Euclidean Algorithm and Indeterminate Equation

July 31, 2004

Ryoji Tatsukawa

Reflecting on the function of Euclidean algorithm to serve in algebra particularly number theory, I think it is necessary to teach the algorithm from the early stage of elementary education. The existing circumstance is that it is alienated from the elementary or secondary education, whose teachers seem to think it would be unnecessary if students could factorize the number into prime factors.

1 Euclidean algorithm

Lemma 1

Let (a, b) be the g. c. m. of a and b, when a is divided by b, let the quotient be k, and the remainder be r,

$$(a, b) = (b, c)$$

Proof: Let the common devisor of a and b be k, we find

$$a = ka', \quad b = kb' \quad \text{where } (a', b') = 1$$

Since $a = kb + c$, $c = a - kb = k(a' - kb')$

Therefore (the common devisor of a and b) $\supseteq$ (the common devisor of b and c)

Similarly (the common devisor of b and c) $\supseteq$ (the common devisor of a and b)

(the common devisor of a and b) = (the common devisor of b and c)

$$\therefore (a, b) = (b, c)$$

Theory 1

When a is divided by b, the remainder is c, when b is divided by c, the remainder is d, $\cdots$ the remainders continualy decrease.

$$(a, b) = (b, c) = (c, d) = \cdots\cdots = (l, 0) \quad \text{where } a > b > c > d > \cdots > l$$

l is the g.c.m. of a and b. (*Euclidean algorithm*)

Lemma 2 $(a, b) = (b, a)$ ……①

$(a, b) = (a-b, b)$ ……②

Proof: ① *is trivial.*

Of ②, *let the common devisor of a and b, be k.*

$a = ka'$, $b = kb'$ (a', b' : *integers*)

$\therefore a-b = k(a'-b')$

Therefore the common divisor of $a-b$ *and b is k.*

Conversly, let the common divisor $a-b$ *and b, be d,*

$a-b = db'$, $b = db''$ (b', b'' : *integers*)

$a = b + db' = d(b'' + b')$

Therefore, all of the common divisor of a and b equals to that of $a-b$ *and b.*

$\therefore (a, b) = (a-b, b)$

The Nine Chapters on the Mathematical Arts (*the 1st century A.D.*) *which was compiled the mathematics in the past into a text. The Euclidean algorithm is written in the chapter one, Rectangular Fields, Fangtian,"*方田,*" as follows:*

Problem 6 Given another fraction Tell: reducing it, what is obtained? Answer: If the $\frac{7}{13}$ *denominator and nu-* $\frac{49}{91}$ *merator can be halved, halve them. If not, lay down the denominator and numerator, subtract the smaller number from the greater. Repeat the process to obtain the g.c.m.,dengushu,* 等数. *Reduce them by the dengushu.*

副置分母子之数、以少減多、更相減損、求其等也、以等数約之 [9)]

49	49	7	7	7	7	7	7
91	42	42	35	28	21	14	7

*Remark: It says this algorithm Mutual Subtraction Algorithm,"*更相減損.*"*

In the Elements of Book Vll, Propositions 2, Euclidean algolithm is written as follows:

Given two numbers not prime to one another, to find their greatest common measure.

Proposition 1 Two unequal numbers being set out, and the less being continually subtracted in turn from the greater, if the number which is left never measures the one before it until a unit is left, the original numbers will be prime to one another.

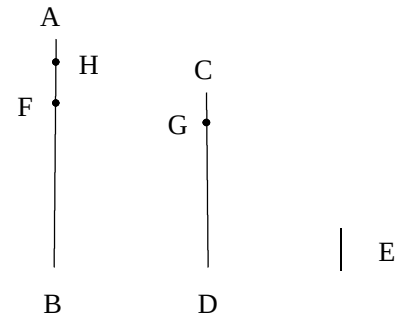
For, the less of two unequal numbers AB, CD being continually subtracted from the greater, let the number which is left never measure the one before it until a unit is left;

I say that AB, CD are prime to one another,

that is, that a unit alone measures AB, CD.

