不 定 方 程 (续 2)

例 6．求方程$W!=x!+y!+z!$的所有正整数解.

(1983 年加拿大数学竞赛题)

【解】由对称性,不妨设$x\le y\le z$.显然$W\ge z+1$，于是$(z+1)!\le W!=x!+y!+z!\le 3z!$,

即$(z+1)!\le 3z!$, 于是$z+1\le 3, z\le 2$. 由$x\le y\le z$知，

（1） $z=2, y=2, x=2$时，$W=3$;

（2） $z=2, y=2, x=1$时，W无解；

（3） $z=2, y=1, x=1$时，W无解；

（4） $z=1, y=1, x=1$时，W无解；

于是原方程只有一组正整数解：$x=2, y=2, z=2$，$W=3$.

【评述】建立“递推关系”也是解竞赛题的一种常用技巧.对于不定方程,如果能建立未知数的某种递推关系,并且再知一组简单解(相当于递推数列中的初始值),那么,就可以通过递推关系得到所有解,请看例 7.

例 7：确定m^2+n^2的最大值.其中m、n为整数，且满足：

m、$n\in\{1,2,\cdots,1981\}, (n^2-mn-m^2)^2=1.$ ①

（第 22 届 IMO 试题）

【解】只需找到适合①的最大m、n，由$n^2-mn-m^2=\pm 1$可得$n^2=m^2+mn\pm 1\ge m^2$.因m、n为不大于 1981 的正整数，因此有$n\ge m$，当且仅当$m=n=1$时等号成立.

显然$m=1, n=1$是①的一组解.当$m\ne 1, n\ne 1$时，$n-m>0$，且有（递推关系）：

$$(n^2-mn-m^2)^2=[(n-m)^2+m(n-m)-m^2]^2=[m^2-m(n-m)-(n-m)^2]^2.$$

于是，若（m,n）是①的一组解，那么（$n-m,m$）也是①的一组解.由于$n>m$，则可从（n,m）出发，递降得到（1，1）.反之,亦成立.即由解（1，1）出发，利用从（$n-m,m$）$\to$（n,m）可得到满足$m,n\in\{1,2,\cdots,1981\}$的全部解.即

（1，1）→（1，2）→（2，3）→（3，5）→（5，8）→（13，21）→（21，34）→（34，35）→（55，89）→（89，144）→（144，233）→（233，377）→（377，610）→（610，987）→（987，1579）.

因此,所求的 m^2+n^2 的最大值为 $987^2+1597^2=3524578$.

例 8：证明：有无穷多个正整数 n, 使得 $[\sqrt{2}n]$ 是完全平方数.

【证明】因方程 $x^2-2y^2=-1$ ① 有正整数解 $x=y=1$，因此有无穷多组正整数解.任取一组解 u,v, 则 $2v^2=u^2+1$

将上式两边同乘以 u^2，得 $2(uv)^2=u^4+u^2$, 故 $u^2<\sqrt{2}uv<u^2+1$. 所以 $[\sqrt{2}uv]=u^2$ 是一个平方数，即取 $n=uv$ 得出无穷多个符合要求的 n.

例 9：设 a,b,c,d 为正整数，$ab=cd$. 证明：$a^4+b^4+c^4+d^4$ 不是素数.

【证明】由 $ab=cd$,得出 $a=us,b=st,c=vs,d=ut$, 其中 u,v,s,t 都是正整数.

因此 $a^4+b^4+c^4+d^4=(u^4+v^4)(s^4+t^4)$ 不是素数.

例 10：证明：不定方程 $(x+1)^y-x^z=1,x,y,z>1$ ①

仅有一组正整数解 $x=2,y=2$ 及 $z=3$.

【证明】首先，将①模 $x+1$ 化简，得 $(-1)^{z+1}\equiv 1(\mathrm{mod}\, x+1)$, 故 z 是奇数.将①分解为 $(x+1)^{y-1}=x^{z-1}-x^{z-2}+\cdots-x+1$.

