American Journal of Educational Research, 2019, Vol. 7, No. 12, 989-993
Available online at http://pubs.sciepub.com/education/7/12/14
Published by Science and Education Publishing
DOI:10.12691/education-7-12-14

An Elementary Method in Number Theory

Nguyen Thanh Quang[1,*], Phan Duc Tuan[2]

[1]School of Natural Science Education, Vinh University, Vinh City, Vietnam
[2]Department of Applied Mathematics, Saigon University, Ho Chi Minh City, Vietnam
*Corresponding author: ntquangdhv@gmail.com

Received November 06, 2019; Revised December 26, 2019; Accepted December 30, 2019

Abstract In order to apply the role of the analogues between integers and polynomials, in this paper we introduce a unified diagram to the Fermat's theorem, Mason's theorem, Davenport's theorem and some arithmetic conjectures. Further, we show some applications of this diagram in teaching and researching on arithmetic. By using this elementary method in number theory, we obtained some results for polynomials and holomorphic functions in case complex and *p*-adic.

Keywords: *integer, polynomial, analogue, mason's theorem, abc conjecture*

Cite This Article: Nguyen Thanh Quang, and Phan Duc Tuan, "An Elementary Method in Number Theory." *American Journal of Educational Research*, vol. 7, no. 12 (2019): 989-993. doi: 10.12691/education-7-12-14.

1. Introduction

It is a fact frequently remarked upon that integers and polynomials share a number of characteristics, we can list some of the following similarities between integers and polynomials.

1) For integers, we have prime numbers and for polynomials, we have irreducible polynomials.

2) For two integers, as for two polynomials, we can to define the greatest common divisor. Moreover, in both cases, the greatest common divisor is found by the Euclidean algorithm.

3) The absolute value of an integer is an analogue to the degree of a polynomial.

4) The rational numbers are analogues to the rational functions (the quotient of two polynomials).

5) There are two similar versions between theorems of remainder division on integers and on polynomials.

6) The number of distinct prime divisors of an integer is an analogue to the number of linear divisors of a polynomial on the field of complex numbers.

We can continue to extend the list of the analogs through some other concepts, properties and results of integers and polynomials.

On the role of the analogues between integers and polynomials in arithmetic studies, we can say that development of arithmetic, especially in recent decades, is greatly influenced by the analogues between integers and polynomials. In other words, when there is an open question for integers, we try to prove the same results for polynomials. That is often easier to do, perhaps because for the polynomial have a derivative, while a similar concept does not exist for integers.

By using the analogues between integers and polynomials, when studying the Fermat's equation, Mason proved a very nice theorem for polynomials. From this theorem, we obtain an analogue of the Fermat's last theorem for polynomials on the field of complex number fields. Furthermore, Mason's theorem has suggested of the *abc* conjecture. It is very interesting that from the *abc* conjecture, there are many well-known arithmetic conjectures can be deduced. Thus, the *abc* conjecture became a central problem of arithmetic in the twenty-first century.

The analogues between integers and polynomials continue to be extended for polynomials of sevaral variables or holomorphic functions in complex case. By using this method, N. T. Quang, P. D. Tuan (see [1-5]) and C. Toropu (see [6,7]) have also obtained some results on polynomials and *p*-adic entire functions of several variables.

In order to apply the important role of the analogues between integers and polynomials on the teaching and researching of arithmetic, this paper introduces a unified arithmetic diagram to Fermat's theorem, Mason's theorem and Davenport's theorem with some arithmetic conjectures.

2. Content

2.1. Some Base Concepts and Results

2.1.1. Definition. Recall that the *radical* of the nonzero integer m is the product of the distinct prime number that divide m, that is,

$$\mathrm{rad}(m)=\prod_{p|m} p.$$

2.1.2. Definition. Let $f(t)$ be a polynomial of degree n on the field of complex numbers. If $\alpha_1,...,\alpha_r$ are the distinct complex zeros of $f(t)$, then we can factor $f(t)$ into a product of linear terms of the form

$$f(t)=c_n(t-\alpha_1)^{m_1}(t-\alpha_2)^{m_2}\cdots(t-\alpha_r)^{m_r},$$

where the leading coefficient $c_n\neq 0$ and $m_1+\cdots+m_r=n=\deg(f)$. The *radical of the polynomial* $f(t)$ is defined by

$$\mathrm{rad}(f)=(t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_r).$$

The complex zero set of the complex polynomial $f(x)$ is a finite set

$$Z(f)=\{\alpha\in\mathbb{C}: f(\alpha)=0\}=\{\alpha_1,...,\alpha_r\}.$$

Let $N_0(f)$ denote the number of distinct zeros of $f(x)$, that is $N_0(f)=r$. The degree of the radical of $f(t)$ is the number of distinct zeros of $f(t)$, that is $\deg(\mathrm{rad}(f))=N_0(f)$.

