Strengthening proof of Bezout theorem

Yukun Ding

Abstract:

Bezout theorem is a very important theorem of elementary number theory. That is when an integer array $a_1,a_2,...,a_n$ has the property that $a_1,a_2,...,a_n$ are relatively prime,(i.e. $(a_1,a_2,...,a_n)=1$), there exist an infinite number of integer arrays $(x_1,x_2,...,x_n)$ which makes $x_1a_1+x_2a_2+...+x_na_n=1$. Here, there is no particular limits to $(x_1,x_2,...,x_n)$, however, can we add some conditions to it and still keep the conclusion? Firstly, our findings show that when an integer array $a_1,a_2,...,a_n$ satisfies $(a_1,a_2,...,a_n)=1$, there are an infinite number of integer arrays $(x_1,x_2,...,x_n)$ which can make $x_1a_1+x_2a_2+...+x_na_n=1$ and $x_i|x_{i+1}$ (i=1,2,…,n-2) was established at the same time. Further, we found that when n + k integers $a_1,...,a_n,b_1,...,b_k$ meet $(a_1,...,a_n,b_1,...,b_k)=1$, there are an infinite number of integer arrays $(x_1,...,x_n,y_1,...,y_k)$ which can make $x_1a_1+...+x_na_n+y_1b_1+...+y_kb_k=1$, $x_i|x_{i+1}$ (i=1,…,n-1) and $y_j|y_{j+1}$ (j = 1,..., k-1) meet the standard at the same time. In addition, our findings show that when n integers $a_1,a_2,...,a_n$ meet $(a_1,a_2,...,a_n)=1$, it has an infinite number of integer arrays $(x_1,x_2,...,x_n)$ which can make $x_1a_1+x_2a_2+...+x_na_n=1$ and $(x_i,x_j)\geq 2$ meet the standard at the same time, here $1\leq i<j\leq n$. In short, in this paper, through the concise proof, we found a series of strengthening Bezout theorem, which make it more rich and interesting.

裴蜀定理的加强证明

摘要：裴蜀定理是初等数论中一个非常重要的定理，即当 n 个整数 $a_1,a_2,...,a_n$ 满足 $(a_1,a_2,...,a_n)=1$ 时，存在无穷多组整数 $(x_1,x_2,...,x_n)$ 可以使得 $x_1a_1+x_2a_2+...+x_na_n=1$。这里的 $(x_1,x_2,...,x_n)$ 并没有特别的限制，是否可以给 $(x_1,x_2,...,x_n)$ 一些限制条件而使裴蜀定理依然成立呢？我们的研究结果表明当 n 个整数 $a_1,a_2,...,a_n$ 满足 $(a_1,a_2,...,a_n)=1$ 时，存在无穷多组整数 $(x_1,x_2,...,x_n)$ 可以使得 $x_1a_1+x_2a_2+...+x_na_n=1$ 和 $x_i \mid x_{i+1}$ (i=1,3,…,n-2)同时成立。进一步我们发现，当 n+k 个整数 $a_1,...,a_n,b_1,...,b_n$ 满足 $(a_1,...,a_n,b_1,...,b_k)=1$ 时，存在无穷多组整数 | $(x_1,...,x_n,y_1,...,y_k)$ 可以使得 $x_1a_1+...+x_na_n+y_1b_1+...+y_kb_k=1$ 和 $x_i \mid x_{i+1}$ (i=1,…,n-1)和 $y_j \mid y_{j+1}$ （j=1,…,k-1）同时满足。此外，我们的研究结果表明当 n 个整数 $a_1,a_2,...,a_n$ 满足 $(a_1,a_2,...,a_n)=1$ 时，存在无穷多组整数 $(x_1,x_2,...,x_n)$ 可以使得 $x_1a_1+x_2a_2+...+x_na_n=1$ 和 $(x_i,x_j)\geq 2$ 同时满足，这里 $1\leq i<j\leq n$。总之，在该论文中，我们通过简洁而巧妙的证明，发现了一系列加强的裴蜀定理，使得裴蜀定理更加丰富而有趣。

Strengthening proof of Bezout theorem

Bezout theorem is a very important theorem of elementary number theory, by which lots of mathematic questions at various levels can be solved. Therefore, the further understanding of this theorem is very necessary.