For, if AB, CD are not prime to one another,

some number will measure them.



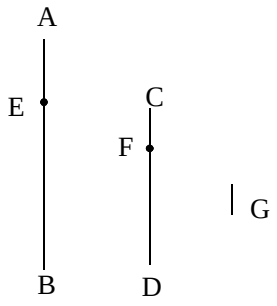
Let a number measure them, and let it be E; let CD, measuring BF, leave FA less than itself, let AF, measuring DG, leave GC less than itself, and let GC, measuring FH, leave a unit HA..

Since, then, E measures CD, and CD measures BF, therefore E also measures BF, therefore E also measures BF. But it also measures the whole AB; therefore it will also measure the remainder FA. But AF measures DG; therefore E also measures DG; therefore E also measures DG. But it also measures the whole DC; therefore it will also measures the remainder GC. But GC measures FH; therefore E also measures FH. But it also measures the whole FA; therefore it will also measure the remainder, the unit AH, through it is a number: which is impossible. Therefore no number will measure the numbers AB, CD; therefore AB, CD are prime to one another. Q. E. D.

Proposition 2 Given two numbers not prime to one another, to find their greatest common measure.

Let AB, CD be the two given numbers not prime to one another. Thus it is required to find the g. c. m. of AB, CD. If now CD measures AB — and it also measures itself — CD is a common measure of AB, CD.

And it is manifest that it is also the greatest; for no greater number than CD will measure CD. But, if CD does not measure AB, then, the less of the numbers AB, CD being continually subtracted from the greater, some number will be left which will measure the one before it.



For a unit will not be left; otherwise AB, CD will be prime to one another, which is contrary to the hypothesis. Therefore some number will be left which will measure the one before it. Now let CD, measuring BE, leave EA less than itself, let EA, measuring DF, leave FC less than itself, and let FC measure EA.

Since then, FC measures AE, and AE measures DF, therefore FC will also measure DF. But it also measures itself; therefore it will also measure the whole CD.

But CD measures BE; therfore FC also measures BE. But it also measures EA; therefore it will also measure the whole AB. But it also measures CD; therefore FC measures AB, CD. Therefore FC is a common measure of AB, CD.

If FC is not the g. c. m. of AB, CD, some number which is greater than FC will measure the numbers AB, CD. Let such a number measure them, and let it be G.

Now, since G measures CD, while CD measures BE, G also measures BE. But it also measures the whole BA; therefore it will also measure the remainder EA. But AE measures DF. But it also measure the whole CD; therefore it will also measure the remainder FC, that is, the greater will measure the less: which is impossible.

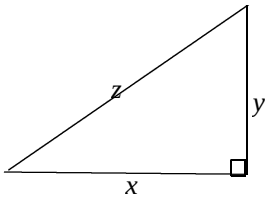
Therefore no number which is greater than FC will measure the numbers AB, CD; therefore FC is the g. c. m. of AB, CD. From this it is manifest that if a number measure two numbers, it will also measure their g. c. m. Q. E. D.

2 Indeterminate equation

1) Diophantine equation $ax + by = c$ *where* $(a, b) = c$

2) Pellian equation $x^2 - Ny^2 = m$

3) Pythagorean numbers $x^2 + y^2 = z^2$



Diophantine equation *where* x, y, z *are positive integers*

When $(a, b) = c$, *it is possible to find such other integers* x, y *that* $ax + by = c$.