This is an important Diophantine inequality for polynomials on the field of complex numbers.

2.1.3. Mason's theorem (see [8]) If a,b,c are nonzero, relative prime polynomials, not all constant, and if $a+b=c$ then

$$\max\{\deg(a),\deg(b),\deg(c)\}\leq N_0(abc)-1,$$

where $N_0(abc)$ *denotes the number of distinct zeros of the polynomial* abc.

2.2. Some Corollaries of Mason's Theorem

The following arithmetic conjecture, by Marshall Hall in 1971, when he studied Diophantine equations $x^3-y^2=k$, where k is a given integer.

2.2.1. Hall's conjecture. *There is a positive constant* C *such that for any integers* x *and* y *for which* $x^3\neq y^2$,

$$\left|x^3-y^2\right|>C\sqrt{|x|}.$$

In 1965, Davenport [9] proved an analogue of the above conjecture in the case of polynomials. This is a direct consequence of Mason's theorem.

2.2.2. Davenport's theorem ([9])**.** *Let* f *and* g *be nonconstant, relatively prime polynomials. Then*

$$\deg(f^3-g^2)\geq\frac{1}{2}\deg(f)+1.$$

Proof. We apply Mason's theorem with $a=g^2$, $b=f^3-g^2$, $c=f^3$. Then

$$\begin{aligned}\deg(g^2)&\leq N_0(g^2(f^3-g^2)f^3)-1\\&=N_0(g(f^3-g^2)f)-1\\&\leq\deg(g(f^3-g^2)f)\\&=\deg(g)+\deg(f^3-g^2)+\deg(f).\end{aligned}$$

It follows that

$$2\deg(g)\leq\deg(g)+\deg(f^3-g^2)+\deg(f)-1.$$

Similarly, we have

$$3\deg(f)\leq\deg(g)+\deg(f^3-g^2)+\deg(f)-1.$$

From two inequalities, we obtain

$$\deg(f^3-g^2)\geq\frac{1}{2}\deg(f)+1.$$

Davenport's theorem is proved.

By using Mason's theorem, we find many other versions of Davenport's theorem.

2.2.3. Generalized Davenport's theorem. *Let* f,g *be relatively prime non-constant polynomials and let* m,n *be any positive integers. Then*

$$\deg(f^n-g^m)\geq\frac{nm-n-m}{m}\deg(f)+1.$$

Proof. We apply Mason's theorem with $a=f^n$, $b=g^m-f^n$, $c=g^m$. Then

$$\begin{aligned}\deg(f^n)&\leq N_0(f^n(f^n-g^m)g^m)-1\\&=N_0(f(f^n-g^m)g)-1\\&\leq\deg(f(f^n-g^m)g)-1\\&=\deg(f)+\deg(f^n-g^m)+\deg(g)-1.\end{aligned}$$

It follows that

$$n\deg(f)\leq\deg(f)+\deg(f^n-g^m)+\deg(g)-1. \quad (1)$$

Multiply the inequality (1) by $(m-1)$ we have

$$\begin{aligned}&(m-1)n\deg(f)\\&\leq(m-1)\deg(f)+(m-1)\deg(f^n-g^m)\\&\quad+(m-1)\deg(g)-(m-1).\end{aligned} \quad (2)$$

We have

$$m\deg(g)\leq\deg(f)+\deg(f^n-g^m)+\deg(g)-1. \quad (3)$$

From (2) and (3) we have

$$(nm-n-m)\deg(f)\leq m\deg(f^n-g^m)-m. \quad (4)$$

From (4) we obtain the generalized Davenport's inequality:

$$\deg(f^n-g^m)\geq\frac{nm-n-m}{m}\deg(f)+1.$$

The Fermat last theorem states that, for $n\geq 3$ the Fermat's equation $x^n+y^n=z^n$ has no solution in positive integers. The Fermat's equation has solutions in complex polynomials for $n=2$, for example:

$$(1-t^2)^2+(2t)^2=(1+t^2)^2.$$

We shall use Mason's theorem to prove Fermat's last theorem for complex polynomials.

