Pure Mathematics 理论数学, 2023, 13(12), 3439-3446
Published Online December 2023 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2023.1312356

Hans汉斯

应用费尔马小定理求解一些同余和不定方程

苑金臣，郭艳凤*，王军霞

中国地质大学(武汉)数学与物理学院，湖北 武汉

收稿日期：2023年11月9日；录用日期：2023年12月11日；发布日期：2023年12月20日

摘 要

本文主要利用费尔马小定理研究一些同余方程和不定方程解的问题。根据费尔马小定理证明问题的条件和思想，通过详细的推导得到了一些重要的结论。这些结论主要包括 $21x^{18}+2y^{15}-x^4-3\equiv 0\pmod 7$ 和 $x^2+3\equiv 0\pmod 5$ 无整数解；不定方程 $x^3-3xy^2+y^3=2981$ 和 $15x^2-7y^2=9$ 无整数解。此外，还利用费尔马小定理考虑了一些多项式问题和五次不定方程 $x^5+y^5=z^5$ 的解，并给出了其他的一些应用。

关键词

费马小定理，同余方程，不定方程，整数解

Using Fermat's Little Theorem to Solve Some Congruence Equations and Indefinite Equations

Jinchen Yuan, Yanfeng Guo*, Junxia Wang

School of Mathematics and Physics, China University of Geosciences (Wuhan), Wuhan Hubei

Received: Nov. 9th, 2023; accepted: Dec. 11th, 2023; published: Dec. 20th, 2023

Abstract

In this paper, using Fermat's little theorem, the solutions of some congruence equations and indefinite equations are mainly studied. Through the idea of Fermat's small theorem in the proof, some important conclusions are obtained according to the detailed derivation. These conclusions are mainly given. The equations $21x^{18}+2y^{15}-x^4-3\equiv 0\pmod 7$ and $x^2+3\equiv 0\pmod 5$ have not integer

*通讯作者。

文章引用: 苑金臣, 郭艳凤, 王军霞. 应用费尔马小定理求解一些同余和不定方程[J]. 理论数学, 2023, 13(12): 3439-3446. DOI: 10.12677/pm.2023.1312356

solutions. The indefinite equations $x^3-3xy^2+y^3=2981$ and $15x^2-7y^2=9$ have not integer solutions. In addition, some polynomial problems are also considered. And the solutions of pentadic indefinite equation $x^5+y^5=z^5$ are investigated by using Fermat's small theorem. Finally, the others applications of the Fermat's small theorem are given.

Keywords

Fermat's Little Theorem, Congruence Equations, Indefinite Equations, Integer Solutions

Copyright © 2023 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

众所周知，费尔马小定理是数论中的著名定理[1] [2] [3] [4] [5]，具体定理如下。

[1] [2] p 是素数，a 是整数，$p\nmid a$ 则 $a^{p-1}\equiv 1(\bmod p)$。

费尔马小定理有着广泛的应用，对研究同余方程和不定方程解的问题起着非常重要的作用。本文主要从费尔马小定理出发，研究一些同余方程和不定方程的整数解问题。

众所周知，对于许多同余方程与不定方程的问题，通常用素数 p 的剩余类去进行代入验证。但实际上可利用费尔马小定理去进行简化运算和证明。本文将对于此类的一些问题给出具体详细的证明思路，同时也采用费尔马小定理讨论费尔马大定理所涉及的不定方程在 $n=5$，$n=7$ 与 $n=3$ 情形下的一些结果，主要结果包括当 $n=5$，$n=7$ 时，倘若存在解，则讨论了解的某种性质，而 $n=7$ 是一种特殊情况；同时也讨论了 $n=3$ 时相应结果的证明。

本文通过费尔马小定理的主要思想和具体的推导过程，主要得到了下面的结果。首先，得到两个同余方程 $21x^{18}+2y^{15}-x^4-3\equiv 0(\bmod 7)$ 和 $x^2+3\equiv 0(\bmod 5)$ 无整数解的结果。其次，得到两个不定方程 $x^3-3xy^2+y^3=2981$ 和 $15x^2-7y^2=9$ 无整数解的结果。最后，利用费尔马小定理的主要思想考虑了一些多项式的问题，例如在五次不定方程 $x^5+y^5=z^5$ 中必定 $5\mid xyz$ 等诸多问题。