Proof: *Let* $a = a_1$, $b = a_2$. *By Euclidian algorithm,*

$$a_1 = k_1a_2 + a_3 \quad (0 < a_3 < a_2) \quad \cdots\cdots\cdots\cdots(1)$$

$$a_2 = k_2a_3 + a_4 \quad (0 < a_4 < a_3) \quad \cdots\cdots\cdots\cdots(2)$$

$$a_3 = k_3a_4 + a_5 \quad (0 < a_5 < a_4) \quad \cdots\cdots\cdots\cdots(3)$$

$$\cdots\cdots$$

$$a_{n-1} = k_{n-1}a_n + a_{n+1} \quad (0 < a_{n+1} < a_n) \quad \cdots\cdots\cdots\cdots(4)$$

$$\therefore \quad a_n = k_n a_{n+1} \quad \cdots\cdots\cdots\cdots(5)$$

By (1),(2) $a_4 = -ak_2 + b(1 + k_1k_2)$ $\cdots\cdots\cdots\cdots(6)$

By (3),(6) $a_5 = a(1 + k_2k_3) - b(k_1 + k_3 + k_1k_2k_3)$

Similarly,

$$a_{n+1} = ax + by \quad \textit{where } x, y \textit{ are integers}$$

$\therefore$ a_{n+1} *is the g. c. m. of* a *and* b *where* $(a, b) = c$.

Aryabhata's solution

The Aryabahatiya is the oldest mathematical text in the ancient India that the solution of Diophantine equation was written. And it is said that the solution was as follows:

(A) $ax + c = by$ *where* $(a, b) = c$

(1) When b *is divided by* a, *let the quotient be* q, *and the remainder be* r,

$$b = aq + r \quad (r < a)$$

$$\therefore \quad ax + c = (qa + r)\, y$$

(2) Let $x = qy + z$

(B) $az + c = ry$

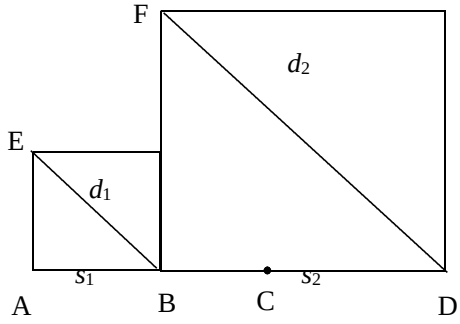
Using Euclidean argolithm, we make the coefficients of unknowns smaller and smaller successively.

(C) $1 \cdot v + c = sw$ *or* $1 \cdot v - c = sw$

Counting back from (C) to (A), we can represent the x *and* y *as the expression for* w. *This is the same as today's solution.*

Pellian equation $x^2 - 2y^2 = 1$

In c. 400 B.C., the ancient India and Greek had gotten $\frac{17}{12}, \frac{577}{408}$ *as the approximate fraction of* $\sqrt{2}$. *Bandhayana, ancient Indian had gotten it and according to Proclus (410 - 485), the Pythagorean school had gotten it by using the following construction, Fig. 1.*



(Fig. 1)

Extending the side AB, of a square with the diagonal BE lay off

$$BC = AB, \quad CD = EB.$$

$$AD^2 + CD^2 = (AB + BD)^2 + (BD - AB)^2$$
$$= 2AB^2 + 2BD^2$$

But $CD^2 = EB^2 = 2AB^2$

$$AD^2 = 2BD^2 = FD^2$$

$\therefore$ $BD = AB + EB$, $FD = AD = 2AB + EB$

Let $AB = s_1$, $BD = s_2$, $EB = d_1$, *and* $FD = d_2$, *we find* $s_2 = s_1 + d_1$, $d_2 = 2s_1 + d_1$

$$\therefore \quad s_{n+1} = s_n + d_n, \quad d_{n+1} = 2s_n + d_n$$

Setting $s_1 = 1$, $d_1 = 1$, *we find*

$$\begin{cases} s_1 = 1 \\ d_1 = 1, \end{cases} \quad \begin{cases} s_2 = 2 \\ d_2 = 3, \end{cases} \quad \begin{cases} s_3 = 5 \\ d_3 = 7, \end{cases} \quad \begin{cases} s_4 = 12 \\ d_4 = 17, \end{cases} \quad \cdots\cdots$$

$$\therefore \quad \frac{d_4}{s_4} = \frac{17}{12}, \frac{d_8}{s_8} = \frac{577}{408}$$

