International Journal of Mathematics and Statistics Invention (IJMSI)
E-ISSN: 2321 – 4767 P-ISSN: 2321 - 4759
www.ijmsi.org Volume 12 Issue 2 || Mar.-Apr. 2024 || PP-55-56

Quadratic Residues and a Simple Theorem

D.Bratotini and M.Lewinter

Date of Submission: 25-04-2024 Date of acceptance: 02-05-2024

Abstract

We produce infinite classes of solutions of the Diophantine equation, $c=\frac{ab+1}{b-a}$, where *a*, *b*, and *c* are natural numbers such that $a \neq b$. We use them to show that $\frac{1}{abc}=\frac{1}{a}-\frac{1}{b}-\frac{1}{c}$.

Theorem 1: Let *a*, *b*, and *c* be natural numbers such that $a \neq b$, and $c=\frac{ab+1}{b-a}$. Then

$$\frac{1}{abc}=\frac{1}{a}-\frac{1}{b}-\frac{1}{c} \qquad (*)$$

Proof: Multiplying both sides of (*) by abc yields $1 = bc - ac - ab = c(b-a) - ab$, which becomes $c(b-a) = ab + 1$. Then $c=\frac{ab+1}{b-a}$. ■

Example 1: Let $a = 27$, $b = 37$, and $c = 100$. Since $\frac{ab+1}{b-a}=\frac{27\cdot 37+1}{37-27}=\frac{999+1}{10}=100=c$, we have $\frac{1}{99900}=\frac{1}{27}-\frac{1}{37}-\frac{1}{100}$. (Verify!)

Example 2: Let $a = 1$, $b = 2$, and $c = 3$. Since $\frac{1\cdot 2+1}{2-1}=3=c$, we have $\frac{1}{6}=\frac{1}{1}-\frac{1}{2}-\frac{1}{3}$.

Infinite Class of Solutions 1: If $b - a = 1$, we get $c = \frac{a(a+1)+1}{1} = a^2 + a + 1$, implying that there are infinitely many solutions of (*) of the form

$$a = a$$
$$b = a + 1$$
$$c = a^2 + a + 1$$

Infinite Class of Solutions 2: If $b - a = 2$ and *a* and *b* are odd, then $ab + 1$ is even, and, therefore, divisible by $b - a$. This generates infinitely many solutions.

Note that if $b - a = 3$, there are no solutions. If $b - a = 3$, then $b = a + 3$, in which case $ab + 1 = a(a + 3) + 1 = a^2 + 3a + 1$. Then $c=\frac{a^2+3a+1}{3}=a+\frac{a^2+1}{3}$. Since $a^2 = 0$ or $1 \pmod 3$, we have $a^2 + 1 = 1$ or $2 \pmod 3$, and is, therefore, not divisible by 3.

Theorem 2: There are infinitely many positive integer values for which $b - a \neq 1$ or 2, and $c = \frac{ab+1}{b-a}$ is a natural number.

We will need a definition and a preliminary fact to prove this.

Definition: a is a *quadratic residue* mod n if there exists an x such that $x^2 = a$ (mod n). Otherwise, a is a *quadratic nonresidue*.

Preliminary Fact: Let p be an *odd* prime. Then –1 is a quadratic residue mod p if $p = 1$ (mod 4). If $p = 3$ (mod 4), then –1 is a quadratic nonresidue mod p. [1][2]

Proof of Theorem 2: Let $b - a = p$, where $p = 1$ (mod 4). Then $b = a + p$, in which case $ab + 1 = a(a + p) + 1 = a^2 + ap + 1$. We will have a solution if and only if $a^2 + ap + 1 = 0$ (mod p). This is equivalent to $a^2 + 1 = 0$ (mod p), or $a^2 = -1$ (mod p) which has a solution by the Preliminary Fact.

Example: The prime number, 5, satisfies $5 = 1$ (mod 4). Now $b - a = 5$. Then $b = a + 5$, in which case $ab + 1 = a(a + 5) + 1 = a^2 + 5a + 1$. We have a solution if and only if $a^2 + 5a + 1 = 0$ (mod 5). This is equivalent to $a^2 + 1 = 0$ (mod 5), or $a^2 = -1$ (mod 5) which has a solution, $a = 2$ (mod 5). If $a = 2$, we have $b = 7$, and $c = \frac{2 \cdot 7 + 1}{5} = \frac{15}{5} = 3$. Also, $\frac{1}{2 \cdot 7 \cdot 3} = \frac{1}{2} - \frac{1}{7} - \frac{1}{3}$, or $\frac{1}{42} = \frac{1}{2} - \frac{1}{7} - \frac{1}{3}$. That is, $1 = 42\left(\frac{1}{2} - \frac{1}{7} - \frac{1}{3}\right) = 21 - 6 - 14$.

What happens if $b - a = n$, and n is composite? We will need a Second Preliminary Fact.

Second Preliminary Fact: Let n be a *composite* number. Then –1 is a quadratic residue mod n if for each *odd* prime divisor, p, we have $p = 1$ (mod 4). [1][2]

Using the Second Preliminary Fact, we obtain infinitely many solutions for which $b - a = n$, where n is composite and for each *odd* prime divisor, p, we have $p = 1$ (mod 4).

References

[1]. M.Lewinter, J.Meyer, Elementary Number Theory with Programming, Wiley & Sons. 2015.

[2]. D. Burton, Elementary Number Theory, McGraw-Hill, 2005.