Research Journal of Mathematics and Statistics 6(4): 49-55, 2014
ISSN: 2042-2024, e-ISSN: 2040-7505

Submitted: May 04, 2014 Accepted: June 08, 2014 Published: November 25, 2014

# On Some Algebraic Properties of the Euclidean Algorithm with Applications to Real Life

E.A. Alhassan, K.N. Simon, J.M. Bunyan and A. Gregory
Department of Mathematics, University for Development Studies, P.O. Box 24,
Navrongo Campus, Ghana

**Abstract:** The study analyzed the algebraic properties of the Euclidean algorithm in details. The analysis included a detailed step by step approach in understanding the algorithm, the extended form of the algorithm, computation of the Greatest Common Divisor (GCD) and its algebraic properties and their applications in algebra an d cryptography. We also showed how the Euclidean algorithm could be applied to trading for the maximization of returns. In our approach, we assumed that gcd[$a(x)$; $b(x)$] is the monic polynomial of minimal degree within the set G = {$s(x)a(x)+t(x)b(x)$: $s(x)$, $t(x) \in F[x]$} and thus, examining all equations of the form $p(x)$ = $s(x)a(x)+t(x)b(x)$.

**Keywords:** Algebra, algebraic properties, cryptography, division property, Euclidean algorithm, greatest common divisor, trading

## INTRODUCTION

The Euclidean Algorithm, the oldest algorithm that has survived the test of time is a very useful tool for calculating the greatest common divisor of two integers and for those matter two polynomials. This is attained through the use of the algorithm and its reciprocal subtraction (Glasby, 1999).

Properties of the Euclidean algorithm include the division algorithm, the inverse property and backward substitution.

These properties are applied in finding multiplicative inverses of integers and matrices in modulo arithmetic, least common multiple (events occurring together in different successive time intervals), trading, solving linear congruence in cryptography and modeling population growth (Honsberger, 1976).

The algorithm is also applied in music, agriculture, modeling rabbit birth rate, design of games and number theory (Narkiewicz, 2000).

In the 19$^{th}$ century, application of the algebraic properties of the Euclidean algorithm led to the development of new number systems such as Gaussian and Eisenstein integers (Bashmakova, 1948; Fowler, 1999).

In music, there is a correspondence between ratios and intervals as well as a correspondence between the mathematical relationships of different ratios and the musical relationships of different intervals. For example, combining two musical intervals together, gives you another. A fourth plus a fifth is an octave; a major third plus a minor third is a fifth. More complicated musical intervals like semitones are usually defined by looking at the difference between some pair of more simple intervals, just as the tone was defined as the difference between a fifth and the fourth. Euclid's algorithm provides a way of dealing with equations of musical pitch, potentially helping musicians and instrument makers to tune musical instruments (Gerard, 1973).

The Euclidean algorithm is also used to design the Euclid's game. Playing the Euclid's game involves the use of the cognitive, psychomotor and effective domains thereby arousing and sustaining the interest of the individuals in mathematics.

The Euclidean algorithm has also been improved to form the lame's theorem which was used to develop the Fibonacci numbers (Knuth, 1997).

The stem Brocot tree is also an application of the Euclidean algorithm which enables us to find fine features, carry out binary encoding, continuous fraction on the stem Brocot tree and fractions on a binary tree.

The analysis of the Algebraic properties of the Euclidean algorithm has become necessary due to its usefulness. By analysis of the properties of the algorithm, we mean the determination of good bounds (especially upper) for the algorithm's consumption of resources such as time and space. Such bounds are generally expressed in terms of the size of the inputs, or in the case of integer inputs in terms of the inputs themselves. The analysis of the algorithm has become an important field of study in computer science and algebra. As Knuth (1970) post it in 1970, the advent high-speed computing machines which are capable of carrying out so faithfully has led to intensive studies of

**Corresponding Author:** E.A. Alhassan, Department of Mathematics, University for Development Studies, P.O. Box 24, Navrongo Campus, Ghana

the properties of the algorithm, opening a fertile field for mathematical investigation. In this study, we present a detailed step by step approach in understanding the Euclidean algorithm, the extended form of the algorithm, computation of the Greatest Common Divisor (GCD) and its applications for the maximization of returns in trading. Further, we applied the division property to find the gcd, quotient and the remainder of algebraic expressions in a given modulo.