2. 同余方程的无整数解问题

同余方程 $x^2+3\equiv 0(\bmod 5)$ 无整数解。

证明：如果 $x\equiv 0(\bmod 5)$，显然出现矛盾。假定 x 是方程的解，则 $5\nmid x$。

由费尔马小定理可得 $x^4\equiv 1(\bmod 5)$。

原同余式两端平方，可得 $x^4+6x^2+9\equiv 0(\bmod 5)$，即 $1+5x^2+x^2+9\equiv 0(\bmod 5)$。

由此可知 $x^2\equiv 0(\bmod 5)$，与 $5\nmid x$ 矛盾，所以原同余式无整数解。证毕。

注：在文献[1]中第 36 页例 3 中的证明思想是把 $x\equiv 0,1,2,3,4,5(\bmod 5)$ 代入验证。若应用费尔马小定理证明，只需平方一次即可。由上述证明思路，容易得到另一个同余方程 $x^2+2\equiv 0(\bmod 5)$ 也无整数解。

简化同余方程 $21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0(\bmod 7)$ 无整数解。

在文献[2]中第 193 页例 3 是先简化同余方程 $21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0(\bmod 7)$，最后结果是直接带入 $x\equiv 0,\pm 1,\pm 2,\pm 3(\bmod 7)$ 计算知该同余方程无解。本文利用费尔马小定理来证明。当 $7\nmid x$，则 $x^6\equiv 1(\bmod 7)$。

因而当 mod7 时有

$$x^7=x^6\cdot x\equiv x(\bmod 7),x^8\equiv x^2(\bmod 7),x^9\equiv x^3(\bmod 7),x^{10}\equiv x^4(\bmod 7),x^{12}\equiv 1(\bmod 7),$$

$$x^{15}\equiv x^{12}\cdot x^3\equiv x^3(\bmod 7),9\equiv 2(\bmod 7),16=14+2\equiv 2(\bmod 7),-27=1-28\equiv 1(\bmod 7),$$

$$64=63+1\equiv 1(\bmod 7),24\equiv 3(\bmod 7)。$$

在以下证明中，需要用到这些简单的事实。

证明： 首先讨论 $x^2\equiv 0(\bmod 7)$ 的情况，即 $x\equiv 0(\bmod 7)$。

由于代入原同余方程 $21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0(\bmod 7)$ 中可以得到 $-3\equiv 0(\bmod 7)$，产生矛盾。

因而 $7\nmid x$，原同余方程去掉系数为 7 的倍数的项可得 $2x^{15}-x^{10}+4x-3\equiv 0(\bmod 7)$。此式等价同余方程 $2x^3-x^4+4x-3\equiv 0(\bmod 7)$。该方程的等价形式为 $x^4+3\equiv 2x^3+4x(\bmod 7)$。

上式两端平方后进行逐步简化，每步都是 mod7，依次可得 $x^8+6x^4+9\equiv 4x^6+16x^4+16x^2(\bmod 7)$，从而 $x^2+6x^4+9\equiv 4+16x^4+16x^2(\bmod 7)$。进一步可得 $5\equiv 10x^4+15x^2(\bmod 7)$，即 $-2\equiv 3x^4+x^2(\bmod 7)$。

接着对 $-2\equiv 3x^4+x^2(\bmod 7)$ 两端再平方后简化，同样每步 mod7，又依次可得 $4\equiv 9x^8+6x^6+x^4(\bmod 7)$，从而有 $4\equiv 2x^2+6+x^4(\bmod 7)$。

因此，可知 $-2\equiv x^4+2x^2(\bmod 7)$。于是 $4\equiv x^8+4x^6+4x^4(\bmod 7)$，从而有 $4\equiv x^2+4+4x^4(\bmod 7)$，进一步可知 $4x^4+x^2\equiv 0(\bmod 7)$，也就是 $4x^4\equiv -x^2(\bmod 7)$，即 $4x^2\equiv -1(\bmod 7)$。