2.2.4. Theorem (see [[10], pp. 183]) *If* $n \geq 3$, *then Fermat's equation* $x^n + y^n = z^n$ *has no solution in nonzero, relatively prime polynomials, not all constant.*

Proof. Let $n \geq 3$, and suppose that x, y, z are nonzero, relatively prime polynomials, not all constants, such that $x^n + y^n = z^n$. We apply Mason's theorem with $a = x^n, b = y^n, c = z^n$. Then

$$N_0(abc) = N_0\left(x^n y^n z^n\right) = N_0(xyz).$$

Since $\deg\left(x^n\right) = n\deg(x)$, we obtain

$$\begin{aligned} n\deg(x) &\leq n\max\{\deg(x), \deg(y), \deg(z)\} \\ &= \max\left\{\deg\left(x^n\right), \deg\left(y^n\right), \deg\left(z^n\right)\right\} \\ &= \max\{\deg(a), \deg(b), \deg(c)\} \\ &\leq N_0(abc) - 1 \\ &= N_0(xyz) - 1 \\ &\leq \deg(xyz) - 1 \\ &= \deg(x) + \deg(y) + \deg(z) - 1. \end{aligned}$$

It follows that

$$\begin{aligned} & n\left(\deg(x) + \deg(y) + \deg(z)\right) \\ & \leq 3\left(\deg(x) + \deg(y) + \deg(z)\right) - 3 \\ & \leq n\left(\deg(x) + \deg(y) + \deg(z)\right) - 3. \end{aligned}$$

This is impossible. The Fermat's last theorem for polynomials has been proved.

2.2.5. Theorem. *The generalized Fermat's equation* $x^m + y^n = z^k$ *has no solution in nonconstant, relatively prime polynomials if*

$$\frac{1}{m} + \frac{1}{n} + \frac{1}{k} \leq 1,$$

where m, n, k *are positive integers.*

Proof. Let $\frac{1}{m} + \frac{1}{n} + \frac{1}{k} \leq 1$, and suppose that x, y, z are nonconstant, relatively prime polynomials such that $x^m + y^n = z^k$. By using the Mason's theorem with $a = x^m, b = y^n, c = z^k$, we have

$$\begin{aligned} \deg(a) &\leq N_0(abc) - 1 \\ &= N_0\left(x^m y^n z^k\right) - 1 \\ &= N_0(xyz) - 1 \\ &\leq \deg(xyz) - 1 \\ &= \deg(x) + \deg(y) + \deg(z) - 1. \end{aligned}$$

Since $\deg(a) = \deg\left(x^m\right) = m\deg(x)$, we obtain

$$\begin{cases} m\deg(x) \leq \deg(x) + \deg(y) + \deg(z) - 1 \\ n\deg(x) \leq \deg(x) + \deg(y) + \deg(z) - 1 \\ k\deg(x) \leq \deg(x) + \deg(y) + \deg(z) - 1. \end{cases}$$

It follows that

$$\frac{1}{m} + \frac{1}{n} + \frac{1}{k} \geq \frac{\deg(x) + \deg(y) + \deg(z)}{\deg(x) + \deg(y) + \deg(z) - 1} > 1.$$

This is impossible. The Fermat's generalized theorem for polynomials has been proved.

If in the ring of integers we have a theorem that says that the equation $x^4 + y^4 = z^2$ has no solution in positive integers, then in the complex polynomial ring we have the following result.

2.2.6. Theorem. *The equation* $x^4 + y^4 = z^2$ *has no solution in nonzero, relatively prime polynomials, not all constant.*

Proof. We suppose that (f, g, h) are nonzero, relatively prime polynomials, not all constant, such that $x^4 + y^4 = z^2$. We apply Mason's theorem with $a = f^4, b = g^4, c = h^2$. Then

$$\begin{aligned} & \max\left\{\deg\left(f^4\right), \deg\left(g^4\right), \deg\left(h^2\right)\right\} \\ & \leq N_0\left(f^4 g^4 h^2\right) - 1 \\ & = N_0(fgh) - 1 \\ & \leq \deg(fgh) - 1 \\ & \leq \deg(f) + \deg(g) + \deg(h) - 1. \end{aligned}$$

It follows that

$$4\deg(f) \leq \deg(f) + \deg(g) + \deg(h) - 1 \quad (5)$$

$$4\deg(g) \leq \deg(f) + \deg(g) + \deg(h) - 1 \quad (6)$$

$$2\deg(h) \leq \deg(f) + \deg(g) + \deg(h) - 1. \quad (7)$$

From (7) we have

$$\deg(h) \leq \deg(f) + \deg(g) - 1. \quad (8)$$

From inequalities (5) and (6), we obtain

$$\deg(f) + \deg(g) \leq \deg(h) - 1. \quad (9)$$

From (8) and (9), it follows that $0 \leq -2$. We have a contradiction.

