3.7 On the integer roots of a special class of prime degree polynomial equations

R.A.D.Piyadasa
Departmentof mathematics,Universiy of Kelaniya,Kelaniya,
Kelaniya,Sri Lanka
E-mail: Piyadasa54@yahoo.com

ABSTRACT

On the integer roots of a special class of prime degree polynomial equations

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

(Dedicated to late professor C.R.Kulatilaka)

Integer solutions of polynomial equations are very important in many respects [1]. However, solutions of general polynomial equations of degree five or bigger than five cannot be solved in radicals as well known. Even in case of a simple polynomial equation $x^3+15xb+28=0$, where $(3,b)=1$, it may be difficult to discard the integer solutions without knowing the value of b. The theorem will be explained in the next section , is capable of discarding all integral solutions of this equation using only one condition $(3,b)=1$. Also**,** it is useful to discard integer roots of a special class of prime degree polynomials as explained in this contribution.

Theorem and its proof.

$x^p+pbx-c^p=0$ has no integer solutions if $(p,b)=(p,c)=1$, where b,c are any non zero integers and p is any prime .The equation $x^p+p^m bx-c^p=0, m\geq 2$ has no integer solutions if $c\neq k(pa+1)$,where $(p,b)=(p,c)=1=(b,c)$.Also, the equation $x^p+pbx+c=0$ has no integer roots if $c=-a^p+p^m t\ ,m\geq 2$, where $(a,p)=(b,p)=1$.

Lemma.1

Let p be any odd prime and let a , b be any two non-zero integers satisfying $(a,p)=(b,p)=1$. If $s=a^p\pm b^p\equiv 0(\text{mod}\ p^\mu)$, then $\mu\geq 2$ and $a\pm b\equiv 0(\text{mod}\ p^{\mu-1})$. In particular if $p=2$, then $2^3\,|\,(a^2-b^2)$.

Proof of Lemma.1

$s=a^p-a\pm(b^p-b)+a\pm b$

Due to Fermat's little theorem, $p\,|\,(a^p-a)$, $p\,|\,(b^p-b)$ and since $p\,|\,s$, it follows that $a\pm b\equiv 0(\text{mod}\ p)$.

Now, let p be any odd prime and $s=a^p-b^p$, $a-b=p^k t$, where $(p,t)=1$, and $k\geq 1$.

$$s=\left(b+p^k t\right)^p-b^p \qquad (1)$$

$$=\left(p^{k+1}t\right)\left[p^{kp-(k+1)}t^{p-1}+p^{kp-2k}t^{p-2}b+\cdots+\frac{{}^p c_r}{p}p^{kp-(r+1)k}t^{r-1}b^r+........+b^{p-1}\right]=p^\mu x \qquad (2)$$

since $s \equiv 0(\text{mod } p^{\mu})$, where $(p,x)=1$. Obviously ${}^{p}c_{r} \equiv 0(\text{mod } p)$ and therefore $\mu = k+1$ since the term in the closed bracket is co-prime with p .Hence, $k+1=\mu$ and $\mu \geq 2$ since $k \geq 1$. The proof is almost exactly the same for the case $s = a^p + b^p$ .If $p = 2$, then $2^3 \mid (a^2 - b^2)$ since both a and b are odd and hence $a \pm b \equiv 0(\text{mod } 2)$ and one of $a-b,\ a+b$ must be divisible 2^l, $l > 1$ due to $(2,a)=1=(2,b)$.

Lemma.2

The real solutions of the polynomial equation

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots\cdots + a_n = 0 \qquad (3)$$

of x and degree n with integral coefficients $a_1, a_2 \cdots\cdots a_n$ are integers or irrational numbers. Proof of this lemma is simple and we assume this lemma without proof.

Proof of the theorem.

Theorem of our interest is

$$x^p + pbx - c^p = 0 \qquad (4)$$

has no integer solutions.

By the Lemma.2, the equation has integer or irrational solutions. If this equation has an integer solution when $(p,b)=(p,c)=1$,let it be $x = l$ and $(p,l)=1$ By substitution of this root in the equation, one obtains

$$l^p - c^p + pbl = 0 \qquad (5)$$

By the lemma $p^2 \| (l^p - c^p)$, and therefore $p \mid b$ and this is a contradiction Therefore the equation has no integral root not divisible by p .If it has an integer root which is divisible by p , let $x = p^{\beta}k, (p,k)=1$. Then, we have

$$p^{p\beta}k^p + p^{p+1}bk - c^p = 0 \qquad (6)$$

This is again a contradiction since $(p,c)=1$,and hence the equation has no integer solutions for any odd prime p. In case of $p = 2$, $(2,b)=(2,c))=1$, and therefore both b,c are odd. Therefore $(a-c),(a+c)$ are both even for any odd a and hence no any odd integer satisfies the equation since $(2,b)=1$. It is clear that c in the equation (6) can be negative.

Now, consider the equation

$$x^p + p^m bx - c^p = 0 \qquad (7)$$

If $(c,p)=1$, any integer root of this equation is also co-prime to p .Assume that an integer h satisfies the equation. Then $h^p + p^m bh - c^p = 0$ .By Lemma.1, $h - c = p^{m-1}t$ for some t and since h should be a factor of c^p , h should be of the form $h = k^p$,where k is a factor of c .Therefore $k^p = c + p^{m-1}i$ and $k^p - k = c - k + p^{m-1}t$ .Hence , $c - k = pd$ for some d since $k^p - k$ is divisible by p due to Fermat's little theorem. Also, k is a factor of c and therefore d is divisible by k .Therefore $c = k(pa+1)$ for some a and if this condition is violated, that is, if $c \neq k(pa+1)$,then the equation has no integer root k . Last part of the theorem follows at once from the Lemma.1.

The equation $x^3 + 15xb + 28 = 0$, $(b,3) = 1$ considered in the introduction of the paper can be written as

$$x^3 + 15xb + 1 + 3^3 = 0 \tag{8}$$

It is obvious that that any root x of this equation can not be divisible by 3 since $(3,1) = 1$.If x is not divisible by 3, then $x^3 + 1$ is divisible by 3^2 which contradicts $(3,b) = 1$.Hence the equation has no integer roots.

References

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