## MATERIALS AND METHODS

**Description of the Euclidean algorithm:** Let F be a Field and $a(x)$, $b(x)$ be two polynomials such that $a(x)$, $b(x) \in F[x]$, then the Euclidean algorithm constructs gcd[$a(x)$; $b(x)$] explicitly. The basic method is simple. If $q(x)$ is any polynomial, then gcd[$a(x)$, $b(x)$] = gcd[$a(x)$-$q(x)$ $b(x)$; $b(x)$].

In particular, $a(x)$ can be replaced in the calculation by its remainder $r(x)$ upon division by $b(x)$ Assuming that $a(x)$ has degree as big as that of $b(x)$, the remainder $r(x)$ will have smaller degree than $a(x)$; so the gcd of the original pair of polynomials will be equal to the gcd of a new pair with smaller total degree. We can continue by decreasing the degree of the remainder at each stage until the process stops with remainder 0 and at this point the gcd becomes clear.

In our study we assume that gcd($a(x)$; $b(x)$) is the monic polynomial of minimal degree within the set: G = $\{s(x)a(x)+t(x)b(x)$: $s(x)$, $t(x) \in F[x]\}$. Thus, we examine all equations of the form $p(x)$ = $s(x)a(x)+t(x)b(x)$.

Looking for one in which nonzero $p(x)$ has minimal degree. The unique monic scalar multiple of this $p(x)$ is then equal to gcd($a(x)$, $b(x)$). If we have two suitable equations:

$$m(x) = e(x)a(x) + f(x)\ b(x) \quad (1)$$

$$n(x) = g(x)a(x) + h(x)\ b(x) \quad (2)$$

Then we can find a third with left hand side of smaller degree. Assume that the degree of $m(x)$ is at least as big as that of $n(x)$. By the Division Algorithm A.2, there are $q(x)$ and $r(x)$ with $m(x) = q(x)n(x)+r(x)$ and deg($r(x)$) <deg $n(x)$). Subtracting $q(x)$ times Eq. (2) from Eq. (1) we have the desired:

$$r(x) = m(x)\text{-}q(x)n(x) = (e(x)\ \text{-}q(x)\ g(x))\ a(x) + (f(x)\text{-}q(x)h(x))\ b(x) \quad (3)$$

Next, we divide $r(x)$ into $n(x)$ and, using Eq. (2) and (3), further reduces the degree of the left hand side. Continuing as before, we must ultimately arrive at an equation with 0 on the left. The left hand side of the previous equation will then have the desired minimal degree. The benefit of this method of calculation is that, the appropriate polynomials $s(x)$ and $t(x)$ are produced at the same time as the greatest common divisor (gcd).

To succeed with this approach we must have two equations to begin with.
These are provided by:

$$a(x) = 1\times a(x) + 0 \times (bx) \quad (4)$$

$$b(x) = 0\times a(x) + 1 \times b(x) \quad (5)$$

Assume that deg($a(x)$)≥deg ($b(x)$) with $a(x) \neq 0$. At Step i we construct the equation:

$$E_i : r_i(x) = s_i a(x) + t_i(x) b(x)$$

Equation $E_i$ is constructed from $E_{i-1}$ and $E_{i-2}$, the appropriate initialization being provided by (4) and (5):

$$r_{-1}(x) = a(x); s_{-1}(x) = 1; t_{-1} = 0:$$
$$r_0 = b(x); s_0(x) = 0; t_0 = 1:$$

**Step i:** Starting with $r_{i-2}(x)$ and $r_{i-1}(x)$, use the Division algorithm A.2 to define $q_i(x)$ and $r_i(x)$: $R_{i-2}(x) = q_i(x)r_{i-1}(x)+ r_i(x)$ with deg($r_i(x)$) <deg($r_{i-1}(x)$).
Next define $s_i(x)$ and $t_i(x)$ by:

$$s_i(x) = s_{i-2}(x) - q_i(x)s_{i-1}(x);$$
$$T_i(x) = t_{i-2}(x) - q_i(x)t_{i-1}(x)$$

We then have the equation:

$$E_i : r_i(x) = s_i(x)a(x) + t_i(x)b(x)$$

Begin with i = 0. If we have $r_i(x) \neq 0$, then proceed to Step i+1. Eventually there will be an $i$ with $r_i(x) = 0$. At that point halt and declare gcd($a(x)$; $b(x)$) to be the unique monic scalar multiple of the nonzero polynomial $r_{i-1}(x)$.