3 Mutual relation between the mutual subtraction algorithm and Euclidean algorithm

In the Nine chapters, they calculated the g.c.m. by the mutual subtraction algorithm, "更相減損." *They started with a pair of numbers* (x, y) *or with a pair of line segments* (u, v), *and continually subtract the smaller one from the larger one.*

In the case $x > y$, S: $(x, y) \to (x-y, y)$

In the case $x < y$, T: $(x, y) \to (x, y-x)$

ST: $(x, y) \overset{S}{\to} (x-y, y) \overset{T}{\to} (x-y, 2y-x)$

TS: $(x, y) \overset{T}{\to} (x, y-x) \overset{S}{\to} (2x-y, y-x)$

On the other hand, the transformation by the Pythagorean school is of the side s and the diagonal d of a square as follows.

BA: $(s, d) \overset{B}{\to} (s, s+d) \overset{A}{\to} (2s+d, s+d)$

The two linear transformations BA, ST *are as follows:*

$$\text{BA: } \begin{cases} d' = 2s + d \\ s' = s + d \end{cases} \quad \cdots\cdots\cdots\cdots(1)$$

$$\text{ST: } \begin{cases} x' = x - y \\ y' = -x + 2y \end{cases} \quad \cdots\cdots\cdots(2)$$

This shows that the transformation (*1*) *is an invers of* (*2*).

Remark: It is said that the Pythgorean school proved the construction (*Fig.1*) *by using the Elements of Book II.10.*

4 Archimedes' (the 3rd century B.C.) solution

It is said that Archimedes approximated $\sqrt{3}$ *with the fractions* $\frac{265}{153}$, $\frac{1351}{780}$. *There is no descriptions how he approximated it but some historians speculate he might use the following inequity.*

$$a \pm \frac{b}{2a \pm 1} < \sqrt{a^2 \pm b} < a \pm \frac{b}{2a} \quad \cdots\cdots\cdots\cdots(*)$$

Approximation of $\sqrt{3}$

(*a*) $\frac{5}{3} < \sqrt{3} < \frac{7}{4}$

We set 2 for approximate value of $\sqrt{3}$ *because* $\sqrt{3}$ *is between 1 and* $\sqrt{4}$. *By using inequality* (*), *let* $\sqrt{3} = \sqrt{2^2-1}$ *so that*

$$2 - \frac{1}{2\times 2-1} < \sqrt{2^2-1} < 2 - \frac{1}{2\times 2}$$

$$\therefore \frac{5}{3} < \sqrt{3} < \frac{7}{4}$$

(*b*) $\frac{19}{11} < \sqrt{3} < \frac{26}{15}$

By using (*a*), *we get* $\frac{5\times 3}{3} < 3\sqrt{3} < \frac{7\times 3}{4}$ *that is,* $5 < \sqrt{27} < \frac{21}{4}$

So, we are able to set 5 for approximate value of $\sqrt{27}$.

By using (*), *let* $\sqrt{27} = \sqrt{5^2+2}$ *so that we get*

$$5 + \frac{2}{2\times 5+1} < \sqrt{5^2+2} < 5 + \frac{2}{2\times 5}$$

$$\frac{57}{11} < 3\sqrt{3} < \frac{26}{5}$$

$$\therefore \frac{19}{11} < \sqrt{3} < \frac{26}{15}$$

(*c*) $\frac{265}{153} < \sqrt{3} < \frac{1351}{780}$

By using (*b*), *we get* $\frac{19\times 15}{11} < 15\sqrt{3} < \frac{26\times 15}{15}$ *that is,* $\frac{285}{11} < \sqrt{675} < 26$

So, we are able to set 26 for approximate value of $\sqrt{675}$

By using (*c*), *let* $\sqrt{675} = \sqrt{26^2-1}$ *so that we get*

$$26 - \frac{1}{2\times 26-1} < \sqrt{26^2-1} < 26 - \frac{1}{2\times 26}$$

$$\frac{1325}{51} < 15\sqrt{3} < \frac{1351}{52}$$

$$\therefore \frac{265}{153} < \sqrt{3} < \frac{1351}{780}$$

Note: 1) Approximation is made to both sides alternately.