While the Catalan equation $x^m - y^n = 1$ currently has not been solved for integers, but the corresponding polynomial equation was had the following answer by using the Mason's theorem.

2.2.7. Theorem [11]**.** *The equation* $x^m - y^n = 1$ *has no solution in non-constant polynomials* f, g *and integers* $m > 1$ *and* $n > 1$.

Proof. Let f, g be relatively prime polynomials, not all constant, such that $f^m - g^n = 1$. By using Mason's theorem with $a = f^m, b = -g^n, c = 1$, we have:

$$\begin{aligned} \max\left\{\deg f^m, \deg g^n\right\} &\leq N_0(f^m g^n) - 1 \\ &= N_0(fg) - 1 \\ &\leq \deg(fg) - 1 \\ &\leq \deg(f) + \deg(g) - 1. \end{aligned}$$

From there we have

$$m\deg(f) \le \deg(f) + \deg(g) - 1, \quad (10)$$

$$n\deg(g) \le \deg(f) + \deg(g) - 1. \quad (11)$$

From inequalities (10) and (11), we obtain:

$$(m-2)\deg(f) + (n-2)\deg(g) \le -2. \quad (12)$$

Since $m \ge 2$ and $n \ge 2$, the inequality (12) is impossible. We have a contradiction.

2.3. The *abc* Conjecture and Its Applications

When studying a problem for integers, we often study its analogues on the function fields for polynomials and rational functions. The role of this analogues is not merely to convert objects from integers into polynomials or vice versa, but it also gives us a studying methodology in number theory. Numerical conversion thinking can be applied to studies of polynomials with tools such as derivatives, solutions, multiple solutions, degree, greatest common divisor, factor analysis. In contrast, from the results of polynomials we apply on integers by the similarly techniques.

From Mason's theorem by converting polynomial to integer, the *abc* conjecture was independently formulated by David Masser and Joseph Oesterle in 1986.

2.3.1. The abc Conjecture (see [[10], pp. 185]) For every $\varepsilon > 0$ there exists a number $K(\varepsilon) > 0$ such that, if a, b and c are nonzero, relative prime integers and $a + b = c$, then

$$\max(|a|, |b|, |c|) \le K(\varepsilon)\mathrm{rad}(abc)^{1+\varepsilon}.$$

The *abc* conjecture has a large number of consequences. To prove or disprove this conjecture is an important unsolved problem in number theory. Here are some examples.

The Fermat's last theorem states that, for $n \ge 3$, the Fermat equation $x^n + y^n = z^n$ has no solution in positive integers. If *abc* conjecture were true, it would imply Fermat's last theorem for sufficiently large powers. Goldfeld (1996) described the *abc* conjecture as "the most important unsolved problem in Diophantine analysis".

2.3.2. Asymptotic Fermat's Theorem (see [[10], pp. 185]) The *abc* conjecture implies that there exists an integer n_0 such that the Fermat's equation has no solution in relatively prime integers for any exponent $n \ge n_0$.

Proof. Let x, y, z be relatively prime positive integers such that $x^n + y^n = z^n$. We note that

$$\mathrm{rad}(x^n y^n z^n) = \mathrm{rad}(xyz) \le xyz < z^3.$$

If $n \ge 2$, then $z \ge 3$. Applying the *abc* conjecture with $\varepsilon = 1$ and $K_1 = \max\{1, K(1)\}$, we obtain

$$z^n = \max\{x^n, y^n, z^n\} \le K_1\mathrm{rad}(x^n y^n z^n)^2 < K_1 z^6.$$

So

$$n < 6 + \frac{\log K_1}{\log z} \le 6 + \frac{\log K_1}{\log 3}.$$

Thus, for any exponent $n \ge n_0 = 6 + \left[\frac{\log K_1}{\log 3}\right]$ the Fermat's equation $x^n + y^n = z^n$ has no solution in relatively prime integers. This completes the proof.

The Catalan conjecture assert that the only solution of the equation $x^m - y^n = 1$ in integers x, y, m, n all greater than 1 is $3^2 - 2^3 = 1$.

Now, we consider the Catalan equation only for $\min(m, n) \ge 3$.

