Appl. Math. J. Chinese Univ.
2024, 39(1): 159-173

Diophantine equations and Fermat's last theorem for multivariate (skew-)polynomials

PAN Jie[1] JIA Yu-ming[2] LI Fang[1,*]

Abstract. Fermat's Last Theorem is a famous theorem in number theory which is difficult to prove. However, it is known that the version of polynomials with one variable of Fermat's Last Theorem over $\mathbb{C}$ can be proved very concisely. The aim of this paper is to study the similar problems about Fermat's Last Theorem for multivariate (skew)-polynomials with any characteristic.

§1 Introduction

Fermat's Last Theorem is a famous theorem in number theory, which is named after the famous mathematician Pierre de Fermat, who first gave the conjecture in 1637. The theorem itself is a very simple statement, but it is so difficult that nobody could solve it completely for 358 years until Andrew Wiles gave a complete proof in 1995, for which he was honoured and received the Fields Medal.

In "Arithmetica", a book written by the famous Ancient Greek mathematician Diophantus in the 3rd century A.D., it was stated in Problem II.8 how a given square number can be written into the sum of two other square numbers. In about 1637, Fermat wrote his Last Theorem in the margin of Bachet's edition of the works of Diophantus, which states as follows:

"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain."

Today we state Fermat's Last Theorem in this way:

Theorem 1.1 (Fermat's Last Theorem)**.** *The Diophantine equation*

$$x^n + y^n = z^n$$

has no nontrivial integral solutions for any integer $n \geqslant 3$.

Received: 2021-12-06. Revised: 2022-01-22.
MR Subject Classification: 11C08, 11D41.
Keywords: Fermat's last theorem, polynomial ring, skew polynomial ring.
Digital Object Identifier(DOI): https://doi.org/10.1007/s11766-024-4630-6.
This project is supported by the National Natural Science Foundation of China(12131015, 12071422).
*Corresponding author.

Fermat only gave the proof of Fermat's Last Theorem in a special case where $n = 4$. And in the following many years, mathematicians figured out the proof for special cases where $n = 3, 5, 7$. In 1850, Ernst Kummer proved the cases when $2 < n < 100$, which extended the results to a great extent. When it comes to 1922, the English mathematician Louis Mordell posed a conjecture, the so-called Louis Mordell's conjecture, by which we can get that the Diophantine equation $x^n + y^n = z^n$ has at most a finite number of nontrivial primitive integer solutions, when $n > 2$. By the year 1983, the conjecture had been solved by Gerd Faltings, a German mathematician, who won the 1986 Fields Prize for this work. Other mathematicians, such as Harry Vandiver and Samuel Wagstaff, have extended Kummer's approach by computational methods to all primes less than four million by 1993. However, mathematicians still had no idea how to prove the conjecture for all of the primes.

In about 1955, Goro Shimura and Yutaka Taniyama, two Japanese mathematicians, found a possible relation between elliptic curves and modular forms, which are two apparently completely distinct branches of mathematics. This is called the Taniyama-Shimura-Weil theorem, which makes a great contribution to solving Fermat's last theorem.

Theorem 1.2 (Taniyama-Shimura-Weil theorem)**.** *([8]) If E is a elliptic curve defined over $\mathbb{Q}$, and N is its conductor, then there is a new cusp eigenform f of level N, whose Fourier coefficients c_n are integers such that for every prime p not dividing N, $c_p = a_p$ (where a_p is defined by counting the number of points in E over $\mathbb{F}_p$).*

In 1984, Gerhard Frey noted a link between Fermat's equation and the modularity theorem: if the pair (a, b, c) is a solution to Fermat's equation for $n > 2$, then it could be shown that the elliptic curve $y^2 = x(x - a^n)(x + b^n)$ would have such unusual properties that it was unlikely to be modular, thus we can get a contradiction to the modularity theorem, therefore we can see that all elliptic curves are modular.

At the same time, some mathematicians worked on Fermat's last theorem on polynomials, which can be stated as follows:

Theorem 1.3 (Fermat's last theorem on polynomials)**.** *Suppose n is an integer and $n \geqslant 3$. Then the Diophantine equation*

$$f^n(x) + g^n(x) = h^n(x)$$

has no nonconstant pairwise coprime polynomial solutions in $\mathbb{C}[x]$.

While Fermat's Last Theorem on integers is extremely difficult to prove, the polynomials version is easy to solve. It dates back to 1851 when Liouville gave his proof, which involves integration. Nowadays, there are some easy and basic ways to prove Fermat's Last Theorem on polynomials. The easiest version may be the one using Mason-Stothers theorem.

Suppose $0 \neq f(x) \in \mathbb{C}[x]$, we denote

$$\pi(f) = \textit{the number of distinct roots of } f(x).$$

More specifically, we can write $f(x)$ as

$$f(x) = c\prod_{i=1}^{r}(x - c_i)^{m_i},$$

where $c, c_i \in \mathbb{C}, c_i \neq c_j, m_j \geqslant 1$ for $i \neq j \in [1, r]$. Then $\pi(f) = r$.

Theorem 1.4 (Mason-Stothers Theorem). *([6]) Suppose $f_1(x), f_2(x), f_3(x) \in \mathbb{C}[x]$ with $deg(f_i(x)) \geqslant 1, i = 1, 2, 3$. If $f_1(x) + f_2(x) = f_3(x)$, where $f_1(x), f_2(x), f_3(x)$ are pairwise coprime. Then*

$$max\{deg(f_1(x)), deg(f_2(x)), deg(f_3(x))\} \leqslant \pi(f_1 f_2 f_3) - 1.$$

This theorem can be proved by the basic properties of polynomials, including the divisible property and the degree of polynomials. The Fermat's Last Theorem on polynomials is not hard to prove using this theorem. We omit the proof here, which can be found in relevant books.

It is so interesting that Fermats Last Theorem (FLT) on integers is unbelievably difficult while its polynomial version is quite direct to prove. Therefore we wonder whether there are similar results for other algebraic objects. In the following, we will discuss the relative properties of other polynomials, such as multivariate polynomials.

The paper is organized as follows.

In Section 2 we discuss the FLT problem in a polynomial ring in one variable with the help of Mason-Stothers theorem over an algebraically closed field. In this paper, for a polynomial $f \in F[t]$, we always denote $f' = \frac{df}{dt}$.