2) $\sqrt{3}$ *is correct to 4 places of decimals;* $1.7320261 < \sqrt{3} < 1.732052$

Remark: In our time, we approximate square root by continued fraction as follows.

$$\sqrt{3} = 1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{2} + \cdots$$

5 Brahmagupta's (the 7th century) solution

In the pellian equation $x^2 - Ny^2 = m \quad (m \neq 0)$

$$(x^2 - Ny^2)(z^2 - Nt^2) = (xz \pm Nyt)^2 - N(xt \pm yz)^2 \quad \textit{(Brahmagupta's identity)}$$

$$\because \quad (x^2 - Ny^2)(z^2 - Nt^2) = x^2z^2 + N^2y^2t^2 - N(x^2t^2 + y^2z^2)$$

$$= (xz \pm Nyt)^2 - N(xt \pm yz)^2$$

Remark: $p^2 - Nq^2 = m, \quad r^2 - Ns = n \Rightarrow (pr \pm Nqs)^2 - N(ps \pm qr)^2 = mn$

Let $(x, y) = x^2 - Ny^2, \quad (p, q)(r, s) = (pr + Nqs, ps + qr)$

Let $(p_n, q_n), \quad (p_0, q_0) = (r, s), (p_k, q_k) = (p, q)(p_{k-1}, q_{k-1})$

$$(p_1, q_1) = (1, 1)$$

$$(p_2, q_2) = (2p_1 + 3q_1, p_1 + 2q_1) = (5, 3)$$

$$(p_3, q_3) = (2p_2 + 3q_2, p_2 + 2q_2) = (19, 11)$$

$$(p_4, q_4) = (2p_3 + 3q_3, p_3 + 2q_3) = (71, 41)$$

$$(p_5, q_5) = (2p_4 + 3q_4, p_4 + 2q_4) = (256, 153)$$

……

Since (p_n, q_n) *is a solution of the equation* $x^2 - 3y^2 = -2$,

$$265^2 - 3 \times 153^2 = -2$$

$$(p_1, q_1) = (2, 1)$$

$$(p_2, q_2) = (2p_1 + 3q_1, p_1 + 2q_1) = (7, 4)$$

$$(p_3, q_3) = (2p_2 + 3q_2, p_2 + 2q_2) = (36, 15)$$

$$(p_4, q_4) = (2p_3 + 3q_3, p_3 + 2q_3) = (362, 209)$$

$$(p_5, q_5) = (2p_4 + 3q_4, p_4 + 2q_4) = (1351, 780)$$

……

Since (p_n, q_n) *is a solution of the equation* $x^2 - 3y^2 = 1$,

$$1351^2 - 3 \times 780^2 = 1$$

When $x^2 - Ny^2 = m$,

$$\frac{x}{y} - \sqrt{N} = \frac{1}{y}\frac{m}{x + y\sqrt{N}}$$

Because $\frac{x}{y}$ *is approximately equal to* $\sqrt{N}$ *when x, y are sufficiently large for m*

Since $265^2 - 3\times 153^2 = -2$, *and* $1351^2 - 3\times 780^2 = 1$,

we find the approximate values of $\sqrt{3}$ *is* $\frac{265}{153}$, $\frac{1351}{780}$.

$$\therefore \quad \frac{265}{153} < \sqrt{3} < \frac{1351}{780}$$

6 Solution of the Pythagorean numbers

$x^2 + y^2 = z^2$ *where* x, y, z *are positive integers*

We are able to suppose $(x, y, z) = 1$ *without loss of generality*

When two numbers in the three x, y, z have a common devisor (not 1), remaining one has also a common devisor (not 1). Therefore two in the three x, y, z are namely prime.