**Proof:** For each i, $r_i(x) = r_{i-2}(x) - q_i(x)r_{i-1}(x)$; so $E_i$ holds. This also shows that:

$$\gcd(r_{i-1}(x), r_i(x)) = \gcd(r_{i-2}(x), r_{i-1}(x)) = \ldots$$
$$= \gcd(r_{-1}(x), r_0(x)) = \gcd(a(x), b(x))$$

As long as $i \geq 0$ and $r_i(x) = 0$; deg($r_{i-1}(x)$)< deg($r_i(x)$). Thus in at most deg($b(x)$) steps $r_i(x) = 0$ is reached. Then gcd($r_{i-1}(x)$,0) = gcd($a(x)$,$b(x)$) is the unique monic multiple of $r_{i-1}(x)$, completing verification of the algorithm. Alternatively given $a(x)$ and $b(x)$ being two non-zero polynomials such that deg($a(x)$)> deg($b(x)$) we can use finite division to get the greatest common divisor (gcd). The process is as follows:

$$a(x) = b(x)g(x) + r(x); \deg r(x) < \deg b(x)$$

$$b(x) = r(x)g_1(x) + r_1(x); \deg r_1(x) < \deg r(x)$$
$$r(x) = r_1(x)g_2(x) + r_2(x); \deg r_2(x) < \deg r_1(x)$$
$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots$$
$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots$$
$$r_{k-q}(x) = r_{k-1}(x)g_k(x) + r_k(x)\ ;\ \deg r_k(x) < \deg r_{k-1}(x)$$
$$r_{k-1}(x) = r_k(x)g_{k+1}(x)$$

Note that $r_k(x)$ differ from the required greatest common divisor (gcd) by only a constant factor in F.

By reversing the above process we obtain polynomial:

$$r(x), s(x) : d(x) = r(x)a(x) + s(x)b(x)$$

**Example:** In computing the gcd (776, 544), we apply the Euclidean Algorithm as follows:
First,

$$776 = 544 \cdot 1 + 232 \Leftrightarrow a_1 = 776 \text{ and } b_1 = 544$$
$$544 = 232 \cdot 2 + 80 \Leftrightarrow a_2 = 544 \text{ and } b_2 = 232$$
$$232 = 80 \cdot 2 + 72 \Leftrightarrow a_3 = 232 \text{ and } b_3 = 80$$
$$80 = 72 \cdot 1 + 8 \Leftrightarrow a_4 = 80 \text{ and } b_4 = 72$$
$$72 = 8 \cdot 9 + 0 \Leftrightarrow a_5 = 72 \text{ and } b_5 = 8$$

So,

$$\gcd(776, 544) = 8 (\textit{ie. the last non-zero remainder}).$$

## RESULTS AND DISCUSSION

**Finding events that occur together:** Events that occur at successive time interval can be solved using the ordinary Least Common Multiple (LCM). If these events occur at a larger time interval, the LCM computation becomes tedious. The Euclidean algorithm then becomes the best alternative. Thus, given two events occurring at very large time intervals $a$ and $b$ respectively, we will have:

$$LCM = \frac{a \times b}{\gcd(a, b)}$$

This application is very useful when dealing with the production of the same commodities by different manufacturers. The fact is that, as the supply of the commodity increases, the demand reduces and prices go down. Manufacturers when aware of this occurrence will put the necessary measures in place to reduce losses. Again, this will help farmers avoid post-harvest losses.

**Example:** If two factories $a$ and $b$ manufactures a mowing machine every 299 and 221 days respectively, The number of days it will take for them to manufacture at the same time is calculated as follows:
First, for the gcd(299, 221).
We have:

$$299 = 1 \cdot 221 + 78$$
$$221 = 2 \cdot 78 + 65$$
$$78 = 1 \cdot 65 + 13$$
$$65 = 5 \cdot 13 + 0$$
$$\therefore \gcd(299, 221) = 13$$

Using,

$$LCM = \frac{a \times b}{\gcd(a,b)} = \frac{299 \times 221}{13} = \frac{66079}{13} = 5083$$

This means that on the 5083 day, the two factories will manufacture a mowing machine each.