Theorem 2.3 *Suppose $f_i \in F[t]$, $deg(f_i) \geqslant 1$ for $i = 1, 2, 3$, f_1, f_2, f_3 are pairwise coprime and $f_1 + f_2 = f_3$. If $f_2 f_3' - f_2' f_3 \neq 0$, then $max\{deg(f_1), deg(f_2), deg(f_3)\} \leqslant \pi(f_1 f_2 f_3) - 1$.*

Then we get

Theorem 2.4 *For any $n \geqslant 3$, the equation*

$$f_1^n + f_2^n = f_3^n$$

has no non-constant pairwise coprime solution (f_1, f_2, f_3) in $F[t]$ satisfying $n(f_i f_j' - f_i' f_j) \neq 0, i \neq j$.

In Section 3, we focus on the FLT problem in a polynomial ring with multiple variables to get

Theorem 3.3 *Let K be an integral domain with char $K = 0$, then there are no polynomials $f_1, f_2, f_3 \in K[x_1, x_2, \cdots, x_{m-1}, x_m]$ with $deg_{x_j}(f_i) \geqslant 1$ satisfying*

$$f_1^n + f_2^n = f_3^n,$$

where $j \in [1, m]$ and $n \geqslant 3$ is an integer.

As well as for some cases, FLT holds when *char K* is a prime, see **Proposition 3.5**. And then we figure out the solutions of the equation when FLT does not hold.

Theorem 3.7 *Assume that K is an integral domain with char $K = p$, p is a prime, $n \geqslant 3$ and $n = p^r$ for some $r \in \mathbb{N}$, then all non-constant solutions to the equation $f_1^n + f_2^n = f_3^n$ in $K[x_1, x_2, \cdots, x_{m-1}, x_m]$ are of the form $(f_1, f_2, a(f_1 + f_2))$, where $a \in K$ satisfying $a^n = 1$.*

In Section 4, we talk about the FLT problem in an ore extension or specially in a skew polynomial ring to obtain certain specific results.

And finally in Section 5, we raise questions of FLT, or more generally, of ABC problem in an Euclidean integral domain as our further goals.

§2 Problems about FLT on polynomials in one variable over algebraically closed field with arbitrary characteristic

In the first section, we show a proof of Fermat's Last Theorem of polynomials in one variable over the complex number field, which is a kind of algebraically closed field. Then we wonder what's the case for general algebraically closed field. As is known to all, the complex number field $\mathbb{C}$ has the characteristic zero, but for general algebraically closed field, it may have the characteristic p, where $p = 0$ or p is a prime. For the latter case, Mason-Stothers Theorem doesn't hold, so we will try to figure out when it is right.

Conjecture 2.1 (FLT of Polynomials in one variable over algebraically closed field)**.** *Let $n \geqslant 3$ be an integer. Then the equation*

$$f_1^n(x) + f_2^n(x) = f_3^n(x)$$

has no nonconstant pairwise coprime solutions in $F[x]$, where F is an algebraically closed field.

This conjecture in general is not true. So in the following we will discuss when it is true.

First of all, we can get for some cases the conjecture is true by generalizing the Mason-Stothers theorem to an algebraically closed field.

Let F be an algebraically closed field, and $f(t)$ be a non-zero polynomial in $F[t]$. Then $f(t)$ can be written as $f(t) = c\prod_{i=1}^{r}(t - c_i)^{m_i}$, as in the field $\mathbb{C}$ of complex numbers, where $c, c_i \in F$. Denote by $\pi(f)$ the number of distinct roots of $f(t)$, then $\pi(f) = r$. It is obvious that $\pi(fg) \leqslant \pi(f) + \pi(g)$ if $fg \neq 0$, and the equality holds if and only if $(f, g) = 1$. Here and in the following (f, g) represents the greatest monic common divisor of f and g. We denote f' as the derivative of f.

Lemma 2.2. *If $f(t) \in F[t]$ and $deg(f) \geqslant 1$, then $deg(f) \leqslant deg((f, f')) + \pi(f)$.*

Proof. Suppose

$$f(t) = c\prod_{i=1}^{r}(t - c_i)^{m_i}, c, c_i \in F.$$

When *char* $F = 0$,we can get that

$$\frac{f(t)}{(f(t), f'(t))} = c(t - c_1)(t - c_2)\cdots(t - c_r).$$

Then

$$deg(f) = deg((f, f')) + deg(c\prod_{i=1}^{r}(t - c_i)) = deg((f, f')) + \pi(f).$$

When *char* $F = p$, where p is a prime. If for any $m_i, p \nmid m_i$, then the case is the same as *char* $F = 0$. If there exist $m_{i_1}, m_{i_2}, \cdots, m_{i_k}$ such that $p \mid m_{i_s}, s = 1, 2, \cdots, k$, then we have $(t - c_{i_s})^{m_{i_s}} \mid f'(t)$,thus

$$\frac{f(t)}{(f(t), f'(t))} = \frac{c(t - c_1)(t - c_2)\cdots(t - c_r)}{(t - c_{i_1})\cdots(t - c_{i_k})}.$$

It follows that

$$deg(f) + k = deg((f, f')) + \pi(f),$$

namely

$$deg(f) = deg((f, f')) + \pi(f) - k < deg((f, f')) + \pi(f).$$

Therefore,

$$deg(f) \leqslant deg((f, f')) + \pi(f).$$

□

Theorem 2.3 (Mason-Stothers theorem on an algebraically closed field)**.** *Suppose* $f_i \in F[t]$, $deg(f_i) \geqslant 1$ *for* $i = 1, 2, 3$, f_1, f_2, f_3 *are pairwise coprime and* $f_1 + f_2 = f_3$. *If* $f_2 f_3' - f_2' f_3 \neq 0$, *then* $max\{deg(f_1), deg(f_2), deg(f_3)\} \leqslant \pi(f_1 f_2 f_3) - 1$.