First, let's look at the content of the theorem, set n integers $a_1, a_2, ..., a_n$, d is their greatest common divisor（i.e. $(a_1, a_2, ..., a_n) = d$ ）, then it has an infinite number of integer arrays $(x_1, x_2, ..., x_n)$ which makes $x_1 a_1 + x_2 a_2 + ... + x_n a_n = d$. Specially, if $(a_1, a_2, ..., a_n) = 1$, then there will be an infinite number of integer arrays $(x_1, x_2, ..., x_n)$ which makes $x_1 a_1 + x_2 a_2 + ... + x_n a_n = 1$.

There are many proof methods of the theorem, it is not difficult to prove it, our idea is to take some restrictions to the integer arrays $(x_1, x_2, ..., x_n)$, which make this theorem still succeed. We start from the n = 2, if $(a_1, a_2) = 1$, there are an infinite number of integer arrays (x_1, x_2) makes $x_1 a_1 + x_2 a_2 = 1$. We guess that here (x_1, x_2) can satisfy $x_1 | x_2$（i.e. x_1 divide exactly into x_2）, which makes $x_1 a_1 + x_2 a_2 = 1$. If the conditions set up, we will get $x_1 | 1$, and we also can say the x_1 = 1 or -1, which $x_2 a_2 = 1 \pm a_1$. Obviously, the equation may not have integer solutions, such as a_1=5 , a_2=7.

Then we came to see the case when n = 3, if $(a_1, a_2, a_3) = 1$, there are infinite integer arrays (x_1,x_2,x_3) which makes $x_1a_1+x_2a_2+x_3a_3=1$, we wonder if here in (x_1,x_2,x_3), there is a relation of being divided? Assumed that $x_1|x_2$ and $x_2|x_3$, we will learn $x_1|1$, namely $x_1=1$ or -1. If the conditions are set up, we may get the equation $x_2a_2+x_3a_3=1\pm a_1$, apparently which may not have integer solutions, as the example that $a_1=77, a_2=119, a_3=187$ shows. So the conclusion is not established. So when n = 3, whether there are an infinite number of integer arrays (x_1,x_2,x_3) , and two of them have the relations of division, for example $x_1|x_2$, makes the $x_1a_1+x_2a_2+x_3a_3=1$ established. Fortunately, the theorem is set up.

We first prove a **lemma 1: if** $(a_1,a_2,a_3)=1$**, there are an infinite number of integer k, which make** $(ka_1+a_2,a_3)=1$

Prove 1: if $(a_1,a_3)=1$, prove there are infinite integer k easily, making that $ka_1+a_2\equiv 1(\mathrm{mod}\, a_3)$. The conclusion is established

If $(a_1,a_3)=d\geq 2$, unique decomposition theorem is expressed as below

$a_1=p_1^{\alpha_1}...p_l^{\alpha_l}q$ ($\alpha_i\geq 1$, and p_i is prime number)

$a_3=p_1^{\beta_1}...p_l^{\beta_l}r$ ($\beta_i\geq 1$, and p_i is prime number)

$(a_1,a_3)=d=p_1{}^{\min(\alpha_1,\beta_1)}....p_l{}^{\min(\alpha_l,\beta_l)}$

And it is easy to know that $(r,a_1)=1$, $(p_i,a_2)=1$

It is easy to prove any integer k all have $(ka_1+a_2,p_i)=1$, then $(ka_1+a_2,p_1^{\alpha_1}...p_l^{\alpha_l})=1$

And there is an infinite number of integer k which makes

$ka_1 + a_2 \equiv 1(\bmod r)$, then $(ka_1 + a_2, r) = 1$,

$(ka_1 + a_2, a_3) = 1$ is established.