**Finding the remainder:** The finite division algorithm is used in the remainder theorem to find the remainder of algebraic expressions in a given modulo. This application is useful when sharing things. In higher levels, we use it to share a thing in a given number of parts (referred to as modulo).

**Example:** We can find the remainder if $x^5 + 2x^3 + 4x^2 + x - 1$ is divided by $x^3 - 4x^2 + 3x - 5$ in $Z_7(X)$ as follows:

$$\begin{array}{r} x^2 + 4x + 1 \\ x^3 - 4x^2 + 3x - 5 \overline{)\ x^5 + 2x^3 + 4x^2 + x - 1} \\ \underline{-x^5 + 4x^4 - 3x^3 + 5x^2} \\ 4x^4 - x^3 + 2x^2 + x - 1 \\ \underline{-4x^4 + 2x^3 - 5x^2 + 6x} \\ x^3 - 3x^2 - 1 \\ \underline{-x^3 + 4x^2 - 3x + 5} \\ x^2 - 3x + 4 \rightarrow \textit{remainder} \end{array}$$

**NB:** All workings are performed in $Z_7(X)$ appropriately.

**Theorem 1:** Let G be a group, then for all $a \in G$ there exist $a^{-1} \in G$ such that $(a^{-1})^{-1} = a$.

**Proof:** $(a^{-1})^{-1}\, a^{-1} = e(a) = a$ Post multiplying by $a$, we obtain:

$$[(a^{-1})^{-1}(a^{-1})]a$$
$$= e(a)a \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \quad (6)$$

From the L.H.S $\equiv (a^{-1})^{-1}(a^{-1}a) = (a^{-1})^{-1}$
$$e(a) = (a^{-1})^{-1}e(a^{-1}) = (a^{-1})^{-1}e[(a^{-1})^{-1}]$$
$$= (a^{-1})^{-1} \quad (7)$$

Hence from (1) and (2) $(a^{-1})^{-1} = a$

**Finding inverses by the extended Euclidean algorithm (multiplicative inverse):** When we are working in modular arithmetic, we often need to find the inverse of a number relative to an operation. When we are looking for an additive inverse it is relative to an addition operation and when a multiplicative inverse it is relative to a multiplication operation. Here, we mainly used the extended Euclidean algorithm to find the multiplicative inverse of b in $Z_n$ when n and b are given and the inverses exists. To show this, take two integers $0<b<a$ and consider the Euclidean Algorithm equations which yield gcd($a$, $b$) = $r_j$. Rewrite all of these equations except the last one, by solving for the remainders:

$$r_1 = a - bq_1,$$
$$r_2 = b - r_1q_2,$$
$$r_3 = r_1 - r_2q_3,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$r_{j-1} = r_{j-3} - r_{j-2}q_{j-1},$$
$$r_j = r_{j-2} - r_{j-1}q_j$$

Then, in the last of these equations, $r_j = r_{j-2} - r_{j-1}q_j$, replace $r_{j-1}$ with its expression in terms of $r_{j-3}$ and $r_{j-2}$ from the equation immediately above it. Continue this process successively, replacing $r_{j-2}, r_{j-3}, \ldots\ldots$, until you obtain the final equation:

$$r_j = ax + by$$

With x and y integers. In special cases that gcd($a$, $b$) = 1, the integer equation reads:

$$1 = ax + by$$

Therefore we deduce:

$$1 \equiv by \bmod a$$

So that (the residue of) y is the multiplicative inverse of $b$ mod $a$.

Thus, the integer $a \in Z_n$ has a multiplicative inverse $a^{-1}$ if and only if gcd($n$, $a$) ≡ 1(mod $n$).

