4.26 Simple theorem on the integral roots of special class of prime degree polynomial equations

R.A.D.Piyadasa
Department of Mathematics, University of Kelaniya

ABSTRACT

Even in case of a simple polynomial $x^3 + 15xb + 28 = 0$, where $(3,b) = 1$, it may be extremely difficult to discard the integral solutions without knowing the number b exactly .In this case, one can make use of the method of Tartaglia and Cardan [Archbold J.W.1961] and its solutions can be written as $u + v, u\omega + v\omega^2, u\omega^2 + v\omega,$ where u^3, v^3 are the roots of the equation $x^2 + 28x - 125b^3 = 0,$ and ω is the cube root of unity .Also, u or v can be written as $\left(\dfrac{-28 \pm \sqrt{28^2 + 500b^3}}{2}\right)^{\frac{1}{3}}$ and this expression is obviously zero only when $b = 0$. Therefore if $b \neq 0$, it is very difficult to determine that $k = \left(\dfrac{-28 \pm \sqrt{28^2 + 500b^3}}{2}\right)^{\frac{1}{3}}$ is an integer or not .The theorem will be explained in the following , is Capable of discarding all integral solutions of this equation using only one condition $(3,b) = 1$.The theorem in its naive form discards all integral solutions of the polynomial . $x^p + pbx - c^p = 0,$ where p is a prime and $(p,b) = (p,c) = 1$

Theorem

$x^p + pbx - c^p = 0$ has no integral solutions if $(p,b) = (p,c) = 1$, where b, c are any integers and p is any prime .

Proof

Proof of the theorem is based on the following lemma

Lemma

If $(a,p) = (b,p) = 1,$ and if $s = a^p - b^p$ is divisible by p , then p^2 divides s. This is true even when $s = a^p + b^p$ and p is odd.

Proof of the Lemma

$s = a^p - a - (b^p - b) + a - b$ and since s is divisible by p and $a^p - a$, $b^p - b$ are divisible by p due to Fermat's little theorem, it follows that $a - b$ is divisible by p.

$$a^p - b^p = (a-b)[(a^{p-1} - b^{p-1}) + b(a^{p-2} - b^{p-2}) + \cdots + b^{p-3}(a-b) + pb^{p-1})] \quad (1)$$

From (1), it follows that s is divisible by p^2. Proof of the lemma for $a^p + b^p$ is almost the above. It is well known that the equation

$$x^p + pbx - c^p = 0 \quad (2)$$

has either integral or irrational roots.

If this equation has an integral root l, let $x = l$ and $(p,l) = 1$. Then , $l^p - c^p + pbl = 0.$

From the Lemma, it follows that $p^2 \mid (l^p - c^p)$. Therefore $p \mid b$, and this is a contradiction. Therefore equation has no integral roots which are not divisible by p. If it has an integral solution which is divisible by p, then let $x = p^\beta k, (p,k) = 1$. Then we have, $(p^\beta k)^p + pbp^\beta k - c^p = 0$, and hence $p \mid c$, which is again a contradiction since $(p,c) = 1$ which completes the proof.

As an special case of the theorem, consider the equation

$$x^3 + 15xb + 28 = 0 \tag{3}$$

which can be written as

$$x^3 + 1 + 15xb + 3^3 = 0 \tag{4}$$

and it is clear that this equation has no integral root $l \equiv 0 (\bmod 3)$ since 1 is not divisible by 3. If this equation has an integral root k which is not divisible by 3, then $k^3 + 1 + 15kb + 3^2 = 0$ from which it follows that $3 \mid b$ due to the Lemma(in case of negative c) and is a contradiction. Therefore the equation has no integral roots. In case of $p = 2$, it follows from the theorem that the equation

$$x^2 - 2bx - q^2 = 0$$

where $(2,q) = 1 = (2,b)$'has no integral roots. Again from the theorem it follows that $x^p - pcx - p^{\beta p}\alpha^p - b^p = 0$, where $(p,c) = 1 = (b,p)$ and p is a prime, has no integral solutions.. In particular here, $p^{\beta p}\alpha^3, b^p$ are two components of Fermat triples. It is easy to deduce that this equation has no integral roots. This theorem may hold for some other useful forms of polynomial equations.

References

(1) Archbold,J.W.1961 ,London Sir Issac Pitmann & Sons LTD pp174.