上式两端立方可得 $64x^6\equiv -1(\bmod 7)$。因此有 $65\equiv 0(\bmod 7)$，产生矛盾。所以原同余方程无解。证毕。

3. 不定方程的整数解问题

不定方程 $15x^2-7y^2=9$ 无整数解。

证明： 由于 $3|15$，所以 $3|y$，$3^2|y^2$。于是又得出 $3|x$。

设 $x=3a,y=3b$，代入原不定方程得 $15(3a^2)-7(3b)^2=9$，即有 $9(15a^2-7b^2-1)=0$，$15a^2-7b^2-1=0$。整理可得 $15a^2=7b^2+1$。

下面证明 $15a^2=7b^2+1$ 无整数解。

显然，若 $3|b$，则 $15a^2=7b^2+1$ 矛盾。若 $3\nmid b$，则由费尔马小定理得 $b^2\equiv 1(\bmod 3)$。

将 $b^2\equiv 1(\bmod 3)$ 代入 $15a^2=7b^2+1$ 中，得 $15a^2=7b^2+1\equiv 8(\bmod 3)$，即 $15a^2\equiv 8(\bmod 3)$，矛盾。

于是，$15a^2-7b^2-1\neq 0$，$9(15a^2-7b^2-1)\neq 0$ 所以原不定方程无整数解。证毕。

不定方程 $x^3-3xy^2+y^3=2891$ 无整数解。

证明： 由于 $2891=7^2\times 59$，所以 $7\nmid x$，$7\nmid y$。

这是因为若 $7|x$ 和 $7|y$ 中只要有一个成立，则另一个也成立。

于是 $7^3|x^3-3xy^2+y^3$，但 $7^3\nmid 2891$，矛盾。

由费尔马小定理可知 $x^6\equiv y^6\equiv 1(\bmod 7)$。

原不定方程模 7 可得 $x^3-3xy^2+y^3=0(\bmod 7)$，即 $x^3-3xy^2=-y^3(\bmod 7)$。

上式两端平方后再逐步简化，可依次得

$$+9x^2y^4=y^6(\bmod 7),x^6-6x^4y^2+9x^2y^4=1(\bmod 7),-6x^4y^2+9x^2y^4=0(\bmod 7)。$$

由于 $6\equiv -1$，$9\equiv 2(\bmod 7)$，$-6x^4y^2+9x^2y^4=0(\bmod 7)$，可以进一步简化为 $-x^2\equiv 2y^2(\bmod 7)$。

$-x^2\equiv 2y^2(\bmod 7)$ 两端立方得 $-x^6\equiv 8y^6(\bmod 7)$，即 $-1\equiv 8(\bmod 7)$，产生矛盾。所以原不定方程无解。证毕。

在文献[4]中第 555 页例 19 [IMO, 4(ii)]也证明了 $x^3-3xy^2+y^3=2891$ 无整数解，但这里给出一个新的

简明证法。

在五次不定方程 $x^5+y^5=z^5$ 中必定 $5\mid xyz$。

证明：假设 $5\nmid xyz$，则得 $x^4\equiv y^4\equiv z^4\equiv 1(\bmod 5)$。

记 $x^5=x^4\cdot x=x+5l$，$y^5=y+5m$，$z^5=z+5n$。

代入到原不定方程 $x^5+y^5=z^5$ 中得 $x+5l+y+5m=z+5n$，即 $x+y+5(l+m-n)=z$。

上式中记 $l-m-n=k$，则有 $x+y+5k=z$。将 $x+y+5k=z$ 代入 $x^5+y^5=z^5$ 式，可得

$$0=(x+y)^5-x^5-y^5+5(x+y)^4(5k)+10(x+y)^3(5k)^2+10(x+y)^2(5k)^3+5(x+y)(5k)^4+(5k)^5。$$

把上式简记为

$$0=(x+y)^5-x^5-y^5+5^2A,$$

其中 $A=(x+y)^4k+10(x+y)^3k^2+50(x+y)^2k^3+125(x+y)k^4+125k^5$。

由 $0=(x+y)^5-x^5-y^5+5^2A$ 出发可得

$$\begin{aligned}0&=5x^4y+10x^3y^2+10x^2y^3+5xy^4+5^2A=5xy\left(x^3+2x^2y+2xy^2+y^3\right)+5^2A\\&=5xy\left[(x+y)\left(x^2-xy+y^2\right)+2xy(x+y)\right]+5^2A=5xy(x+y)\left(x^2+xy+y^2\right)+5^2A.\end{aligned}$$