**Example:** Find the multiplicative inverse *of* $19$ *in* $Z_{45}$.

Solution:

$$\gcd(45,19) = 1$$
$$45 = 2.19 + 7$$
$$19 = 2.7 + 5$$
$$7 = 1.5 + 2$$
$$5 = 2.2 + 1$$

Extended:

$$1 = 1.5 - 2.2$$
$$= 1.5 - 2(7 - 1.5)$$
$$= 1.5 - 2.7 + 2.5$$
$$= 3.5 - 2.7$$
$$= 3(19 - 2.7) - 2.7$$
$$= 3.19 - 6.7 - 2.7$$
$$= 3.19 - 8.7$$
$$= 3.19 - 8(45 - 2.19)$$
$$= 3.19 - 8.45 + 16.19$$
$$= 19.19 - 8.45$$
$$\therefore 19^{-1} = 19$$

**Solving systems of congruencies:** The inverse property of the Euclidean algorithm can be applied in solving certain systems of congruencies in cryptography that involves the arrangement of things in a given number of ways (referred to as modulo) and thus, battle problems.

**Example:** If a group of academic scholars in a conference can be fitted to 3 rows leaving 2 left, in 5 rows leaving 4 left and 7 rows leaving 6 left then the total number of scholars who attended the conference can be found as follows.

We translate it into the following system of congruencies:

$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 6 \pmod 7$$

Next,

$$m = m_1 \times m_2 \times m_3$$
$$= 3 \times 5 \times 7$$
$$= 105$$

Further:

$$M_1 = \frac{m}{m_1} = \frac{105}{3} = 35 \equiv 2(\bmod 3)$$
$$M_2 = \frac{m}{m_2} = \frac{105}{5} = 21 \equiv 1(\bmod 5)$$
$$M_3 = \frac{m}{m_3} = \frac{m}{m_3} = \frac{105}{7} = 15 \equiv 1(\bmod 7)$$

Next, we use Euclidean algorithm to compute:

$$y_i = M_i^{-1} (\bmod\ m_i)$$
Im *plies* ,
$$y_1 = M_1^{-1} (\bmod\ 3)$$
$$= 35^{-1} (\bmod\ 3)$$
$$= 2$$
$$y_2 = M_2^{-1} (\bmod\ 5)$$
$$= 21^{-1} (\bmod\ 5)$$
$$= 1$$
$$y_3 = M_3^{-1} (\bmod\ 7)$$
$$= 15^{-1} (\bmod\ 7)$$
$$= 1$$

Finally,

$$x = \sum_{i=1}^{3} a_i M_i y_i \,(\mathrm{mod}\, m)$$
$$\Rightarrow x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$
$$= 2\times 35\times 2 + 4\times 21\times 1 + 6\times 15\times 1$$
$$= 140 + 84 + 90$$
$$= 314(\mathrm{mod}105)$$
$$= 104$$

Therefore, there were 104 scholars at the conference

**Euclidean algorithm in trading:** The Euclidean algorithm could also be applied to trading so as to maximize returns. In trading, retailers normally bid for reduction in prices of goods since they have to resell the commodities and make profit. They therefore price the goods in groups. Most often, some are added free to the retailers. In case there are more retailers, we can simplify their bid into linear congruence, applying the division and inverse property in determining the best bid so as to maximize profit.

**Example:** A wholesaler sells cartons of biscuits. Three retailers agree to buy the cartons in groups.

Retailer one agrees to buy them at every three for ₵ 55.00 of which two will be left and added free to the retailer. Retailer two agrees to buy them at every seven for ₵ 125.00 of which four will be left and given him free. Retailer three agrees to buy it in tens for ₵ 175.00 for which six will be left and added free.

To estimate how many cartons are to be sold we use linear congruence with the application of Euclidean algorithm:

$$X \equiv a_i \,\mathrm{mod} m_i$$
$$X \equiv 2(\mathrm{mod}\ 3)$$
$$X \equiv 4(\mathrm{mod}7)$$
$$X \equiv 6(\mathrm{mod}10)$$

So,

$$m_1 = 3, m_2 = 7, m_3 = 10, a_1 = 2, a_2 = 4, a_3 = 6$$

We first compute:

$$M = m_1 \times m_2 \times m_3 = 3\times 7\times 10 = 210$$

Next,

$$M_1 = \frac{M}{m_1} = \frac{210}{3} = 70$$
$$M_2 = \frac{M}{m_2} = \frac{210}{7} = 30$$
$$M_3 = \frac{M}{m_3} = \frac{210}{10} = 21$$