Prove 2: the unique decomposition theorem will be expressed as

$a_3 = p_1^{\alpha_1} \ldots p_k^{\alpha_k} q_1^{\beta_1} \ldots q_l^{\beta_l} r_1^{\gamma_1} \ldots r_m^{\gamma_m}$

($p_1, \ldots p_k, q_1, \ldots q_l, r_1 \ldots r_m$ are prime numbers, and $\alpha_i, \beta_i, \gamma_i \geq 1$)

1) assumed that $p_i | a_1$, and $(p_i, a_2) = 1$, no matter what's value of k, $(ka_1 + a_2, p_i) = 1$

2) assumed that $(q_i, a_1) = 1$, and $q_i | a_2$ only requires $k \equiv 1(\bmod q_i)$, which makes $(ka_1 + a_2, q_i) = 1$

3) assumed that $(r_i, a_1) = 1$, $(r_i, a_2) = 1$, just need $ka_1 + a_2 \equiv 1(\bmod r_i)$

That is $ka_1 \equiv 1 - a_2(\bmod r_i)$, there must be integer b_i makes $a_1 b_i \equiv 1(\bmod r_i)$,

That is to say $k \equiv b_i(1 - a_2)(\bmod r_i)$, from $q_1, \ldots q_l, r_1, \ldots, r_m$, any two of these are relatively prime, according to the Chinese remainder theorem, the following more than equations must have an infinite number of integer solutions

$$\begin{cases} k \equiv 1(\bmod q_1) \\ \ldots \\ k \equiv 1(\bmod q_l) \\ k \equiv b_1(1 - a_2)(\bmod r_1) \\ \ldots \\ k \equiv b_m(1 - a_2)(\bmod r_m) \end{cases}$$

$(ka_1 + a_2, a_3) = 1$ is established

Using the above lemma 1, we prove the following theorem 1

Theorem 1: if $(a_1,a_2,a_3)=1$, there are an infinite number of integer arrays (x_1,x_2,x_3) , satisfy

1) $x_1a_1+x_2a_2+x_3a_3=1$

2) $x_1|x_2$

Proof: from the above lemma 1, we know that there are infinite k which makes $(ka_2+a_1,a_3)=1$,

From Bezout theorem, there are infinite integer arrays (s,t), which makes $s(ka_2+a_1)+ta_3=1$

Set $x_1=s,x_2=sk,x_3=t$, it is easy to know $x_1|x_2$, the theorem 1 was set up.

Furthermore, let's guess the above conclusions are established to all n (n≥3), that is the following guess: if $(a_1,a_2,...,a_n)=1$, it has an infinite number of integer arrays $(x_1,x_2,...,x_n)$, satisfy

1) $x_1a_1+x_2a_2+...+x_na_n=1$

2) $x_i|x_{i+1}$ (i=1,2,…,n-2)

In order to prove the guess, we should first prove the following lemma 2

Lemma 2: if $(a_1,a_2,...,a_n)=1$, there are infinite number of integer arrays $(m_1,m_2,...,m_{n-2})$ which makes $(a_1+m_1a_2+m_1m_2a_3+...+m_1...m_{n-2}a_{n-1},a_n)=1$

Prove: from the lemma 1 we know that when n = 3, the conclusions are established.

Assumed n = k is set up, let’s prove that when n = k + 1 it was set up

$(a_1, a_2, ..., a_k, a_{k+1}) = 1$, set $a_{k+1} = p_1^{\alpha_1} ... p_l^{\alpha_l} q_1^{\beta_1} ... q_h^{\beta_h}$

($p_1, ... p_l, q_1, ... q_h$ are prime numbers, and $\alpha_i, \beta_i \geq 1$)

1) assumed $(a_1, p_1 ... p_l) = 1$,

Make $m_1 \equiv 0 (\bmod p_1 ... p_l)$, then $(a_1 + m_1 a_2 + m_1 m_2 a_3 + ... + m_1 ... m_{k-1} a_k, p_1 ... p_l) = 1$

2) assumed $q_i ... q_h | a_1$, it is easy to know that $(a_2, a_3, ..., a_k, q_1 ... q_h) = 1$, from inductive assumption we know that there are an infinite number of integer arrays $(m_2, ..., m_{k-1})$, satisfy $(a_2 + m_2 a_3 + ... + m_2 ... m_{k-1} a_k, q_1 ... q_h) = 1$,

Then make $m_1 \equiv 1 (\bmod q_1 ... q_h)$,we can infer that

$(a_1 + m_1 a_2 + m_1 m_2 a_3 + ... + m_1 ... m_{k-1} a_k, q_1 ... q_h) = 1$,

It is easy to know that $(p_1 ... p_l, q_1 ... q_h) = 1$, By the Chinese remainder theorem, we know that the number of integer m_1 which meet the conditions is infinite. Then there are an infinite number of integer arrays $(m_1, m_2, ..., m_{k-1})$, which make $(a_1 + m_1 a_2 + m_1 m_2 a_3 + ... + m_1 ... m_{k-1} a_k, a_{k+1}) = 1$.