Proof. It is easy to get that

$$(f_3, f_3') \mid (f_2 f_3' - f_2' f_3),\ (f_2, f_2') \mid (f_2 f_3' - f_2' f_3),\ (f_1, f_1') \mid (f_2 f_1' - f_2' f_1).$$

And $f_1 + f_2 = f_3$ implies that

$$f_2 f_3' - f_2' f_3 = f_2(f_1' + f_2') - f_2'(f_1 + f_2) = f_2 f_1' - f_2' f_1.$$

Thus $(f_1, f_1') \mid (f_2 f_3' - f_2' f_3)$. Since f_1, f_2, f_3 are pairwise coprime, we have $\prod_{i=1}^{3}(f_i, f_i') \mid (f_2 f_3' - f_2' f_3)$. Because $f_2 f_3' - f_2' f_3 \neq 0$, so by Lemma 2.2 we get

$$\begin{aligned}\sum_{i=1}^{3}(deg(f_i) - \pi(f_i)) &\leqslant \sum_{i=1}^{3} deg(f_i, f_i') = deg(\prod_{i=1}^{3}(f_i, f_i')) \\ &\leqslant deg(f_2 f_3' - f_2' f_3) \leqslant deg(f_2) + deg(f_3) - 1\end{aligned}$$

It follows that

$$deg(f_1) \leqslant \sum_{i=1}^{3} \pi(f_i) - 1 = \pi(f_1 f_2 f_3) - 1.$$

Moreover, since $f_1 + f_2 = f_3$ and $f_2 f_3' - f_2' f_3 \neq 0$, we also have $f_1 f_3' - f_1' f_3 = (f_3 - f_2) f_3' - (f_3' - f_2') f_3 = f_2' f_3 - f_2 f_3' \neq 0$. Then similarly, we get

$$deg(f_2) \leqslant \pi(f_1 f_2 f_3) - 1.$$

Because $f_1 + f_2 = f_3$, $deg(f_3) \leqslant max\{deg(f_1), deg_2\} \leqslant \pi(f_1 f_2 f_3) - 1$. Thus in summary, we get

$$max\{deg(f_1), deg(f_2), deg(f_3)\} \leqslant \pi(f_1 f_2 f_3) - 1.$$

□

Note that when *char* $F = 0$, it can be verified that $f_2 f_3' - f_2' f_3$ is nonzero because f_2 and f_3 are coprime. Then in this case, the Theorem 2.3 becomes usual Mason-Stothers Theorem.

By this theorem, we get that the corollary below

Corollary 2.4 (FLT on polynomials for a special case)**.** *For any* $n \geqslant 3$, *the equation*

$$f_1^n + f_2^n = f_3^n$$

has no non-constant pairwise coprime solution (f_1, f_2, f_3) *in* $F[t]$ *satisfying*

$$n(f_i f_j' - f_i' f_j) \neq 0, i \neq j.$$

Proof. By Theorem 2.3, we can get that if

$${f_2}^n (f_3^n)' - ({f_2}^n)' f_3^n = n f_2^{n-1} f_3^{n-1}(f_2 f_3' - f_2' f_3) \neq 0,$$

then

$$ndeg(f_1) = deg(f_1^n) \leqslant \pi(f_1^n f_2^n f_3^n) - 1 = \pi(f_1 f_2 f_3) - 1 \leqslant deg(f_1) + deg(f_2) + deg(f_3) - 1.$$

Similarly we can replace f_1 by f_2 and f_3 respectively on the left, then we have

$$ndeg(f_i) \leqslant deg(f_1) + deg(f_2) + deg(f_3) - 1, i = 1, 2, 3.$$

Add them together we get

$$n\sum_{i=1}^{n} deg(f_i) \leqslant 3\sum_{i=1}^{n} deg(f_i) - 3.$$

It contradicts to the fact $n \geqslant 3$. □

As we mentioned before, $n(f_i f_j' - f_i' f_j) \neq 0$, $i \neq j$ is ensured by the pairwise coprime condition when F is an algebraically closed field with *char* $F = 0$. So in this case FLT holds.

Corollary 2.5. *Suppose F is an algebraically closed field with char $F = 0$ and $n \geqslant 3$. Then the equation*

$$f_1^n + f_2^n = f_3^n$$

has no non-constant pairwise coprime solution (f_1, f_2, f_3) in $F[t]$.

This corollary is essentially Theorem 1.3.

Now we have proved that the Fermat's last theorem holds over an algebraically closed field under the condition $n(f_i f_j' - f_i' f_j) \neq 0$, $i \neq j$. Then what is the case when $n(f_i f_j' - f_i' f_j) = 0$? In this case FLT does not hold in general, however, when it holds is still not clear to us.

§3 Problems about FLT on multivariate polynomials

In the following, we wonder what is the case for polynomials in m variables. We use another method to deal with the conjecture for polynomials in m variables. The main tool we adopt is the degree function of polynomials.

Problem 3.1 (FLT on polynomials in m variables)**.** *Let $n \geqslant 3$ be an integer. Does the equation*

$$f_1^n(x_1, x_2, \cdots, x_m) + f_2^n(x_1, x_2, \cdots, x_m) = f_3^n(x_1, x_2, \cdots, x_m)$$

have nonconstant pairwise coprime solutions in $K[x_1, x_2, \cdots, x_m]$ for an integral domain K?

It is not true in general. So we will show in Theorem 3.7 what the solutions are in a certain situation and also present some cases where the conjecture holds in Theorem 3.3 as well as Proposition 3.5.

3.1 For the case when characteristic is 0

Lemma 3.2. *Let K be an integral domain with char $K = 0$, then there are no polynomials $f_1, f_2, f_3 \in K[x]$ with $deg(f_i) \geqslant 1$ satisfying*

$$f_1^n + f_2^n = f_3^n,$$

where $n \geqslant 3$ is an integer.

Proof. Since K is an integral domain, we can embed K in its field of fractions QK. Moreover, QK can be further embedded in an algebraically closed field $\overline{QK}$. Then we have the inclusion $K \hookrightarrow QK \hookrightarrow \overline{QK}$. We have $char\ \overline{QK} = char\ K = 0$ and by Proposition 2.5 there are no polynomials $f_1, f_2, f_3 \in \overline{QR}[x]$ with $deg(f_i) \geqslant 1$ satisfying $f_1^n + f_2^n = f_3^n (n \geqslant 3)$. Therefore there exist no polynomials $f_1, f_2, f_3 \in K[x]$ with $deg(f_i) \geqslant 1$ satisfying

$$f_1^n + f_2^n = f_3^n (n \geqslant 3).$$

□

Theorem 3.3. *Let K be an integral domain with $char\ K = 0$, then there are no polynomials $f_1, f_2, f_3 \in K[x_1, x_2, \cdots, x_m]$ with $deg_{x_j}(f_i) \geqslant 1$ satisfying*

$$f_1^n + f_2^n = f_3^n,$$

where $j \in [1, m]$ and $n \geqslant 3$ is an integer.

