A Number-Theoretic Proof of the Solvability of Polynomials

Shahid Nawaz[1]

[1]18 Lake Shore Dr, Apt. 2B
Watervliet, NY 12189, USA
e-mail: snafridi@gmail.com

Abstract In this paper, we prove the solvability of polynomials based on partition function in number theory. Let $p(n)$ be the partition function, where n is the degree of a polynomial. We prove that a polynomial is solvable by radicals if $p(n) \leq n + 1$.

Keywords: Partition function, polynomial, abstract algebra, Galois theory, number theory, computation.

1 Introduction

Polynomial equations has a long history. In 2,000 BC, the Babylonians were able to solve the quadratic equation [1]. Though symbols were not available to them and neither they believed in negative numbers. Their methods were based on words (word-problems). Their method was limited to specific problems. A general method that involved words was given by the Indian mathematician Brahmagupta in seventh century [1]. Later in twelfth century, Omar Khayyam (1048–1131), a Persian polymath, solved the cubic equation using geometric methods. Regarding the general solution, an Italian mathematician, Luca Pacioli (1445–1509) noted in sixteenth century that the cubic equation had no general solution [2]. Scipione del Ferro (1465–1526) and later Niccolo Fontana (1499–1557), aka Tartaglia, solved the depressed cubic equation–a cubic equation that misses the square term. The general cubic equation was solved by Gerolamo Cardano (1501–1576). Ludovico Ferrari (1522–1565) solved the general quartic equation. The challenge was the quintic equation. In 1798, P. Ruffini (1765–1822) and later in 1826, Niels Henrik Abel (1802–1829) proved that the quintic equation has no general solution by radicals. Finally, Évariste Galois (1811–1832) found a connection between group theory and solvability of polynomials and so emerged the Galois theory.

In this paper, we find a connection between partition function in number theory and the solvability of polynomials. A partition is a representation of a non-negative number n to express it as the sum of any number of positive integral parts [3, 4]. Let n be a positive integer, then:

$$n = p_1 + p_2 + \ldots + p_k \,, \tag{1}$$

where p_i is a part of the partition. For example, one can write 5 as $5, 4+1, 2+3, 2+2+1, 3+1+1, 2+1+1+1, 1+1+1+1+1$. One can see that $p(5) = 7$. The

https://doi.org/10.32388/8AOIDT

partition function grows quickly. For instance, $p(200) = 3,972,999,029,388$ [5]. Our main result is given in the following theorem.

Theorem 1. *Let $p(n)$ be the partition of n, where n is the degree of a polynomial, then the polynomial is solvable by radicals if $p(n) \leq n + 1$.*

Proof. It can be checked by direct computation. One can observe that $p(1) = 1 \leq 2$, $p(2) = 2 \leq 3$, $p(3) = 3 \leq 4$, $p(4) = 5 \leq 5$. But $p(5) = 7 \not\leq 6$. And for $n > 5$, $p(n)$ is larger than $n + 1$, as the partition function grows quickly. □

Remark 1. One may ask whether theorem 1 is just a coincident or there is a deep connection between polynomials and partition function. We explore this in what follows.

2 Main results

Let F be a field. Let $F[x]$ be the ring of polynomials with coefficients in F. We also consider monic polynomials where the coefficient of the leading term is unity. We have:

$$f_n(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \,. \tag{2}$$

When dealing with polynomials, it is important to keep track of various rings such as the ring of polynomials, the ring of the coefficients, the ring of zeros of the polynomials. Since we are investigating polynomials in regards to partition, it suffices to keep track of polynomials ring by introducing a convenient notation:

$$f_n := (n, n-1, \ldots, 2, 1, 0) \,, \tag{3}$$

where the entries in the array on the right are the exponents of x. The first entry gives us the degree of polynomial which is n. The length of the polynomial, denoted by $|f_n|$, is defined to be the the number of entries in the array. One can observe that $|f_n| = n + 1$. The actual length of f_n may be smaller than $n + 1$ if there are zero terms where $a_i = 0$. But it is convenient to keep all terms from n to 0. Let there is another polynomial g_n of the same length. We say that the two polynomials f_n and g_n are equal upto their coefficients. Without loss of generality, we may denote all polynomials by symbol f such as f_m and f_n etc.

Upto coefficients, all polynomials live in one unified ring R. The ring R has interesting properties given below.

Theorem 2. *Let f_m and f_n be two polynomials, then*

$$f_m f_n = f_{m+n} \,. \tag{4}$$

Proof. We have

$$f_m = (m, m-1, \ldots, 1, 0) \,. \tag{5}$$

$$f_n = (n, n-1, \ldots, 1, 0) \,. \tag{6}$$

Then

$$\begin{aligned} f_m f_n &= (m, m-1, \ldots, 1, 0)(n, n-1, \ldots, 1, 0) \\ &= (m+n, m+n-1, \ldots, 1, 0) \\ &= f_{m+n}\,, \end{aligned} \tag{7}$$

where the second equality follows from the fact that $x^m x^n = x^{m+n}$. Similarly the other entries can be obtained. □