Next, compute:

$$y_i = M_i^{-1}(\mathrm{mod}\, m_i)$$
$$y_1 = M_1^{-1}(\mathrm{mod}\, m_1)$$
$$y_1 = 70^{-1}(\mathrm{mod}3)$$

From the Euclidean algorithm, we have:

$$70 = 23\cdot 3 + 1$$
$$3 = 1\cdot 3 + 0$$
$$\gcd(70,3) = 1$$

Further, from the extended Euclidean algorithm:

$$1 = 1\cdot 70 - 23\cdot 3$$
$$70^{-1}(\mathrm{mod}3) = 1$$

Hence, $y_1 = 1$.
Again,

$$y_2 = M_2^{-1}(\mathrm{mod}\, m_2)$$
$$y_2 = 30^{-1}(\mathrm{mod}7)$$

Similarly:

$$30 = 4\cdot 7 + 2$$
$$7 = 3\cdot 2 + 1$$
$$2 = 1\cdot 2 + 0$$
$$\gcd(30,7) = 1$$

Thus,

$$1 = 1\cdot 7 - 3\cdot 2$$
$$= 1\cdot 7 - (1\cdot 30 - 4\cdot 7)$$
$$= 1\cdot 7 - 3\cdot 30 + 12\cdot 7$$
$$= 13\cdot 7 - 3\cdot 30$$
$$= 30^{-1}(\mathrm{mod}7) = -3 + 7 = 4$$

Hence, $y_2 = 4$
Next,

$$y_3 = M_3^{-1}(\mathrm{mod}\, m_3)$$
$$y_3 = 21^{-1}(\mathrm{mod}10)$$

Implies,

$$21 = 2\cdot 10 + 1$$
$$10 = 1\cdot 10 + 0$$
$$\gcd(21,10) = 1$$
$$1 = 1\cdot 21 - 2\cdot 10$$
$$21^{-1}(\mathrm{mod}10) = 1$$
$$y_3 = 1$$

By Chinese remainder theorem, we compute finally; $x = \sum_{i=1}^{r} a_i M_i y_i \ (mod\ M)$:

$$
\begin{aligned}
&= [(a_1 M_1 y_1) + (a_2 M_2 y_2) + (a_3 M_3 y_3)] mod\ M \\
&= \left[(2\times 70\times 1) + (4\times 30\times 4) + (6\times 21\times 1)\right] \bmod 210 \\
&= \left[140 + 480 + 126\right] \bmod 210 \\
&= 746 (\bmod 210) \\
&= 116
\end{aligned}
$$

Hence, there are 116 cartons.

Again, if the wholesaler agrees to sell to retailer one, he can sell six times of such cartons in a month. If he agrees to sell for retailer two, he can sell ten times of such cartons in a month. If he also agrees to sell for retailer three, he can sell sixteen times of such cartons in a month. To find which of these retailers the wholesaler should choose to make the maximum profit in a month and assuming the cost price of a carton of the biscuit is ₵ 15.00 with selling price of ₵ 20.00 per carton, we look for the profit on each retailer.
Thus, the total number of cartons is 116.
For agreement with retailer one:

Total sales = 116/3 = 38 with remainder of 2
The selling price in a month is,
38×6×55 = ₵ 12,540.00
Cost price = 15×116×6 = ₵ 10, 440.00
$\text{Pr}\,\textit{ofit} = 12{,}540.00 - 10{,}440.00 = 2{,}100.00$

Hence, the profit is ₵2,100.00.
For agreement with retailer two:

$$\textit{Total sales} = \frac{116}{7} = 16 \textit{ with remainder of } 4.$$

The selling price in a month is:

10×16×125 = ₵20, 000.00
Cost price = 116×15×10 = ₵ 17, 400.00
$\text{Pr}\,\textit{ofit} = 20000 - 17400 = 2{,}600.00$

Hence, the profit is ₵2, 600.00.
For agreement with retailer three:

$$\text{Total sales } \frac{116}{10} = 11 \text{ with remainder of } 6$$

The selling price in the month is:

11×16×175 = ₵30, 500.00
The cost price = $116\times 16\times 15$ = ₵ 27, 840.00
Profit = 30500 – 27840 = ₵ 2, 960.00

Hence the wholesaler should agree to do business with retailer three so as to maximize profit for that month.