Proof. Without loss of generality we assume $j = m$. Denote $R = K[x_1, x_2, \cdots, x_{m-1}]$, then we can get that R is an integral domain with $char\ R = char\ K = 0$ and

$$K[x_1, x_2, \cdots, x_m] = R[x_m].$$

Then by Lemma 3.2 we can get the conclusion. □

In particular, FLT holds when K is a field with $char\ K = 0$, which is a generalization of Theorem 1.3 in multiple variables, that is,

Corollary 3.4. *Let K be a field with $char\ K = 0$, then there are no polynomials $f_1, f_2, f_3 \in K[x_1, x_2, \cdots, x_m]$ with $deg_{x_j}(f_i) \geqslant 1$ satisfying*

$$f_1^n + f_2^n = f_3^n,$$

where $i = 1, 2, 3, j \in [1, m]$ and $n \geqslant 3$ is an integer.

3.2 For the case when the characteristic is a prime

When $char\ K = p$ is a prime, we also get some results in the following special cases.

Proposition 3.5. *Let K be an integral domain with $char\ K = p$, where p is a prime, $n \geqslant 3$ is an integer and there is no $r \in \mathbb{N}$ such that $n = p^r$. Then there are no non-constant solution $f_1, f_2, f_3 \in K[x_1, x_2, \cdots, x_m]$ of the equation*

$$f_1^n + f_2^n = f_3^n$$

satisfying one of the following conditions:

(a) $f_1 \in K[x_1, x_2, \cdots, x_{m-1}]$ with $deg_{x_m}(f_i) \geqslant 1$ for $i = 2, 3$;

(b) $deg_{x_m}(f_i) \geqslant 1$ for $i = 1, 2, 3$, $deg_{x_m}(f_1) \neq deg_{x_m}(f_2)$ and f_1, f_2 are both irreducible;

(c) $deg_{x_m}(f_i) \geqslant 1$ for $i = 1, 2, 3$, $deg_{x_m}(f_1) = deg_{x_m}(f_2)$ and $deg_{x_m}(f_3 - f_2) \neq deg_{x_m}(f_1)$.

Proof. Let $R = K[x_1, x_2, \cdots, x_{m-1}]$, then

$$K[x_1, x_2, \cdots, x_m] = K[x_1, x_2, \cdots, x_{m-1}][x_m] = R[x_m].$$

(a) Suppose there are polynomials $f_1 \in R, f_2, f_3 \in R[x_m]$ with $deg(f_i) \geqslant 1, i = 2, 3$ such that $f_1^n + f_2^n = f_3^n (n \geqslant 3)$, then

$$f_1^n = f_3^n - f_2^n = (f_3 - f_2)({f_3}^{n-1} + {f_3}^{n-2} f_2 + \cdots + {f_2}^{n-1}).$$

It follows that $(f_3 - f_2) \mid f_1^n$. Denote $a = f_3 - f_2 \neq 0$, then

$$f_1^n + f_2^n = f_3^n = (f_2 + a)^n = f_2^n + \binom{n}{1} a f_2^{n-1} + \cdots + \binom{n}{n-1} a^{n-1} f_2 + a^n.$$

So

$$f_1^n = \binom{n}{1} a {f_2}^{n-1} + \cdots + \binom{n}{n-1} a^{n-1} f_2 + a^n.$$

Since $a \neq 0$ and $n \neq p^r$ for any $r \in \mathbb{N}$, there is $i \in [1, n-1]$ such that $\binom{n}{i} \neq 0$. It follows that

$$deg_{x_m}(\binom{n}{1} a {f_2}^{n-1} + \cdots + \binom{n}{n-1} a^{n-1} f_2 + a^n) \geqslant 1,$$

which contradicts to the assumption that $deg_{x_m}(f_1) = 0$.

(b) Without loss of generality, assume $deg_{x_m}(f_1) > deg_{x_m}(f_2)$.

Suppose that there are polynomials $f_1, f_2, f_3 \in K[x_1, x_2, \cdots, x_m]$ satisfying $deg_{x_m}(f_i) \geqslant 1$ for $i = 1, 2, 3$, $deg_{x_m}(f_1) \neq deg_{x_m}(f_2)$, f_1, f_2 are both irreducible such that $f_1^n + f_2^n = f_3^n$. Then we have

$$f_1^n = f_3^n - f_2^n = (f_3 - f_2)({f_3}^{n-1} + {f_3}^{n-2} f_2 + \cdots + {f_2}^{n-1}).$$

Therefore, $(f_3 - f_2) \mid f_1^n$. Denote $g = f_3 - f_2 \neq 0$. Because $deg_{x_m}(f_1) > deg_{x_m}(f_2)$, so $deg_{x_m}(g) > 0$. Hence $g = {f_1}^k$ for some positive integer k since f_1 is irreducible.

If $k = 1$, then $f_1 + f_2 = f_3$, which induces

$$f_1^n + f_2^n = (f_1 + f_2)^n = f_1^n + \binom{n}{1} f_2 {f_1}^{n-1} + \cdots + \binom{n}{n-1} {f_2}^{n-1} f_1 + f_2^n.$$

Therefore,

$$\binom{n}{1} f_2 {f_1}^{n-1} + \cdots + \binom{n}{n-1} {f_2}^{n-1} f_1 = 0.$$

But $deg_{x_m}(f_1) > deg_{x_m}(f_2)$, so

$$deg_{x_m}(\binom{n}{1} f_2 {f_1}^{n-1} + \cdots + \binom{n}{n-1} {f_2}^{n-1} f_1) = deg_{x_m}(\binom{n}{i} f_2^i {f_1}^{n-i}) > 0,$$

where i is the minimal positive integer satisfying $\binom{n}{i} \neq 0$ (the existence of such i is ensured by the assumption that there is no $r \in \mathbb{N}$ such that $n = p^r$). This leads to a contradiction.

Otherwise if $k \geqslant 2$, we can get that

$${f_1}^{n-k} = {f_3}^{n-1} + {f_3}^{n-2} f_2 + \cdots + {f_2}^{n-1}.$$

And $deg_{x_m}(f_3) = deg_{x_m}(f_1) > deg_{x_m}(f_2)$ since $f_1^n + f_2^n = f_3^n$. It follows that

$$deg_{x_m}({f_3}^{n-1} + {f_3}^{n-2} f_2 + \cdots + {f_2}^{n-1}) = (n-1) deg(f_3) > (n-k) deg(f_1) = deg({f_1}^{n-k}),$$

which also leads to a contradiction.

