 1, 1] = 8/5 = 1.6$$

$$\phi^{(5)} = [1; 1, 1, 1, 1, 1] = 13/8 = 1.625$$

$$\phi^{(6)} = [1; 1, 1, 1, 1, 1, 1] = 21/13 = 1.65384615\dots$$

$$\phi^{(7)} = [1; 1, 1, 1, 1, 1, 1, 1] = 34/21 = 1.619047619\dots$$

$$\phi^{(8)} = [1; 1, 1, 1, 1, 1, 1, 1, 1] = 55/34 = 1.617647059\dots$$

27

- the convergents of $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, \dots] = 2.7182818\dots$ are

$$e^{(0)} = [2] = 2$$

$$e^{(1)} = [2; 1] = 3/1 = 3$$

$$e^{(2)} = [2; 1, 2] = 8/3 = 2.666\dots$$

$$e^{(3)} = [2; 1, 2, 1] = 11/4 = 2.75$$

$$e^{(4)} = [2; 1, 2, 1, 1] = 19/7 = 2.7142875\dots$$

$$e^{(5)} = [2; 1, 2, 1, 1, 4] = 87/32 = 2.71875$$

$$e^{(6)} = [2; 1, 2, 1, 1, 4, 1] = 106/39 = 2.7179487\dots$$

$$e^{(7)} = [2; 1, 2, 1, 1, 4, 1, 1] = 193/71 = 2.7183098\dots$$

$$e^{(8)} = [2; 1, 2, 1, 1, 4, 1, 1, 6] = 1264/465 = 2.7182795\dots$$

28

By the definition of the Q -polynomials:

$$\begin{aligned} \begin{pmatrix} P_{n+1} & P_n \\ Q_{n+1} & Q_n \end{pmatrix} &= \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} \begin{pmatrix} q_{n+1} & 1 \\ 1 & 0 \end{pmatrix} = \dots \\ &= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \dots \begin{pmatrix} q_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

by taking the determinant

$$P_{n+1} Q_n - Q_{n+1} P_n = (-1)^n$$

hence

$$\gcd(P_n, Q_n) = 1$$

29

distance between successive convergents

$$x^{(n+1)} - x^{(n)} = \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} = \frac{(-1)^n}{Q_n Q_{n+1}}$$

convergence

$$\begin{aligned} x^{(N)} &= \frac{P_N}{Q_N} = x_{(0)} + \sum_{n=0}^{N-1} x^{(n+1)} - x^{(n)} \\ &= q_0 + \sum_{n=0}^{N-1} \frac{(-1)^n}{Q_n Q_{n+1}} \xrightarrow{N \rightarrow \infty} x \end{aligned}$$

30

- for rational input x

$$\exists N \in \mathbb{N} : x = x^{(N)}$$

- speed of convergence for irrational x

$$\left| x - x^{(N)} \right| = \left| x - \frac{P_N}{Q_N} \right| < \frac{1}{Q_N^2} \quad \text{for all } N \geq 0$$

31

there is a fundamental difference how rational and irrational numbers can be approximated by rational numbers

- $x \in \mathbb{Q} \Rightarrow$ there are only *finitely many* different rational numbers p/q such that

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$$

- $x \notin \mathbb{Q} \Rightarrow$ there are *infinitely many* rational numbers p/q such that

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$$

32

very good approximating rational numbers occur as convergents:

if p/q is a rational number such that

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2}$$

then $p/q = x^{(N)}$ for some $N \in \mathbb{N}$

33

“continuity” of the continued fraction expansion

write

$$x = [q_0; q_1, q_2, q_3, \dots] = [q_0; q_1, q_2, \dots, q_{n-1}, q_n, \lambda]$$

where $1 < \lambda \in \mathbb{R}$ and

$$\lambda = [q_{n+1}, q_{n+2}, \dots]$$

Then

$$x = \frac{\lambda P_n + P_{n-1}}{\lambda Q_n + Q_{n-1}} \in \left(\frac{P_n}{Q_n}, \frac{P_{n-1} + P_n}{Q_{n-1} + Q_n} \right)$$