We take up the following four cases.

(i) *x*: *odd*, *y*: *odd*, *z*: *even* *(ii)* *x*: *odd*, *y*: *odd*, *z*: *odd*

(iii) *x*: *odd*, *y*: *even*, *z*: *odd* *(iv)* *x*: *even*, *y*: *odd*, *z*: *odd*

We may well take up three cases (i), (ii), and (iii) because the cases (iii),(iv) are the same when we exchane x and y.

Of the case of (i),(ii) $x \equiv 1 \pmod 2$, $y \equiv 1 \pmod 2$

$$x^2 \equiv 1 \pmod 4, \quad y^2 \equiv 1 \pmod 4$$

$$\therefore\ x^2 + y^2 \equiv 2 \pmod 4$$

Because $z^2 \equiv 2 \pmod 4$ *does not hold, (i) or (ii) does not hold.*

Of the case of (iii) $y^2 = (z + x)(z - x)$ ·····(1)

Since y is even, $y^2 \equiv 0 \pmod 4$

Since x: *odd*, *z*: *odd*, $z + x$, $z - x$: *even*

Putting $z + x = 2m$, $z - x = 2n$ (m, n: *positive integers*, $m > n$) ·····(2)

We find $x = m-n$, $z = m + n$ (m, n: *namely prime*) ·····(3)

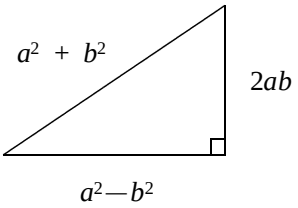
Since $(x, z) = 1$, $(m, n) = 1$

$\because$ When $(m, n) = d \neq 1$, $n = dm$

$x = m(1-d)$, $z = m(1 + d)$

$(x, z) = m \neq 1$

By(1),and(2) $y^2 = 4mn$ ·····(4)



Since m, *and* n *are square nubers,* $m = a^2$, $n = b^2$ ·····(5)

Since $m > n$, $y^2 = 4a^2b^2$

$\therefore$ $y = 2ab$ ·····(6)

By(3),and(5) $x = a^2 - b^2$, $z = a^2 + b^2$ ($a > b$)

$x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$ ($a > b$) (B*rahmagupta*)

Remark: The following cases are well-known.

1) *In the case* $a = 2$, *and* $b = 1$, $x = 3$, $y = 4$, $z = 5$
2) *In the case* $a = 4$, *and* $b = 1$, $x = 15$, $y = 8$, $z = 17$
3) *In the case* $a = 3$, *and* $b = 2$, $x = 5$, $y = 12$, $z = 13$
4) *In the case* $a = 4$, *and* $b = 3$, $x = 7$, $y = 24$, $z = 25$

Reference

[1] *B. L. van der Waelden, Geometry and Algebra in Ancient Civilizations Springer-Verlag 1983*

[2] *Thomas L. Heath, The Thirteen Books of Euclid's Element Vol.2 Dover 1956*

[3] *Thomas L. Heath, A History of Greek Mathematics Vol. 1 Dover 1981*

[4] *Leonard E. Dickson, History of the Theory of Numbers Vol. II Chelsea 1971*

[5] *Taiichi Kitamura, An Introduction to Number Theory, Maki-shoten 1999*

[6] *Sadaharu Takagi, Lecture of the Elementary Number Theory, Iwanami-shoten 2000*

[7] *Wataru Uegaki, Archimedes, Nihon-Hyoron-Sha 1999*

[8] *V. S. Varadarajan: ALGEBRA in ancient and MODERN TIMES, American Mathematical Society, 1998*

〔9〕 Shen Kangshen, John N. Crossley, Anthony W.-C. Lun, The Nine Chapters on the Mathematical Art, Oxford press, 1999