(c) Assume that there are polynomials $f_1, f_2, f_3 \in K[x_1, x_2, \cdots, x_m]$ satisfying $deg_{x_m}(f_i) \geqslant 1$ for $i = 1, 2, 3$, $deg_{x_m}(f_1) = deg_{x_m}(f_2)$, $deg_{x_m}(f_3 - f_2) \neq deg_{x_m}(f_1)$ such that $f_1^n + f_2^n = f_3^n$. Then we have

$$f_1^n = f_3^n - f_2^n = (f_3 - f_2)({f_3}^{n-1} + {f_3}^{n-2} f_2 + \cdots + {f_2}^{n-1}).$$

Therefore, $(f_3 - f_2) \mid f_1^n$. Denote $g = f_3 - f_2$.

If $deg_{x_m}(g) < deg_{x_m}(f_1) = deg_{x_m}(f_2)$, since

$$f_1^n + f_2^n = f_3^n = (g + f_2)^n = g^n + \binom{n}{1} f_2 g^{n-1} + \cdots + \binom{n}{n-1} f_2^{n-1} g + f_2^n,$$

then

$$f_1^n = g^n + \binom{n}{1} f_2 g^{n-1} + \cdots + \binom{n}{n-1} f_2^{n-1} g.$$

Thus

$$deg_{x_m}(f_1^n) = deg_{x_m}(g^n + \binom{n}{1} f_2 g^{n-1} + \cdots + \binom{n}{n-1} f_2^{n-1} g) = deg_{x_m}(\binom{n}{n-i} f_2^{n-i} g^i),$$

where i is the minimal positive integer satisfying $\binom{n}{n-i} \neq 0$ (the existence of such i is ensured by the assumption that there is no $r \in \mathbb{N}$ such that $n = p^r$). So

$$ndeg_{x_m}(f_1) = (n-i)deg_{x_m}(f_2) + ideg_{x_m}(g) < ndeg_{x_m}(f_1),$$

which is impossible.

If $deg_{x_m}(g) > deg_{x_m}(f_1)$, then we have $deg_{x_m}(f_3) > deg_{x_m}(f_1) = deg_{x_m}(f_2)$. On the other hand, however, because $f_1^n + f_2^n = f_3^n$, we can get that

$$deg_{x_m}(f_3^n) = deg_{x_m}(f_1^n + f_2^n) \leqslant max\{deg_{x_m}(f_1^n), deg_{x_m}(f_2^n)\} = deg_{x_m}(f_1^n),$$

which leads to a contradiction. □

In the proposition above, if the condition $deg_{x_m}(f_3 - f_2) \neq deg_{x_m}(f_1)$ is replaced by $deg_{x_m}(g) = deg_{x_m}(f_1) = deg_{x_m}(f_2)$, then we can get $g = af_1$ when f_1 is irreducible, where $a \in K$ is a unit, since $g \mid f_1$, i.e, $f_3 = af_1 + f_2$. Therefore, in this case if the equation $f_1^n + f_2^n = f_3^n$ has a solution, say (f_1, f_2, f_3), then either f_1 is reducible or there is a unit $a \in K$ satisfying $af_1 + f_2 = f_3$.

In particular, the above results hold for polynomial rings with one variable. In the second section, we discuss about the FLT problem when $f_i f_j' - f_i' f_j \neq 0$ for $i \neq j$ with the help of Mason-Stothers Theorem. While in this section, we use the degree function to get more results.

In the above discussion, we mainly focus on cases where $char\ K = 0$ or $char\ K = p$ and there is no $r \in \mathbb{N}$ such that $n = p^r$. However, FLT does not hold when $char\ K = p$ and $n = p^r$ for some $r \in \mathbb{N}$. In this case, it can be checked that $\binom{n}{1} f_1 {f_2}^{n-1} + \cdots + \binom{n}{n-1} f_1^{n-1} f_2 = 0$. Therefore, $f_1^n + f_2^n = (f_1 + f_2)^n$, which means that $(f_1, f_2, f_1 + f_2)$ is a solution to the equation $f_1^n + f_2^n = f_3^n$ for any $f_1, f_2 \in K[x_1, \cdots, x_m]$. So in the following result, we want to figure out all possible solutions in this specific case.

Lemma 3.6. *Assume $f, g \in K[x]$ are two polynomials and K is an algebraically closed field. If there is $n \in \mathbb{Z}_{>0}$ such that $f^n = g^n$, then $f = ag$ for some $a \in K$ satisfying $a^n = 1$.*

Proof. Suppose $f = a_1(x - x_1)^{k_1}(x - x_2)^{k_2} \cdots (x - x_s)^{k_s}$, where $a_1, x_1, \cdots, x_s \in K$, and $k_1, \cdots, k_s$ are positive integers. If $f^n = g^n$, then $f \mid g^n$ and $g \mid f^n$, hence the roots of f are the same with those of g. Therefore we can assume that $g = a_2(x - x_1)^{p_1}(x - x_2)^{p_2} \cdots (x - x_s)^{p_s}$. By $f^n = g^n$ we can get $p_i = k_i$ for any $i \in [1, s]$ and $a_1^n = a_2^n$. So $f = ag$, where $a = \frac{a_2}{a_1}$. □

As we said before, an integral domain can be naturally embedded in an algebraically closed field, so in the above lemma we can only assume K is an integral domain. Hence by similar way, we can get the same conclusion for polynomials in m variables.

Theorem 3.7. *Assume that K is an integral domain with char $K = p$, p is a prime, $n \geqslant 3$ and $n = p^r$ for some $r \in \mathbb{N}$, then all non-constant solutions to the equation $f_1^n + f_2^n = f_3^n$ in $K[x_1, x_2, \cdots, x_{m-1}, x_m]$ are of the form $(f_1, f_2, a(f_1 + f_2))$, where $a \in K$ satisfying $a^n = 1$.*

Proof. First we can prove all the non-constant triples $(f_1, f_2, a(f_1 + f_2))$ are solutions to the equation $f_1^n + f_2^n = f_3^n$, where $f_1, f_2 \in K[x_1, x_2, \cdots, x_{m-1}, x_m]$ and $a \in K$ satisfying $a^n = 1$. In fact,

$$a^n(f_1 + f_2)^n = f_2^n + \binom{n}{1} f_1 {f_2}^{n-1} + \cdots + \binom{n}{n-1} f_1^{n-1} f_2 + f_1^n = f_1^n + f_2^n$$

since *char* $K = p$, p is a prime, and $n = p^r$ for some $r \in \mathbb{N}$.