从 $5\nmid xyz$ 及 $x+y+5(l+m-n)=z$ 式可知 $5\nmid x+y$，只要证明了 $5\nmid x^2+xy+y^2$，则可以得出

$$0=5xy(x+y)\left(x^2+xy+y^2\right)+5^2A。$$

于是产生矛盾。

下证 $5\nmid x^2+xy+y^2$。

设 $x^2+xy+y^2=5m$，平方后得

$$(5m)^2=\left(x^2+xy+y^2\right)^2=x^4+x^2y^2+y^4+2x^3y+2x^2y^2+2xy^3\equiv 2+3x^2y^2+2xy\left(x^2+y^2\right)(\bmod 5),$$

即 $0\equiv 2+3x^2y^2+2xy\left(x^2+y^2\right)(\bmod 5)$。从而可得 $2+3x^2y^2\equiv -2xy\left(x^2+y^2\right)(\bmod 5)$。

上式两端平方后整理，依次可得

$$4+12x^2y^2+9x^4y^4\equiv 4x^2y^2\left(x^4+2x^2y^2+y^4\right)(\bmod 5),$$

$$4+12x^2y^2+9\equiv 4x^2y^2\left(2+2x^2y^2\right)(\bmod 5),$$

$$4+12x^2y^2+9\equiv 8x^2y^2+8x^4y^4(\bmod 5),$$

$$4+4x^2y^2+9\equiv 8(\bmod 5),\quad 4x^2y^2\equiv -5\equiv 0(\bmod 5)。$$

上式两端再平方得 $16x^4y^4\equiv 0(\bmod 5)$，化简后得 $1\equiv 0(\bmod 5)$，矛盾。这就证明了 $5\nmid x^2+xy+y^2$。

所以 $0=5xy(x+y)\left(x^2+xy+y^2\right)+5^2A$ 不成立。证毕。

不定方程

$$(7a+1)x^3+(7b+2)y^3+(7c+4)z^3+(7d+1)xyz=0 \tag{1}$$

仅有整数解 $x=y=z=0$。

证明：本文用费尔马小定理，进行模 7 证明，分几种情况。

当 $7\mid z, 7\nmid xy$ 时，$x^6\equiv y^6\equiv 1(\bmod 7)$，从(1)式得 $x^3+2y^3\equiv 0(\bmod 7)$，即 $x^3\equiv -2y^3(\bmod 7)$。上式平方得 $x^6\equiv 4y^6(\bmod 7)$。于是 $1\equiv 4(\bmod 7)$。矛盾。

当 $7\nmid z, 7\mid x, 7\nmid y$ 时，从(1)式可得 $2y^3+4z^3\equiv 0\pmod 7$。这就是上面(1)的情况。

当 $7\nmid z, 7\nmid x, 7\mid y$ 时，从(1)式可得 $x^3+4y^3\equiv 0\pmod 7$，即 $x^3\equiv -4y^3\pmod 7$。上式平方可得 $x^6\equiv 16y^6\pmod 7$。于是 $1\equiv 16\pmod 7$，矛盾。

当 $7\mid xy, 7\nmid z$ 时，$4z^3\equiv 0\pmod 7$ 没有解。同样，$7\mid yz, 7\nmid x$ 时，无解；$7\mid xz, 7\nmid y$ 时，也无解。

当 $7\nmid xyz$ 时，$x^6\equiv y^6\equiv z^6\equiv 1\pmod 7$。从(1)式得

$$x^3+2y^3+4z^3\equiv -xyz\pmod 7. \tag{2}$$

上式立方可得

$$\left(x^3+2y^3\right)^3+3\left(x^3+2y^3\right)^2\left(4z^3\right)+3\left(x^3+2y^3\right)\left(4z^3\right)^2+64z^9\equiv -\left(xyz\right)^3\pmod 7,$$

即

$$\left[x^9+3x^6\left(2y^3\right)+3x^3\left(2y^3\right)^2+8y^9\right]+3\left(x^6+4x^3y^3+4y^6\right)\left(4z^3\right)+\left(3x^3+6y^3\right)\left(16z^6\right)+64z^9=-\left(xyz\right)^3\pmod 7。$$