Theorem 3. *Let f_m and f_n be two polynomials, then*

$$f_m + f_n = f_{\max(m,n)}\,. \tag{8}$$

Proof.

$$\begin{aligned} f_m + f_n &= (m, m-1, \ldots, 1, 0) + (n, n-1, \ldots, 1, 0) \\ &= (\max(m,n), \max(m,n)-1, \ldots, 1, 0) \\ &= f_{\max(m,n)}\,, \end{aligned} \tag{9}$$

where the second equality follows from the fact when two polynomials are added, then the polynomial with smaller number of terms will be absorbed in the longer polynomial. □

Note that theorem 3 gives a paradoxical result when $m = n$. Which gives $2f_n = f_n$. Since $f_n \neq 0$, this implies that $2 = 0$. In fact, the paradox appears due to the fact the polynomials are unique up to coefficients. The paradox can be resolved by multiplying 2 through out and then redefine the coefficients.

Theorem 4. *Let $n \leq m$. Then f_n divides f_m. Further, $\frac{f_m}{f_n} = f_{m-n}$.*

Proof. By division algorithm we have:

$$f_m = f_n f_k + f_l\,, \tag{10}$$

where f_k and f_l are two polynomials with $l < k$. By using theorems 2 and 3 we have

$$f_m = (\max(n+k, l), \max(n+k, l) - 1, \ldots, 1, 0)\,. \tag{11}$$

Since $n + k > l$, therefore $\max(n + k, l) = n + k$. Hence

$$f_m = f_{n+k}\,. \tag{12}$$

This means that $m = n + k$. Also by theorem 2 we have:

$$f_m = f_n f_k \Rightarrow \quad \frac{f_m}{f_n} = f_k\,. \tag{13}$$

From it follows that $f_n | f_m$. The second part of the theorem also follows as $k = m - n$. So then $\frac{f_m}{f_n} = f_{m-n}$. □

Since our main concern is to prove the solvability of polynomials. We set the criterion in the following definition.

Definition 1. Let L be a partition. Let p_i be a part that appears m times in L. Then, in the chain of equalities, the polynomial is said to be solvable if p_i does not appear m times in another partition.

For example, let $n = 100$. Consider the following chain of equalities of 100:

$$f_{100} = f_{96+2+2} = f_{94+2+2+1+1} = \dots .$$

Here $L_1 = 96 + 2 + 2$ and $L_2 = 94 + 2 + 2 + 1 + 1$. One can see that in L_1 and L_2 the part 2 appears twice. Thus a polynomial for $n = 100$ is not solvable.

Now we give a second proof of theorem 1 based on definition 1.

Proof. We prove it by direct computation. We start with $n = 1$ which is trivially true as the chain of equalities contains f_1 only. For $n = 2$ we have:

$$f_2 = f_{1+1} . \tag{14}$$

Since it satisfies the criterion set in definition 1 as no part is repeating on both side of the equalities. Next is $n = 3$. The chain of equalities is given by:

$$f_3 = f_{2+1} = f_{1+1+1} . \tag{15}$$

It also satisfies the criterion of definition 1. Now $n = 4$, we have:

$$f_4 = f_{3+1} = f_{2+2} = f_{2+1+1} = f_{1+1+1+1} , \tag{16}$$

which also meets the condition of definition 1. For $n = 5$. We have:

$$f_5 = f_{4+1} = f_{2+2+1} = f_{3+2} = f_{3+1+1} = f_{2+1+1+1} = f_{1+1+1+1+1} . \tag{17}$$

One can see that it violates definition 1 as in $f_{4+1} = f_{2+2+1}$ the part 1 appears one times. Hence $n = 5$ is not solvable. The generalization is straightforward. Let $n > 5$. We would have partitions like

$$f_{\overline{n-1}+1} = f_{\overline{n-3}+2+1} = \dots . \tag{18}$$

One can see that part 1 repeats one time in both partitions. Hence a polynomial is insolvable for $n \geq 5$.

We have partly proved the theorem. The next part is to prove solvabiity by radicals. Consider g_n given by:

$$g_n = (n, 0) \tag{19}$$

One can see it has only two terms. Writing it explicitly in terms of the coefficients, we have:

$$g_n(x) = x^n + a_0 . \tag{20}$$

Let α be a root, then:

$$\alpha = (-a_0)^{1/n} e^{2\pi i/n} \,. \tag{21}$$

Since g_n and f_n are equivalent upto coefficients, we have:

$$f_n = g_n((-a_0)^{1/n}) \,. \tag{22}$$

□

In summary, a polynomial is solvable by radicals if $p(n) \leq n+1$, where $p(n)$ is the partition function.

References

[1] J. Stillwell, "Mathematics and Its History," (Springer, New York 2010)

[2] T.W. Judson, "Abstract Algebra," `abstract.pugetsound.edu`

[3] G.H. Hardy and E.M. Wright, "An Introduction to the Theory of Numbers," sixth ed. (Oxford University Press, New York, 2008)

[4] T.M. Apostal, "Introduction to Analytic Number Theory," (Springer, 1976)

[5] G.E Andrews, "Number Theory," (Dover Publication, Inc., New York, 1994)