Next we prove all non-constant solutions to the equation $f_1^n + f_2^n = f_3^n$ in $K[x_1, x_2, \cdots, x_{m-1}, x_m]$ satisfying the relation $f_3 = a(f_2 + f_1)$, where $a \in K$ satisfying $a^n = 1$. Since *char* $K = p$, p is a prime, and $n = p^r$ for some $r \in \mathbb{N}$, then

$$\binom{n}{1} f_1 {f_2}^{n-1} + \cdots + \binom{n}{n-1} f_1^{n-1} f_2 = 0.$$

So if $f_1^n + f_2^n = f_3^n$, then $f_3^n = (f_1 + f_2)^n$. Therefore, by lemma 3.6, $f_3 = a(f_1 + f_2)$, where $a \in K$ satisfying $a^n = 1$. □

§4 Problems about FLT on skew polynomial rings

Skew polynomial rings are one of the most active and important study objects in noncommutative algebra. Noether and Schmeidler are the first to consider this kind of rings and it is later systematically studied by Ore in 1933 both in the context of differential equations and as operators on finite fields. Skew polynomial rings are so important since they are used to characterize various kinds of radicals such as Jacobson radical, Baer radical, and Krull dimensions of such rings. They are also applied to constructing finite dimensional algebras as well as classifying all valuations of these algebras. Moreover, they are also applied in solving ordinary differential equations, control theory and Coding theory.

In this section, we would like to discuss FLT problem on skew polynomial rings.

Definition 4.1. Suppose R is an associative ring with identity 1, α is an nonzero endomorphism of R. We call the map $\delta : R \to R$ an α-derivation on R if δ satisfies the relations below:

$$\delta(a + b) = \delta(a) + \delta(b), \delta(ab) = \delta(a)b + \alpha(a)\delta(b),$$

in which $a, b \in R$.

Definition 4.2. Let R be an associative ring with identity 1, α is an nonzero endomorphism of R and δ is an α-derivation on R. The ring

$$R[x; \alpha, \delta] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in R, n \in \mathbb{N}\}$$

is called an **Ore extension** if the addition is defined as usual and the multiplication is defined subject to the relation

$$xr = \alpha(r)x + \delta(r),$$

for all $r \in R$.

If $\delta = 0$, then $R[x;\alpha] = R[x;\alpha,0]$ is called a **skew polynomial ring**.

If $\alpha = Id_R$ the identity map, then $R[x;\delta] = R[x;Id_R,\delta]$ is called a **differential operator ring**.

If $\delta = 0$ and α is the identity map in $R[x;\alpha,\delta]$, then the relation $xr = \alpha(r)x + \delta(r)$ reduces to $xr = rx$. In this case the Ore extension degenerates to a general polynomial ring. In this section, by monic polynomial we mean the summand monomial of this polynomial with largest x-degree having coefficient 1 when it is represented in the form rx^k for $r \in R, k \in \mathbb{N}$.

Lemma 4.3. *Assume that R is an associative ring with identity 1, $R[x;\alpha,\delta]$ is an ore extension satisfying $2x \neq 0$ and $n \geq 3$ is an integer. If $f_1^n + f_2^n = f_3^n$ holds for monic polynomials $f_i \in R[x;\alpha,\delta]$ for $i = 1,2,3$, then we can get $deg(f_i) = deg(f_3) > deg(f_j)$, where $\{i,j\} = \{1,2\}$.*

Proof. If $deg(f_1) = deg(f_2)$, then because $x \neq 0$ and $f_1^n + f_2^n = f_3^n$, f_3 can not be a monic polynomial. Hence there must be $deg(f_i) = deg(f_3) > deg(f_j)$, where $\{i,j\} = \{1,2\}$. □

Lemma 4.4 (Algebra of differential operators)**.** *([5]) Suppose R is an algebra over a field K and δ is a derivation of R. Then in the algebra $R[x,\delta]$ of differential operators associated to δ, for any integer $n > 0$ and any element $r \in R$ we have*

$$x^n r = \sum_{k=0}^{n} \binom{n}{k} \delta^k(r) x^{n-k}.$$

Definition 4.5. We call a solution (f_1, f_2, f_3) to the Diophantine equation $f_1^n + f_2^n = f_3^n$ in $R[x;\alpha,\delta]$ **trivial** if either $f_1^n = 0$ or $f_2^n = 0$.

Proposition 4.6. *Suppose R is an integral domain with identity 1, char $R = 0$, $n \geqslant 3$ an integer. Then, the Diophantine equation $f_1^n + f_2^n = f_3^n$ has only trivial solutions for $f_1, f_2, f_3 \in R[x;\alpha,\delta]$ satisfying f_i is a monic polynomial for $i = 1,2,3$ if one of the following conditions is satisfied:*

(i) $\delta = 0$ and $\alpha(r) = mr$ for any $r \in R$ and some $m \neq 2,3 \in R$;

(ii) $\alpha = Id_R$.

Proof. (i) Suppose (f_1, f_2, f_3) is a solution to the Diophantine equation

$$f_1^n + f_2^n = f_3^n$$

where $f_i \in R[x;\alpha]$ is a monic polynomial for $i = 1,2,3$. Then by Lemma 4.3, without loss of generality we have

$$deg(f_1) = deg(f_3) > deg(f_2).$$

Assume

$$\begin{aligned} f_1 &= x^t + a_1x^{t-1} + a_2x^{t-2} + \cdots + a_{t-1}x + a_t, \\ f_2 &= x^s + c_1x^{s-1} + c_2x^{s-2} + \cdots + c_{s-1}x + c_t, \\ f_3 &= x^t + b_1x^{t-1} + b_2x^{t-2} + \cdots + b_{t-1}x + b_t, \end{aligned}$$

where $a_i, b_i, c_i \in R$. Then,

$$\begin{aligned} &(x^t + a_1x^{t-1} + a_2x^{t-2} + \cdots + a_{t-1}x + a_t)^n + (x^s + c_1x^{s-1} + c_2x^{s-2} + \cdots + c_{s-1}x + c_t)^n \\ &= (x^t + b_1x^{t-1} + b_2x^{t-2} + \cdots + b_{t-1}x + b_t)^n. \end{aligned}$$

We can compute the coefficient of x^{nt-1} in f_1^n as follows

$$\begin{aligned}&a_1x^{t-1}(x^t)^{n-1}+x^ta_1x^{t-1}(x^t)^{n-2}+\cdots+(x^t)^{n-1}a_1x^{t-1}\\=&a_1x^{nt-1}+m^ta_1x^{nt-1}+\cdots+m^{nt-t}a_1x^{nt-1}\\=&(1+m^t+m^{2t}+\cdots+m^{nt-t})a_1x^{nt-1}.\end{aligned}$$

In the same way, we can get the coefficient of x^{nt-1} in f_3^n, which is $(1+m^t+m^{2t}+\cdots+m^{nt-t})b_1$, then it follows that

$$(1+m^t+m^{2t}+\cdots+m^{nt-t})a_1x^{nt-1}=(1+m^t+m^{2t}+\cdots+m^{nt-t})b_1x^{nt-1}.$$

Since R is an integral domain with $char\ R=0$, we have $a_1x=b_1x$.