Namely when n = k + 1 is set up, by mathematical induction we know that when $n \geq 3$, if $(a_1, a_2, ..., a_n) = 1$, then there are an infinite number of integer arrays $(m_1, m_2, ..., m_{n-2})$,

Which make $(a_1 + m_1 a_2 + m_1 m_2 a_3 + ... + m_1 ... m_{n-2} a_{n-1}, a_n) = 1$

From the above lemma 2, it is easy to prove the theorem 2 which we guessed before is established, namely

Theorem 2: if $(a_1, a_2, ..., a_n) = 1$**, there are an infinite number of integer arrays** $(x_1, x_2, ..., x_n)$**, satisfy**

1） $x_1a_1 + x_2a_2 + ... + x_na_n = 1$

2） $x_i \left| x_{i+1} \right.$ **(i=1,2,…,n-2)**

Prove: from the lemma 2, it can be seen that there are an infinite number of integer arrays (x, y) which makes

$x(a_1 + m_1a_2 + m_1m_2a_3 + ... + m_1...m_{n-2}a_{n-1}) + ya_n = 1$ established

Set $x_1 = x, x_2 = xm_1, x_3 = xm_1m_2, ..., x_{n-1} = xm_1m_2...m_{n-2}, x_n = y$

It is easy to know theorem 2 was set up

Furthermore , we proposed the following guess: $n \geq 2$, $k \geq 2$, if $(a_1, ..., a_n, b_1, ..., b_k) = 1$, then there are an infinite number of integer arrays $(x_1, ..., x_n, y_1, ..., y_k)$, satisfy

1） $x_1a_1 + ... + x_na_n + y_1b_1 + ... + y_kb_k = 1$

2） $x_i \left| x_{i+1} \right.$ (i=1,…,n-1) and $y_j \left| y_{j+1} \right.$ (j=1,…,k-1)

In order to prove the guess, we first prove the lemma 3 below

Lemma 3:If $(a_1, ..., a_n, b_1, ..., b_k) = 1$**, there are an infinite number of integer arrays** $(m_1, ..., m_{n-1}, t_1, ..., t_{k-1})$ **which make**

$(a_1 + m_1a_2 + m_1m_2a_3 + ... + m_1...m_{n-1}a_n, b_1 + t_1b_2 + t_1t_2b_3 + ... + t_1...t_{k-1}b_k) = 1$

Prove: set $(a_1, a_2, ..., a_n) = d$, so $(b_1, ..., b_k, d) = 1$

From lemma 2, we can infer that there are an infinite number of integer arrays $(t_1, ..., t_{k-1})$ which make $(b_1 + t_1b_2 + t_1t_2b_3 + ... + t_1...t_{k-1}b_k, d) = 1$,

So, it is easy to know that $(a_1, a_2, ..., a_n, b_1 + t_1b_2 + t_1t_2b_3 + ... + t_1...t_{k-1}b_k) = 1$

From lemma2, we also infer that there are an infinite number of integer arrays $(m_1,...,m_{n-1})$ which make

$(a_1+m_1a_2+m_1m_2a_3+...+m_1...m_{n-1}a_n, b_1+t_1b_2+t_1t_2b_3+...+t_1...t_{k-1}b_k)=1$

From the above lemma 3, it is easy to prove that the theorem 3 we guessed before is established, namely

Theorem 3: $n\ge 2$ **,** $k\ge 2$**, if** $(a_1,...,a_n,b_1,...,b_k)=1$**, there are an infinite number of integer arrays** $(x_1,...,x_n,y_1,...,y_k)$**, satisfy**

1) $x_1a_1+...+x_na_n+y_1b_1+...+y_kb_k=1$

2) $x_i\,|\,x_{i+1}$ **(i=1,…,n-1) and** $y_j\,|\,y_{j+1}$ **(j=1,…,k-1)**

Prove: from the lemma 3, it can be seen that there are an infinite number of integer arrays (m,t) which makes