**Backward substitution and the general difference equation formula:** Backward substitution is also another important property of the Euclidean algorithm. This is seen when we try to make the greatest common divisor (gcd) the subject, carry out series of substitutions until the multiplicative inverse is obtained. This important property is useful in generating the general term of a number of mathematics formulae involving series. It can be applied also in statistics when finding the dual of an autoregressive process. Besides, it can be applied in difference equations to find composite formula when modeling population growth.

In modeling population growth, this property is very useful. Let $x_0$ be the initial population of an area, $\alpha$ be the growth rate of the population and $x_n$ be the general term then:

$x_1 = \alpha x_0$
$x_2 = \alpha x_1$
…….
……....
$x_n = \alpha x_{n-1}$

By backward substitution:

**Step 1:** $x_n = \alpha x_{n-1}\ but\ x_{n-1} = \alpha x_{n-2}$
**Step 2:** $x_n = \alpha^2 x_{n-2}\ again\ x_{n-2} = \alpha x_{n-3}$
**Step 3:** $x_n = \alpha^3 x_{n-3}\ also\ x_{n-3} = \alpha x_{n-4}$
**Step 4:** $x_n = \alpha^4 x_{n-4}$
……
……..
**Step n:** $x_n = \alpha^n x_{n-n} = \alpha^n x_0$

By obtaining the composite formula, we can find the population at any time t without wasting time to calculate the preceding populations.

**Example:** Suppose the population of bats increases at a constant rate of 2% each year and the initial population of the bats is 100:

- Deduce a formula to model the population of the bats in subsequent years.
- What will be the population of the bats in 30 years' time?

**Solution:**

- Let $x_0 = 100$ and rate of increase $\alpha = 1.02$

$x_1 = 1.02x_0 = 1.02(100)$
$x_2 = 1.02x_1 = 1.02\big(1.02(100)\big) = (1.02)^2(100)$
$x_3 = 1.02x_2 = (1.02)(1.02)^2(100)$
$= (1.02)^3(100)$
……
$x_n = (1.02)^n x_0 = (1.02)^n 100$

- Let $n = 15$ and $x_0 = 100$ then

$$x_{15} = (1.02)^{15}x_0 = (1.02)^{15}100$$
$$x_{15} = (1.02)^{15}100 = 135\ bats$$

## CONCLUSION

The study identified the inverse as an algebraic property of the Euclidean algorithm. This property has been applied in trading to maximize profit and used to find the inverse of numbers and matrices in a given modulo and further in cryptography to solve linear congruence problems.

Further, we applied the division property to find the gcd, quotient and the remainder of algebraic expressions in a given modulo. It was also used to find when two events occurring at successive time interval will occur together so as to prepare for their occurrences. Finally, the study provided an easier way of proving the Euclidean algorithm.

## REFERENCES

Bashmakova, I.G., 1948. The arithmetical books of Euclid's elements (Russian). Trudy Sem. MGU Istor. Mat. Istor.-Mat. Issledov., 1(1948): 296-328.

Fowler, D.H., 1999. The Mathematics of Plato's Academy. Oxford University Press, Oxford.

Gerard, B., 1973. Bossa and bossas: Recent changes in Brazilian urban popular music. Ethnomusicology, 17(2): 209-233.

Glasby, S.P., 1999. Extended Euclid's algorithm via backward recurrence relations. Math. Mag., 72(3): 228-230.

Honsberger, R., 1976. A theorem of Gabriel Lame. Ch. 7, In: Mathematical Gems II. Math. Assoc. Amer., Washington, DC, pp: 54-57.

Knuth, D.E., 1970. The analysis of algorithms. Actes, Congrès Intern. Math., Tome 3, pp: 269-274.

Knuth, D.E., 1997. The art of Computer Programming. Vol. 1: Fundamental Algorithms. 3rd Edn., Addison-Wesley, Reading, MA.

Narkiewicz, W., 2000. The Development of Prime Number Theory: From Euclid to Hardy and Littlewood. Springer-Verlag, New York.