由于 $x^9\equiv x^3\pmod 7, y^9\equiv y^3\pmod 7, z^9\equiv z^3\pmod 7, 64=63+1\equiv 1\pmod 7, 16=14+2\equiv 2\pmod 7$，

则上式简化为

$$\left[x^3+6y^3+3x^3\left(4y^6\right)+y^3\right]+\left[12z^3+48x^3y^3z^3+48z^3\right]+\left(3x^3+6y^3\right)\left(16z^6\right)+z^3\equiv -\left(xyz\right)^3\pmod 7。$$

从而

$$\left[x^3+6y^3+12x^3+y^3\right]+\left[12z^3+48x^3y^3z^3+48z^3\right]+\left(3x^3+6y^3\right)\left(16z^6\right)+z^3\equiv -\left(xyz\right)^3\pmod 7,$$

其中 $48x^3y^3z^3\equiv -x^3y^3z^3\pmod 7; 7y^3\equiv 0\pmod 7; 16z^6\equiv 2\pmod 7$。

从上式可得

$$x^3+12x^3+\left(-3z^3\right)+6x^3+12y^3+z^3\equiv 0\pmod 7,$$

$$12x^3+12y^3-2z^3\equiv 0\pmod 7,$$

$$-2x^3-2y^3-2z^3\equiv 0\pmod 7,$$

$$x^3+y^3\equiv -z^3\pmod 7.$$

上式依次平方可得

$$x^6+2x^3y^3+y^6=z^6\pmod 7,$$

$$1+2x^3y^3+1\equiv 1\pmod 7,$$

$$2x^3y^3\equiv -1\pmod 7,$$

$$4x^6y^6\equiv 1\pmod 7.$$

于是从上面可知 $4\equiv 1\pmod 7$，矛盾。

综上所述，x, y, z 中，只要有一个不是 7 的倍数就矛盾，3 个都不是 7 的倍数也矛盾。如果三个都是 7 的倍数，可设 $x=7e, y=7f, z=7g$，代入(2)式可得

$$\left(7a+1\right)e^3+\left(7b+2\right)f^3+\left(7c+4\right)g^3+\left(7d+1\right)efg=0. \tag{3}$$

如果(3)式中出现上面所讨论的情况就是矛盾，否则过程继续下去。由于 x, y, z 是具体数，如果可被 7 的任意次幂所整除，只有 $x=y=z=0$，过程才可继续下去。这就说明(1)式仅有解 $x=y=z=0$。证毕。

4. 其他应用

关于一个多项式的问题。

([4])设 a,b 是整数，$11\nmid a$，证明 $11\nmid a^2+5b^2$。

证明：用反证法。

若 $11\mid a^2+5b^2$，显然 $11\nmid b$。否则得出 $11\mid a$，矛盾。

由费尔马小定理知 $a^{10}\equiv b^{10}\equiv 1(\bmod 11)$。若 $11\mid a^2+5b^2$，则 $11\mid\left(a^2+5b^2\right)^5$。于是

$$11\mid a^{10}+5a^8\left(5b^2\right)+10a^6\left(5b^2\right)^2+10a^4\left(5b^2\right)^3+5a^2\left(5b^2\right)^4+\left(5b^2\right)^5。$$

而

$$\begin{aligned}&a^{10}+5a^8\left(5b^2\right)+10a^6\left(5b^2\right)^2+10a^4\left(5b^2\right)^3+5a^2\left(5b^2\right)^4+\left(5b^2\right)^5\\&\equiv 1+5a^8\left(5b^2\right)+5a^2(5b^2)^4+10a^6\left(5b^2\right)^2+10a^4\left(5b^2\right)^3+5^5(\bmod 11)\\&\equiv 1+5a^2\left(5b^2\right)\left[a^6+\left(5b^2\right)^3\right]+10a^4\left(5b^2\right)^2\left(a^2+5b^2\right)+5^5(\bmod 11).\end{aligned}$$