And in the same way we can get $a_2=b_2$. In fact, we just need to compute the coefficients of x^{nt-2} in f_1^n and f_3^n respectively. By comparing the coefficients we have

$$(F_1(m)a_1^2+F_2(m)a_2)x^{nt-2}=(F_1(m)b_1^2+F_2(m)b_2)x^{nt-2},$$

where $F_1(m),F_2(m)$ are polynomials of m with positive coefficients. Since $a_1x=b_1x$, it follows that $F_2(m)a_2x=F_2(m)b_2x$. Because R is an integral domain with $char\ R=0$, so $a_2x=b_2x$. In this way, we can get $a_ix=b_ix$ for all $i=1,2,\cdots,t$ successively. Therefore, $f_1=f_3$, and $(f_2)^n=0$, i.e, (f_1,f_2,f_3) is a trivial solution.

(ii) Consider $R[x;Id_R,\delta]$. Suppose (f_1,f_2,f_3) is a solution to the Diophantine equation

$$f_1^n+f_2^n=f_3^n$$

where $f_i\in R[x;id_R,\delta]$ is a monic polynomial for $i=1,2,3$. Then by Lemma 4.3, without loss of generality we have

$$deg(f_1)=deg(f_3)>deg(f_2).$$

Denote

$$\begin{aligned}f_1&=x^t+a_1x^{t-1}+a_2x^{t-2}+\cdots+a_{t-1}x+a_t,\\f_2&=x^s+c_1x^{s-1}+c_2x^{s-2}+\cdots+c_{s-1}x+c_t,\\f_3&=x^t+b_1x^{t-1}+b_2x^{t-2}+\cdots+b_{t-1}x+b_t,\end{aligned}$$

where $a_i,b_i,c\in R$. Then,

$$\begin{aligned}&(x^t+a_1x^{t-1}+a_2x^{t-2}+\cdots+a_{t-1}x+a_t)^n+(x^s+c_1x^{s-1}+c_2x^{s-2}+\cdots+c_{s-1}x+c_t)^n\\&=(x^t+b_1x^{t-1}+b_2x^{t-2}+\cdots+b_{t-1}x+b_t)^n.\end{aligned}$$

We can compute the coefficient of x^{nt-1} in f_1^n as follows

$$\begin{aligned}&a_1x^{t-1}(x^t)^{n-1}+x^t\cdot a_1x^{t-1}\cdot(x^t)^{n-2}+\cdots+(x^t)^{n-1}\cdot a_1x^{t-1}\\&=a_1x^{nt-1}+\sum_{k=0}^{t}\binom{t}{k}\delta^k(a_1)x^{nt-1-k}+\sum_{k=0}^{2t}\binom{2t}{k}\delta^k(a_1)x^{nt-1-k}+\cdots\\&+\sum_{k=0}^{(n-1)t}\binom{(n-1)t}{k}\delta^k(a_1)x^{nt-1-k}.\end{aligned}$$

We first compute the coefficient of x^{nt-1}. It equals

$$(1+\binom{t}{0}+\binom{2t}{0}+\cdots+\binom{(n-1)t}{0})a_1=na_1,$$

Thus by comparing the coefficients in both sides we get $na_1=nb_1$, and then $a_1=b_1$ since R is an integral domain with $char\ R=0$. And in the same way we can get $a_2=b_2$. In fact, we can

compute the coefficients of x^{nt-2} in f_1^n and f_3^n respectively as

$$\binom{n}{2}t\delta(a_1)+\binom{n}{2}a_1^2+na_2=\binom{n}{2}t\delta(b_1)+\binom{n}{2}b_1^2+nb_2.$$

Since $a_1=b_1$, it follows that $na_2=nb_2$. Then $a_2=b_2$. In this way, we can get $a_i=b_i$ for all $i=1,2,\cdots,t$ successively. Therefore, $f_1=f_3$, and $c^n=0$, i.e, (f_1,f_2,f_3) is a trivial solution. □

In Proposition 4.6, we talk about the case where $\alpha(r)=mr$. We can similarly define a relation $yx=qxy$ in $K\langle x,y\rangle$ over a field K. This leads to the following definition of the quantum planes.

Definition 4.7. We call the quotient algebra $K_q[x,y]=K\langle x,y\rangle/I_q$ the quantum plane, where I_q is the two-sided ideal generated by the element $yx-qxy$.

In the definition above, when $q=1$, we get the usual commutative relation $yx=xy$, which corresponds to classical plane geometry; when $q\neq 1$, the algebra $K_q[x,y]$ is non-commutative, which corresponds to the quantum plane.

Lemma 4.8. *([5]) Suppose α is the automorphism of the polynomial ring $K[x]$ determined by $\alpha(x)=qx$, then the algebra $K_q[x,y]$ is isomorphic to the Ore extension $K[x][y;\alpha,0]$.*

According to the above lemma, we can regard a quantum plane $K_q[x,y]$ as a skew polynomial ring. Thus the results about skew polynomial rings naturally hold for quantum planes. So we state the following result without proof.

Corollary 4.9. *Suppose $K_q[x,y]$ is a quantum plane with char $K=0$ and $n\geqslant 3$ is an integer. Then the Diophantine equation $f_1^n+f_2^n=f_3^n$ has only trivial solutions for monic polynomials in $k_q[x,y]$ satisfying $deg_y(f_i)\geqslant 1$ for $i=1,3$ and $f_2\in k[x]$.*

Similarly we can induce the results to the algebra $M_q(2)$, whose definition is as follows.