易知 x 必须是偶数，否则上式两边的奇偶性不同，类似地，将①变形为 $(x+1)^{y-1}+(x+1)^{y-2}+\cdots+(x+1)+1=x^{z-1}$, 可见 y 也是偶数.

现在记 $x=2x_1,y=2y_1$, 则由①得 $[(x+1)^{y_1}-1][(x+1)^{y_1}+1]=x^z$ ②

因 x 是偶数，故 $(x+1)^{y_1}-1$ 与 $(x+1)^{y_1}+1$ 的最大公约数是 2，又显然有 $x\mid(x+1)^{y_1}-1$，由这些及②推出，必须 $(x+1)^{y_1}-1=2x_1^z,(x+1)^{y_1}+1=2^{z-1}$.

这意味着 $2^{z-1}>2x_1^z$, 故 $x_1=1$，即 $x=2$，所以 $y=2$ 及 $z=3$.

【评述】方程①是著名的卡特郎（*Catalan*）猜想的特殊情形.卡特郎猜想 3^2 与 2^3 是仅有

的一对差为 1 的正整数方幂,即不定方程 $x^a - y^b = 1, a, b > 1$ ③

只有一组正整数解 $x = 3, y = 2, a = 2$ 及 $b = 3$.

例 11：证明：不定方程 $x^4 + y^4 = z^2$ ① 没有正整数解.

【证明】采用反证法，设①有正整数解，我们在所有这样的解中选 取一组使 z 最小的解.论证的想法是由此构造出另一组解 (r, s, t)，使得 $0 < t < z$，由于已选择为最小，这就导出矛盾.

首先,此时必有 $(x, y) = 1$,因设 $d = (x, y)$ 而 $d > 1$,则由①知 $d^4 \mid z^2$，即 $d^2 \mid z$ 所以 $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2})$ 也是①的一组正整数解，但 $\frac{z}{d^2} < z$，这和 z 的选取相违.

将①改写为 $(x^2)^2 + (y^2)^2 = z^2$.

由于 $(x, y) = 1$，故 $(x^2, y^2) = 1$ 于是 (x^2, y^2, z^2) 是一组本源的勾股数.由定理三知，存在整数 $a > b > 0, (a, b) = 1, a, b$ 一奇一偶，使得（不妨设 y 为偶数）

$x^2 = a^2 - b^2, y^2 - 2ab, z = a^2 + b^2.$ ②

由 $x^2 + b^2 = a^2$ 及 $(a, b) = 1$ 知，a 是奇数，b 是偶数.再应用上述定理，存在整数 $p > q > 0, (p, q) = 1, p, q$ 一奇一偶，使得 $x = p^2 - q^2, b = 2pq, a = p^2 + q^2$.

由②得到 $y^2 = 4pq(p^2 + q^2)$, 即 $(\frac{y}{2})^2 = pq(p^2 + q^2)$,

因 $(p, q) = 1$, 易知 $p, q, p^2 + q^2$ 两两互素，上式表明它们的积是整数的平方，故存在正整数 r, s, t 使得 $p = r^2, q = s^2, p^2 + q^2 = t^2$, 从而 $r^4 + s^4 = t^2$.

于是我们得出了①的一组正整数解 (r, s, t). 但 $0 < t\sqrt{p^2 + q^2} = \sqrt{a} < 4\sqrt{z} < z$, 和 z 的最小性矛盾.

【评述 1】由例 10 立即推出,费马方程 $x^n + y^n = z^n, n > 2$, 当 $n = 4$ 时没有正整数解.

【评述 2】例 11 的证明方法,称为无穷递推法,这是费马首先提出的一个重要方法.

采用无穷递降法证明不定方程无正整数解（满足某种限制的解）的主要步骤是：从相反的结论出发，假设存在一组正整数解，设法造出这个方程的另一个正整数解，而新的解比原来的解“严格地小”.这里所谓严格的小，是指某一个与解有关的，取正整数的量严格递减.