2.3.3. Asymptotic Catalan theorem (see [[10], pp. 186]) *The abc conjecture implies that the Catalan equation has only finitely many solutions.*

Proof. Let (x, y, m, n) be a solution of the Catalan equation with $\min(m, n) \ge 3$. Then x and y are relatively prime. It follow from the *abc* conjecture with $\varepsilon = \frac{1}{4}$ that there exists a constant $K_2 = K\left(\frac{1}{4}\right)$ such that

$$y^n < x^m \le K_2\mathrm{rad}(x^m y^n)^{\frac{5}{4}} = K_2\mathrm{rad}(xy)^{\frac{5}{4}} \le K_2(xy)^{\frac{5}{4}}.$$

We have

$$m\log x \le \log K_2 + \frac{5}{4}(\log x + \log y),$$

$$n\log y \le \log K_2 + \frac{5}{4}(\log x + \log y).$$

It follows that

$$m\log x + n\log y \le 2\log K_2 + \frac{5}{2}(\log x + \log y). \quad (13)$$

So

$$\left(m - \frac{5}{2}\right)\log x + \left(n - \frac{5}{2}\right)\log y \le 2\log K_2.$$

Since $x \ge 2$ and $y \ge 2$, we have

$$m + n < \frac{2\log K_2}{\log 2} + 5.$$

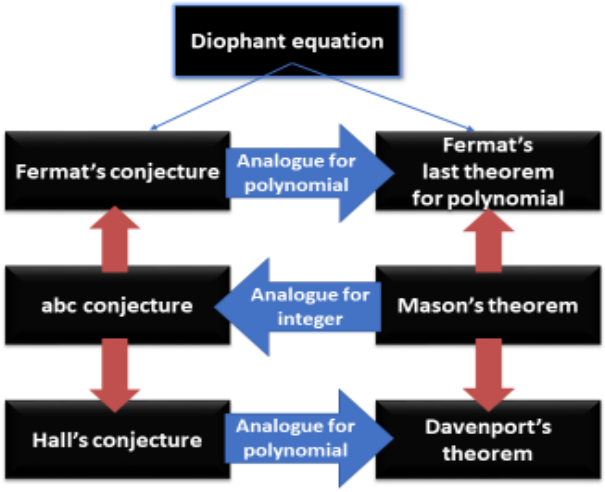
Thus, there are only finitely many pairs of exponents (m, n) for which the Catalan equation is solvable. For fixed exponents $m \ge 3$ and $n \ge 3$, inequality (13) has only finitely many solutions in positive integers x and y. This completes the proof.

3. Conclusion

Thus, from a basic problem of arithmetic is the problem of solving Diophantine equations, we have a unified arithmetic diagram (see diagram below). This diagram established a relationship between Fermat's last theorem, asymptotic Fermat's theorem, Mason's theorem, Davenport's theorem with the Hall conjecture and the *abc* conjecture.

Through the above analysis, we confirm that arithmetic has many different fields but they are united in a perfect whole. This unity is a way for much hope to conquer the heights of mathematics.

The beauty of mathematics is the unity. This makes arithmetic become closer. As a result, our learning and teaching on arithmetic are becoming more interesting and effective.



References

[1] Nguyen Thanh Quang and Phan Duc Tuan (2007), A note on Browkin-Brzezinski's Conjecture, Int. J. Contemp. Math. Sciences, Vol. 2, pp. 1335-1340.

[2] Nguyen Thanh Quang and Phan Duc Tuan (2008), An Extension of Davenport's Theorem for Functions of Several Variables, International Journal of Algebra, Vol. 2, No. 10, pp. 469-475.

[3] Nguyen Thanh Quang and Phan Duc Tuan (2008), A generalization of the abc Conjecture over Function Fields, Journal of Analysis and Applications, Vol. 6, pp. 69-76.

[4] Phan Duc Tuan, Nguyen Thanh Quang (2016), Picard values and uniqueness p-adic meromorphic functions, Acta Mathematica Vietnammica, Vol. 41, No.4, pp. 563-582.

[5] Phan Duc Tuan, Nguyen Thanh Quang (2016), Differential polynomials and value-sharing, Annales Univ. Sci. Budapest., 45, pp. 23-44.

[6] William Cherry and Cristina Toropu (2009), Generalized abc theorems for non-Archimedean entire functions of several variables in arbitrary characteristic, Acta Arithmetica, Vol. 136, No. 4, pp. 351-384.

[7] Cristina Toropu (2014), abc theorems in functional case, Dissertation of Philosophy Doctor on Mathematics, The University of New Mexico.

[8] Mason, R. C. (1984), Diophantine Equations over Function Fields, Cambridge University Press.

[9] H. Davenport (1965), On Norske Vid. Selsk. Forrh. 38, pp. 86-87.

[10] Melvyn B. Nathanson (2000), Elementary Methods in Number Theory, Springer.

[11] Melvyn B. Nathanson (1974), Catalan's equation in Amer. Math. Monthly, Vol. 81, pp. 371-373.