Jayani, Manike, K.R.C. & R.A.D.Piyadasa
University of Kelaniya

*Paper: Diversity*

# Simple proof of two important theorems in number theory

Fermat's theorem (Theorem.1) which can be stated mathematically as $x^3 = y^2 + 2$ has only one solution that $x = 3, y = \pm 5$, has been proved using complex number field, unique factorization domain (UFD), etc.Fermat's proof of this theorem is vague [1] ,and as it is a well known theory related to the elliptic curves $x^3 = y^2 + c$, where $c$ is a constant, it is very difficult. The main objective of this paper is to prove this theorem and another [2], hereafter referred to as theorem.2, known to be difficult to prove, using a simple mathematical technique.

**Proof of the theorem .1**

$$x^3 = y^2 + 2 \tag{1.1}$$

We solve the above equation using elementary mathematics. First we notice that $y$ can not be even since then $y^2 + 2 \equiv 0 (\mathrm{mod}\, 2)$ (1.2)

and $x^3 \equiv 0(\mathrm{mod}\, 2^3)$ .Assume that $y \equiv 0(\mathrm{mod}\, 3)$ .Then if $y = 3j$ ,

$$x^3 + 1 = (x+1)[(x+1)^2 - 3x] = 9j^2 + 3 \tag{1.3}$$

from which it follows that $3 | (x+1)$ and $9 | (x^3 + 1)$ .But $9j^2 + 3$ can not be divisible by $9$ .Therefore $y$ is not divisible by $3$ .Hence $y = 3j \pm 1$ and

$$y^2 + 2 = 9j^2 \pm 6j + 3 = x^3 \tag{1.4}$$

Therefore $x$ is divisible by $3$ . Let $x = 3k$ .The

$$27(k^3 - 1) = y^2 - 25 = (y+5)(y-5) \tag{1.5}$$

This is obviously true when $k = 1, y = \pm 5$, that is,

$$x = 3, y = \pm 5 \tag{1.6}$$

Now we will show this is the only solution. We can write

$$27(k-1)(k^2 + k + 1) = A(y+5)[(y-5)/A] \tag{1.7}$$

and $$(y+5)A = k^2 + k + 1, 27(k-1) = \frac{y-5}{A} \tag{1.8}$$

where $A$ is an integer or a rational number. From these two equations, we get

$$[27A(k-1) + 10]A = (k^2 + k + 1) \tag{1.9}$$

This quadratic in $k$ must be satisfied by $k = 1$. Hence $A = \frac{3}{10}$ and we get from (1.9)

$$(100k-43)(k-1)=0 \tag{1.10}$$

Hence

$$k=1, k=\frac{43}{100} \tag{1.11}$$

and we conclude that $k=1$ is the only integer solution.

**Proof of Theorem .2**

We state theorem.2 as that the Diophantine equation,

$$x^3+x^2+x+1=d^2 \tag{2.1}$$

which is very difficult to prove [2], has only solution $x=1, x=7$ for x

We will solve the above equation also using our elementary mathematical technique.

If $x$ is odd, then $d$ should be even and let $d=2k$. Then our equation becomes

$$x^3+x^2+x+1=4k^2 \tag{2 .2}$$

It is obvious that $x=1, k=1$ satisfy the equation. Therefore $x=1$ is a solution of the equation and corresponding value of $d=2$. Assume that there are some other even $d$ values satisfying the equation. Now, we write (2.2) in the form

$$x(x^2+x+1)=(2k-1)(2k+1) \tag{2.3}$$

Clearly, $2k-1, 2k+1$ are co-prime, and hence we write

$$A(2k-1)=x, \frac{2k+1}{A}=x^2+x+1 \tag{2.4}$$

Since $x=1$, we get from these relations

$$x+2A=A^2(x^2+x+1) \tag{2.5}$$

$$(A-1)(3A+1)=0 \tag{2.6}$$

When $A=1$, $x=\pm 1$ and when $A=-\frac{1}{3}$, we get from (2.5)

$$x^2-8x+7=0 \tag{2.7}$$

which gives $x=1$, $x=7$. These are the only natural number solutions of the equation, corresponding to even $d$ numbers. Now, let $d=2m+1$, then we get

$$4m(m+1)=x(x^2+x+1) \tag{2.8}$$

from $x^3+x^2+x+1=d^2$. Let $Ax=4m$ and $\frac{x^2+x+1}{A}=m+1$. From these two relations, we get

$$A(Ax+4)=(x^2+x+1)4 \tag{2.9}$$

Since $x=0$ is an integer solution of the equation, we get $A=1$. Therefore we must have

$$4x^2+3x=0 \tag{2.10}$$

which gives no integer value for $x$ other than zero. Therefore $x=1, x=7$ are the only natural number solutions of the equation.

**References**

[1] Fermat and solution of $x^3 = y^2 + 2$ ,J.V.Leyendekkers; A.G.Shanon, *International Journal of Mathematical Education in Science andTechnology*,Vol.33,Issue.1, Jan.2002, pp.91-95

[2] Edwards H.M. (1977) *Fermat's last theorem: A Genetic Introduction to Algebraic Number Theory*. Springer-Verlag, pp.38