由于 $x^3+y^3=(x+y)\left(x^2-xy+y^2\right)$，上式第二项含 $\left(a^2\right)^3+\left(5b^2\right)^3$，同时

$$5^5=(22+3)\cdot(22+3)\cdot 5\equiv 3\cdot 3\cdot 5(\bmod 11),$$

所以 $11\mid\left(a^2+5b^2\right)^5\equiv 1+0+0+3\cdot 3\cdot 5=46(\bmod 11)$，矛盾。因此 $11\nmid a^2+5b^2$。证毕。

设有方程

$$x^7+y^7=z^7, \tag{4}$$

且 $x\equiv 1(\bmod 7)$ 与 $y\equiv 1(\bmod 7)$ 不能同时成立，则必定 $7\nmid xyz$。

分析：费尔马小定理是数论中一个著名定理，我们用费尔马小定理证明了若整数满足 $x^5+y^5=z^5$，则必定 $5\mid xyz$。本文利用[3]中的方法来进行证明。

证明：(1) 若 $7\nmid xyz$，由费尔马小定理，则 $x^6\equiv y^6\equiv z^6\equiv 1(\bmod 7)$。

记 $x^7=x^6\cdot x=x+7l$；$y^7=y+7m$；$z^7=z+7n$，代入(4)式中有

$$x+7l+y+7m=z+7n.$$

记 $x+y+7(l+m-n)=x+y+7k=z$，代入(4)式中有

$$\begin{aligned}x^7+y^7=z^7&=(x+y+7k)^7\\&=(x+y)^7+7(x+y)^6(7k)+21(x+y)^5(7k)^2+35(x+y)^4(7k)^3\\&\quad+35(x+y)^3(7k)^4+21(x+y)^2(7k)^5+7(x+y)(7k)^6+(7k)^7.\end{aligned}$$

于是

$$\begin{aligned}0=&(x+y)^7-x^7-y^7+7(x+y)^6(7k)+21(x+y)^5(7k)^2+35(x+y)^4(7k)^3\\&+35(x+y)^4(7k)^3+35(x+y)^3(7k)^4+21(x+y)^2(7k)^5+7(x+y)(7k)^6+(7k)^7.\end{aligned}$$

因此

$$\begin{aligned}0=&7x^6y+21x^5y^2+35x^4y^3+35x^3y^4+21x^2y^5+7xy^6+7^2(x+y)^6k+3\cdot 7^2(x+y)^5\left(7k^2\right)\\&+5\cdot 7^2(x+y)^4\left(7^2k^3\right)+5\cdot 7^2(x+y)^3\left(7^3k^4\right)+3\cdot 7^2(x+y)^2\left(7^4k^5\right)+7^2(x+y)\left(7^5k^6\right)+7^2\left(7^5k^7\right),\end{aligned}$$

即

$$0 = x^6y + 3x^5y^2 + 5x^4y^3 + 5x^3y^4 + 3x^2y^5 + xy^6 + 7T, \tag{5}$$

其中

$$T = (x+y)^6 k + 3(x+y)^5 (7k^2) + 5(x+y)^4 (7^2k^3) + 5(x+y)^3 (7^3k^4) + 3(x+y)^2 (7^4k^5) + (x+y)(7^5k^6) + 7^5k^7.$$

记 $A = x^6y + 3x^5y^2 + 5x^4y^3 + 5x^3y^4 + 3x^2y^5 + xy^6$。从上式可看出，只要证明了 $7 \nmid A$，则(5)式不成立，也就证明了 $7 \nmid xyz$ 是矛盾的。

(2) 下面用反证法证 $7 \nmid A$。

由于 $x \equiv 1 \pmod 7$，则 $x^3 \equiv 1 \pmod 7$ 或 $x^3 \equiv -1 \pmod 7$。同样 $y^3 \equiv 1 \pmod 7$ 或 $y^3 \equiv -1 \pmod 7$，这就有(1)中情况的组合，下面分别讨论。

当 $x^3 \equiv -1 \pmod 7$，$y^3 \equiv -1 \pmod 7$，$x^3y^3 \equiv 1 \pmod 7$ 时，(5)式就是

$$\begin{aligned} 0 &\equiv x^6y + 3x^5y^2 + 5x^4y^3 + 5x^3y^4 + 3x^2y^5 + xy^6 + 7T \pmod 7 \\ &\equiv y - 3x^2y^2 + 5x + 5y - 3x^2y^2 + x + 7T \pmod 7 \\ &\equiv 6(x+y) - 6x^2y^2 + 7T \pmod 7. \end{aligned}$$