如上述过程可以无限地进行下去，则由于严格递减的正整数列只有有限多项，两者产生矛盾.

有一些不定方程需要应用稍深入的同余知识：二次剩余（或称平方剩余）.这里只介绍一个最基本、最常用的结果：

引理　设 p 是 $4k+3$ 型的素数，则 $x^2+1\equiv 0(\bmod p)$　　③

没有整数解.

换句话说,对于素数 x, x^2+1 的素因子或者是 2，或者 $\equiv 1(\bmod 4)$

证明颇简单.假定有 x 满足③，则 $x^2\equiv -1(\bmod p)$，故 $x^{p-1}\equiv(-1)^{\frac{p-1}{2}}(\bmod p)$. 但 $p\nmid x$，于是由费马小定理知，$x^{p-1}\equiv 1(\bmod p)$, 进而 $(-1)^{\frac{p-1}{2}}\equiv 1(\bmod p)$, 即 $-1\equiv 1(\bmod p)$，得 $p=2$，这不可能.

例 12：设 p 是 $4k+3$ 型的素数，n 是正整数且 $p\mid n$. 若 n 可以表示为两个素数的平方和，即存在整数 x, y, 使得　$n=x^2+y^2$ ① 则 n 中 p 的幂次是偶数.

【证明】首先证明 x, y 均被 p 整除.假设不然，可设 $p\nmid x$，则有整数 x_1，使 $xx_1\equiv 1(\bmod p)$. 以 x_1^2 乘①的两边，再模 p，得出（注意到 $p\mid n$）

$(x_1 y)^2+1\equiv 0(\bmod p)$.

因 $p\equiv 3(\bmod 4)$，这与引理矛盾，故 $p\mid(x, y)$. 设 $p^a \parallel (x, y)$, 则 $p^{2a}\mid n$. 我们证明 $p^a\parallel n$，即 n 中 p 的幂次是偶数.

记 $n=p^{2\alpha}m, x=p^{\alpha}x_1, y=p^{\alpha}y_1$, 则 m, x_1, y_1 都是整数，且 $p\nmid(x_1, y_1)$. 由①得 $m=x_1^2+y_1^2$.

假设 $p\mid m$，则由上述相同的论证表明 $p\mid(x_1, y_1)$，导出矛盾，这就证明了本题的断言.

【评述】例 12 的论证表明：如设 p 是 $4k+3$ 型的素数，若有整数 x, y 使得 $x^2+y^2\equiv 0(\bmod p)$　　则 x, y 均被 p 整除.

例 13：证明：方程 $y^2=x^3-5$　　①

没有整数解.

【证明】首先,若 x 是偶数，将①模 4 得 $y^2 \equiv 3(\bmod 4)$，此不可能.若 x 是奇数，当 $x \equiv 3(\bmod 4)$ 时，由①得 $y^2 \equiv 2(\bmod 4)$，仍不可能.故 $x \equiv 1(\bmod 4)$，于是 $x^2+x+1 \equiv 3(\bmod 4)$，仍不可能.故 $x \equiv 1(\bmod 4)$，于是 $x^2+x+1 \equiv 3(\bmod 4)$，因此 x^2+x+1 必有一个 $4k+3$ 型的素因子 p，将①变形为

$$y^2=(x-1)(x^2+x+1)-4 \qquad ①$$

并模 p，得 $y^2+2^2 \equiv 0(\bmod p)$.由例 12 评述可知，必有 $p \mid (2, y)$,即 $p=2$，这不可能.故方程①没有整数解.

【评述 1】上面的论证中，先用同余导出了（有解的）某些必要条件，目的是为了使①的右边产生 $4k+3$ 型的素因子，以应用引理或例 12 评述中的事实.

【评述 2】任一个 $\equiv 3(\bmod 4)$ 的整数必有 $4k+3$ 型的素因子.这一简单的结论在这一类论证中最为有用.