34

and conversely: for any fixed q_0, q_1, \dots, q_n the mapping

$$\lambda \mapsto \frac{\lambda P_n + P_{n-1}}{\lambda Q_n + Q_{n-1}}$$

is a bijection from $(1, \infty)$ onto $\left(\frac{P_n}{Q_n}, \frac{P_{n-1} + P_n}{Q_{n-1} + Q_n} \right)$, i.e.,

for all $\xi \in \left(\frac{P_n}{Q_n}, \frac{P_{n-1} + P_n}{Q_{n-1} + Q_n} \right)$ one has $\xi^{(n)} = \frac{P_n}{Q_n}$

35

LEHMER’s “fast” Euclidean algorithm

- the basic idea

assume that a, b are very big numbers, \hat{a}, \hat{b} are small numbers such that

$$\frac{a}{b} \approx \frac{\hat{a}}{\hat{b}}$$

then the sequence of quotients produced by $EA(a, b)$ and by $EA(\hat{a}, \hat{b})$ will be the same in the beginning — as long as this holds one may compute $EA(\hat{a}, \hat{b})$ instead of $EA(a, b)$, which is much more economical

- making this idea a bit more concrete

take the following approximations

$$a \mapsto \hat{a} = \lfloor a/\beta^m \rfloor \quad b \mapsto \hat{b} = \lfloor b/\beta^m \rfloor$$

by taking the most significant β -digits of a and b

36

- check that

$$\frac{\hat{a}}{\hat{b}+1} < \frac{a}{b} < \frac{\hat{a}+1}{\hat{b}}$$

and also

$$\frac{\hat{a}}{\hat{b}+1} < \frac{\hat{a}}{\hat{b}} < \frac{\hat{a}+1}{\hat{b}}$$

so that one can state

as long as the quotient sequences of $EA(\hat{a}, \hat{b}+1)$ and $EA(\hat{a}+1, \hat{b})$ coincide, they also coincide with the quotient sequences of both $EA(\hat{a}, \hat{b})$ and $EA(a, b)$

37

it can be checked how long the quotient sequences of $EA(\hat{a}, \hat{b}+1)$ and $EA(\hat{a}+1, \hat{b})$ by computing just the quotient sequence of $EA(\hat{a}, \hat{b})$

let $\alpha = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and $\beta = \langle \beta_1, \beta_2, \beta_3 \rangle$ be the vectors that are iteratively updated in the extended Euclidean algorithm for $EA(a, b)$ — assume that coincidence of the quotient sequences for $EA(a, b+1)$ and $EA(a+1, b)$ has been checked up to a certain stage, then the next quotients will be

$$\lfloor \frac{\alpha_1 + \alpha_3}{\beta_1 + \beta_3} \rfloor \text{ for } EA(a, b+1)$$

$$\lfloor \frac{\alpha_3}{\beta_3} \rfloor \text{ for } EA(a, b)$$

$$\lfloor \frac{\alpha_2 + \alpha_3}{\beta_2 + \beta_3} \rfloor \text{ for } EA(a+1, b)$$

38

- LEHMER's algorithm

algorithm: *lehmergcd*

input: $a, b \in \mathbb{N}$

output: $\text{gcd}(a, b)$

if $a < b$ **then**

return(*lehmergcd*(b, a))

end if

if $b < \beta$ **then**

return(*igcd*(a, b))

end if

lehmergcd(*lehmerstep*(a, b))

39

algorithm *lehmerstep*

$m := L_\beta(a)$

$\hat{a} := a \text{ div } \beta^m; \hat{b} := b \text{ div } \beta^m$

$\alpha := \langle 1, 0, \hat{a} \rangle; \beta := \langle 0, 1, \hat{b} \rangle$

while not $\beta_1 + \beta_2 = 0$ **or** $\beta_1 + \beta_3 = 0$ **do**

$q := \lfloor \frac{\alpha_1 + \alpha_3}{\beta_1 + \beta_3} \rfloor$

if $q \neq \lfloor \frac{\alpha_2 + \alpha_3}{\beta_2 + \beta_3} \rfloor$ **then**

break

end if

$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} := \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

end while

if $\alpha_2 = 0$ **then**

return($b, \text{irem}(a, b)$)

else

return($\alpha_1 \cdot a + \alpha_2 \cdot b, \beta_1 \cdot a + \beta_2 \cdot b$)

end if

40