Definition 4.10. *([5])* The algebra $M_q(2)$ is the quotient of the free algebra $K[a,b,c,d]$ by the two-sided ideal J_q generated by the six relations below

$$\begin{aligned} ba&=qab, \quad & db&=qbd,\\ ca&=qac, \quad & dc&=qcd,\\ bc&=cb, \quad & ad-da&=(q^{-1}-q)bc. \end{aligned}$$

We have

$$A_0=K\subset A_1\subset A_2\subset A_3\subset A_4=M_q(2),$$

where

$$A_1=K[a],A_2=K[a,b]/(ba-qab),A_3=K[a,b,c]/(ba-qab,ca-qac,cb-bc).$$

Then we can get some basic results for $A_1,A_2,A_3,A_4=M_q(2)$.

Lemma 4.11. *([5], Lemma IV.4.2) There is an isomorphism between A_2 and the Ore extension $A_1[b,\alpha_1,0]$, where α_1 is the automorphism of A_1 determined by $\alpha_1(a)=qa$.*

Lemma 4.12. *([5], Lemma IV.4.3) The algebra A_3 is isomorphic to the algebra $A_2[c;\alpha_2,0]$, where α_2 is the automorphism of A_2 determined by $\alpha_2(a)=qa$, and $\alpha_2(b)=b$.*

Lemma 4.13. *([5], Lemma IV.4.5) The algebra $A_4=M_q(2)$ is isomorphic to the Ore extension $A_3[d;\alpha_3,\delta]$, where α_3 is the automorphism of A_3 determined by $\alpha_3(a)=a,\alpha_3(b)=qb,\alpha_3(c)=qc$, and δ is an endomorphism of A_3 on the basis $\{a^ib^jc^k\}_{i,j,k\geqslant 0}$ by $\delta(b^jc^k)=0$ and*

$$\delta(a^ib^jc^k)=(q-q^{-1})\frac{1-q^{2i}}{1-q^2}a^{i-1}b^{j+1}c^{k+1}.$$

Thus we have the following corollary.

Corollary 4.14. *Suppose A_2 is the algebra defined as above. If char $K=0$ and $n\geqslant 3$ is an integer, then the Diophantine equation $f_1^n+f_2^n=f_3^n$ has only trivial solutions for monic polynomials in A_2 satisfying $deg_b(f_i)\geqslant 1$ for $i=1,3$ and $f_2\in A_1$.*

And since $A_3\cong A_2[c;\alpha_2,0]$, we can get the analogous result as above.

When R is an integral domain with *char* $R=p$ a prime, if $p\nmid k$ for any $k=2,3,\cdots,n$, by the similar discussion, we can prove an analogous result.

Proposition 4.15. *Suppose R is an integral domain with identity 1, char $R=p$ a prime and $R[x;id_R,\delta]$ is a differential operator ring. If $p\nmid k$ for any $k=2,3,\cdots,n$, then the Diophantine equation $f_1^n+f_2^n=f_3^n$ has only trivial solutions for monic polynomials in $R[x;id_R,\delta]$ satisfying $deg(f_i)\geqslant 1$ for $i=1,3$ and $f_2\in R$.*

§5 Some discussion about FLT and ABC Conjecture on Euclidean domain

As we know, the ring of polynomials over a field is a special case of Euclidean domain, thus we wonder how about the FLT problem in an Euclidean domain. We first give the definitions of degree function and Euclidean domain.

Definition 5.1. A degree function is a map $deg: D-\{0\}\to\mathbb{R}^+\cup\{0\}$ satisfying the following two properties:

(i) deg converts mutiplication to addition, namely, $deg(ab)=deg(a)+deg(b)$;

(ii) deg detects the unit of the integral domain, namely, $deg(a)=0$ if and only if a is a unit.

As two easy examples, we consider the ring of integers $\mathbb{Z}$, and the ring of polynomials $F[x]$, where F is a field. It's easy to check that $deg(a)=log(|a|)$ in $\mathbb{Z}$ and the ordinary degree function in $F[t]$ satisfy the above two conditions, thus they are both degree functions.

Definition 5.2. An integral domain D with degree function is called a Euclidean integral domain if it satisfies any one of the following two conditions for all $a,b\in D-\{0\}$:

(i) $a=bq$ for some q, namely b divides a;

(ii) $a=bq+r$ with $deg(r)<deg(b)$, where r is the remainder.

It is obvious to see, the ring of integers $\mathbb{Z}$, and the ring of polynomials $F[x]$ we mentioned above are Euclidean domain.

Conjecture 5.3 (FLT on Euclidean domain). *Suppose R is a Euclidean domain. Then there are no $a_1, a_2, a_3 \in R$ with $deg(a_i) > 0$ such that*

$$a_1^n + a_2^n = a_3^n,$$

where $n \geqslant 3$ is an integer.

This conjecture is not true in general, since the ring of polynomials over a field is also a Euclidean domain and the conjecture is not true in this case as we explained in the second section. But what we care about is that when the conjecture is true and when not.

Conjecture 5.4 (ABC Conjecture on Euclidean domain). *Suppose R is a Euclidean domain and φ is a function of R. Given $\varepsilon > 0$, there exists $C(\varepsilon) > 0$, such that for any non-zero relatively coprime elements $a, b, c \in R$ with $a + b = c$, we have $max\{\varphi(a), \varphi(b), \varphi(c)\} \leqslant C(\varepsilon)N_0(abc)$, where $N_0(m) = \varphi(\prod_{p|m} p)$ is the image of the product of the prime factors of m with mutiplicity 1 under the function φ.*

Declarations

Conflict of interest The authors declare no conflict of interest.

References

[1] H Cohen. *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.

[2] H M Edwards. *Fermats Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Graduate Texts in Mathematics 50, Spinger-Verlag, New York, 1977.

[3] A Granville, J Thomas. *Its As Easy As abc*, Tucker, 2002.

[4] K R Goodearl, R B Warfield. *An Introduction to Noncommutative Noetherian Rings*, Cambridge University Press, London Mathematical Society Student Texts 61 (Second Edition), 2004.

[5] C Kassel. *Quantum groups*, Graduate Texts in Mathematics 155, Spinger-Verlag, New York, 1995.

[6] S Lang. *Algebra*, Graduate Texts in Mathematics 211, Spinger-Verlag, New York, 2002.

[7] P Ribenboim. *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[8] P Ribenboim. *Fermat's Last Theorem for amateurs*, Springer-Verlag, 2000.

[9] S Singh. *Fermat's Last Theorem*, Fourth Estate Ltd, 1997.

[1]School of Mathematical Sciences, Zhejiang University, Hangzhou 310058, China.
Emails: 11635015@zju.edu.cn, fangli@zju.edu.cn.
[2]Henan Experimental High School, Zhengzhou 450003, China.
Email: Yuming_Jia@126.com