若(5)式成立，有

$$\begin{aligned} x + y - x^2y^2 &\equiv 0 \pmod 7, \\ x + y &\equiv x^2y^2 \pmod 7. \end{aligned} \tag{6}$$

上式两端四次方可得

$$(x+y)^4 = (xy)^8 = (xy)^6 (xy)^2 \equiv (xy)^2 \equiv x + y \pmod 7.$$

由于 $7 \nmid x + y$，从上式可得

$$\begin{aligned} (x+y)^3 &\equiv 1 \pmod 7, \\ x^3 + 3x^2y + 3xy^2 + y^3 &\equiv 1 \pmod 7, \\ -1 + 3x^2y + 3xy^2 - 1 &\equiv 1 \pmod 7, \\ 3x^2y + 3xy^2 &\equiv 3 \pmod 7. \end{aligned} \tag{7}$$

对(6)式两端同乘 x^2y^2 可得

$$\begin{aligned} x^2y^2(x+y) &\equiv x^4y^4 \equiv -xy \pmod 7, \\ x^3y^2 + x^2y^3 &\equiv -xy \pmod 7, \\ -x^2 - y^2 &\equiv -xy \pmod 7, \\ x^2 + y^2 &\equiv xy \pmod 7. \end{aligned}$$

上式两端立方可得

$$\begin{aligned} x^6 + 3x^4y^2 + 3x^2y^4 + y^6 &\equiv (xy)^3 = 1 \pmod 7, \\ 1 - 3xy^2 - 3x^2y + 1 &= 1 \pmod 7, \\ -3x^2y - 3xy^2 &\equiv -1 \pmod 7, \\ 3x^2y + 3xy^2 &\equiv 1 \pmod 7. \end{aligned} \tag{8}$$

从(7)式，(8)式知$1\equiv 3\pmod 7$，显然矛盾。当$x^3\equiv 1\pmod 7, y^3\equiv -1\pmod 7, (xy)^3\equiv -1\pmod 7$时，(4)式就是

$$0=y+3x^2y^2-5x-5y-3x^2y^2+x+7T\equiv -4x-4y+7T\pmod 7.$$

若(4)式成立，就得$7\mid x+y$，这与$x+y+7k=z, 7\nmid z$矛盾。

当$x^3\equiv -1, y^3\equiv 1, (xy)^3\equiv -1\pmod 7$时，(4)式就是

$$0=y-3x^2y^2-5x-5y+3x^2y^2+x+7T\equiv -4x-4y+7T\pmod 7.$$

同(6)式一样，矛盾。

综合以上可知(5)式不成立，所以$7\mid xyz$。证毕。

5. 总结

本文主要是对费尔马小定理在不定方程和方程有无整数解的应用。对于很多可以通过简单的余数进行判别的问题，本文仅仅通过费尔马小定理的方式进行证明，效果同样很好。另一方面，本文用费尔马小定理去证明一些简单用余数判别不了的问题，也就是我们常见的不定方程和同余方程。在这些问题中，通过费尔马小定理进行探究，取得了一些很好的成果。总体来说，对于简单的可以采用余数判别的问题，还可以用余数判别法，结合费尔马小定理同时应用如无穷递降法之类的方法进行辅助证明，可将数论中的求解问题推广到更广的范围。

基金项目

本论文由高等学校大学数学教学研究中心项目(项目编号 CMC20220209)和中国地质大学(武汉)教学改革研究重点项目(项目编号 2022086)资助。

参考文献

[1] 柯召, 孙琦. 数论讲义(上册) [M]. 第 2 版. 北京: 高等教育出版社, 2009.

[2] 潘承洞, 潘承彪. 简明数论[M]. 北京: 北京大学出版社, 2007.

[3] 柯召, 孙琦. 数论讲义(下册) [M]. 北京: 高等教育出版社, 1990.

[4] 潘承洞, 潘承彪. 初等数论[M]. 第 3 版. 北京: 北京大学出版社, 2017.

[5] Edwards, H.M. (2011) Fermat's Last Theorem: A Genetic introduction to Algebraic Number Theory. Science Press, Beijing.