$m(a_1+m_1a_2+m_1m_2a_3+...+m_1...m_{n-1}a_n)+t(b_1+t_1b_2+t_1t_2b_3+...+t_1...t_{k-1}b_k)=1$,

set $x_1=m, x_2=mm_1,...,x_n=mm_1m_2...m_{n-1}, y_1=t, y_2=tt_1,...,y_k=tt_1t_2...t_{k-1}$

It easy to know that theorem 3 was set up

Now, let's prove the interesting theorem 4

Theorem 4: $n\ge 3$**, if** $(a_1,...,a_n)=1$**, there are an infinite number of integer arrays** $(x_1,...,x_n)$**, satisfy**

1) $x_1a_1+...+x_na_n=1$

2) $(x_i,x_j)\ge 2$ **,** $1\le i<j\le n$

Prove: Set $a_t=p_{1,t}^{\alpha_{1,t}}\cdots p_{k_t,t}^{\alpha_{k_t,t}}$ $\quad 1\le t\le n$

Set $B = q_1 q_2 ... q_n$, $B_i = \dfrac{B}{q_i}$ ($q_1,...,q_n$ are prime numbers which are different from $p_{1,t},..., p_{k_t,t}, 1 \le t \le n$)

Set $c_i = B_i a_i$, $1 \le i \le n$

Then it is easy to know that $(c_1, c_2,..., c_n) = 1$, from the Bezout theorem, we know that there are an infinite number of integer arrays $(y_1,..., y_n)$ which make $y_1 c_1 + ... + y_n c_n = 1$

Therefore $y_1 B_1 a_1 + ... + y_n B_n a_n = 1$

Set $x_i = y_i B_i$ then $(x_i, x_j) \ge \dfrac{B}{q_i q_j} \ge 2$

We can also strengthen the theorem 2 into the theorem 5

Theorem 5: if $(a_1, a_2,..., a_n) = 1$, there are an infinite number of integer arrays $(x_1,..., x_n)$, satisfy

1) $x_1 a_1 + x_2 a_2 + ... + x_n a_n = 1$

2) $x_i \mid x_{i+1}$ **(i=1,2,…,n-2)**

3) $(x_i, x_n) \ge 2$ **(i=2,…,n-1)**

Prove: Set $a_t = p_{1,t}^{\alpha_{1,t}} ... p_{k_t,t}^{\alpha_{k_t,t}}$ $1 \le t \le n$

Set $b_1 = q_1 a_1, b_n = q_2 a_n, b_i = q_1 q_2 a_i$, $2 \le i \le n-1$

(q_1, q_2 are prime numbers which are different from $p_{1,t},..., p_{k_t,t}$, $1 \le t \le n$)

Therefore $(b_1,..., b_n) = 1$

From the theorem 2, we can infer that there are an infinite number of integer arrays $(y_1, y_2, ..., y_n)$, satisfy

1) $y_1b_1 + y_2b_2 + ... + y_nb_n = 1$,

2) $y_i | y_{i+1}$ (i=1,2,…,n-2)

From 1), we can infer that $y_1q_1a_1 + y_2q_1q_2a_2 + ... + y_{n-1}q_1q_2a_{n-1} + y_nq_2a_n = 1$

Set $x_1 = y_1q_1, x_n = y_nq_2, x_i = y_iq_1q_2$, $2 \le i \le n-1$

Therefore there are an infinite number of integer arrays $(x_1, x_2, ..., x_n)$,

satisfy 1) $x_1a_1 + x_2a_2 + ... + x_na_n = 1$

2) $x_i | x_{i+1}$ (i=1,2,…,n-2)

3) $(x_i, x_n) \ge 2$ (i=2,…,n-1)

After continuous exploration, we get a series of very interesting theorems 1-5 as well as important lemmas 1-3. Finally, we proved theorems 2-5 which are stronger than Bezout theorem. To the best of our knowledge, the similar conclusion on Bezout theorem was scarcely reported. Therefore, we could see if we continue to explore some old and classic theorem, we can get some interesting new results. We wish this article can play a valuable role on Bezout theorem.

Bibliography

[1] PanChengDong, PanChengBiao, *The concise number theory* , Beijing university press, 1998.1

[2] ShenWenXuan, ZhangYao, LengGangSong, TangLiHua, *The Olympic mathematics elementary theory,* hunan normal university press, 2009.8