同余在数学竞赛中的应用

邹　明

（山东省青岛二中，266104）

中图分类号：O156.1　　文献标识码：A　　文章编号：1005－6416(2013)11－0005－04

（本讲适合高中）

同余是数论的重要概念，其性质及相关重要定理是解决数论问题的重要工具. 本文给出同余的定义与定理，并举例说明其应用.

1　定义与定理

定义 1　若整数 a、b 除以整数 $m(m>1)$ 的余数相同，则称 a、b 模 m 同余，记为

$a\equiv b(\bmod m)$.

定义 2　设 $m>1,(a,m)=1$. 若整数 c $(1\leqslant c\leqslant m-1)$ 使得 $ac\equiv 1(\bmod m)$，则称 c 为 a 对模 m 的逆或倒数，记为

$c\equiv a^{-1}(\bmod m)$，且 $(a^{-1},m)=1$.

费马小定理　设 p 是素数. 则对任意的正整数 a 有 $a^p\equiv a(\bmod p)$.

特别地，当 $(p,a)=1$ 时，$a^{p-1}\equiv 1(\bmod p)$.

威尔逊定理　设 p 是大于 1 的整数. 则

p 是素数 $\Leftrightarrow (p-1)!\equiv -1(\bmod p)$.

欧拉定理　设正整数 a、m 满足 $m>1$，且 $(a,m)=1$. 则 $a^{\varphi(m)}\equiv 1(\bmod m)$.

定义 3　设 $(a,m)=1$，d_0 是使

$a^d\equiv 1(\bmod m)$

的最小正整数. 则 d_0 称为 a 对于模 m 的阶，记为 $\delta_m(a)=d_0$.

2　应用

例 1　求 $10^{10^{\cdots^{10}}}$（100 个 10）被 7 除所得的余数.

解　$10^{10^{\cdots^{10}}}\equiv(7+3)^{10^{\cdots^{10}}}\equiv 3^{10^{\cdots^{10}}}$

$\equiv(7+2)^{50\cdots0}\equiv 2^{5\times 10^9}\equiv 2^{3\times 166\cdots6+2}$

$\equiv 4(7+1)^{166\cdots6}\equiv 4(\bmod 7)$.

收稿日期：2013－08－19

例 2　证明：对任意的正整数 n，均有

$13\mid\sum_{k=0}^{n}2\,012^k(-1)^kC_{2n+1}^{2k+1}$.

证明　由 $-2\,012\equiv 3\equiv 4^2(\bmod 13)$，得

$8\sum_{k=0}^{n}2\,012^k(-1)^kC_{2n+1}^{2k+1}$

$\equiv 2\sum_{k=0}^{n}4^{2k+1}C_{2n+1}^{2k+1}$

$\equiv(1+4)^{2n+1}-(1-4)^{2n+1}$

$\equiv 5^{2n+1}+3^{2n+1}\equiv 5^{2n+1}-10^{2n+1}$

$\equiv 5^{2n+1}(1-2^{2n+1})(\bmod 13)$.

因为 $2^{12}\equiv 1(\bmod 13)$，所以，

$2^{2(n+6)+1}\equiv 2^{2n+1}(\bmod 13)$.

验证知当 $n=0,1,\cdots,5$ 时，$13\nmid(2^{2n+1}-1)$.

所以，$13\mid\sum_{k=0}^{n}2\,012^k(-1)^kC_{2n+1}^{2k+1}$.

例 3　**卢卡斯（Lucas）定理**　设 p 为素数，$a,b\in\mathbf{N}_+$，整数 a_i、b_i 满足 $0\leqslant a_i,b_i\leqslant p-1$ $(i=0,1,\cdots,k)$，且

$a=a_kp^k+a_{k-1}p^{k-1}+\cdots+a_1p+a_0$，

$b=b_kp^k+b_{k-1}p^{k-1}+\cdots+b_1p+b_0$.

则 $C_a^b\equiv C_{a_k}^{b_k}C_{a_{k-1}}^{b_{k-1}}\cdots C_{a_0}^{b_0}(\bmod p)$.

证明　由 p 为素数，知对 $j(1\leqslant j\leqslant p-1)$，有 $C_p^j=\frac{p}{j}C_{p-1}^{j-1}\equiv 0(\bmod p)$.

故 $(1+x)^p=1+C_p^1x+\cdots+C_p^{p-1}x^{p-1}+x^p$

$\equiv 1+x^p(\bmod p)$.

由此得

$(1+x)^a=(1+x)^{a_0}(1+x)^{a_1p}\cdots(1+x)^{a_kp^k}$

$\equiv(1+x)^{a_0}(1+x^p)^{a_1}\cdots(1+x^{p^k})^{a_k}(\bmod p)$.

比较 x^b 项的系数得

$C_a^b\equiv C_{a_k}^{b_k}C_{a_{k-1}}^{b_{k-1}}\cdots C_{a_0}^{b_0}(\bmod p)$.

推论1 当且仅当存在 $i\in\{0,1,\cdots,k\}$ 使得 $b_i>a_i$ 时，$C_a^b\equiv0(\mathrm{mod}\ p)$.

推论2 当且仅当 a 在二进制表示下的每一个数位上的数均不小于 b 的相应数位上的数时，C_a^b 为奇数.

例4 求 $2\,013^{2\,013^{2\,013}}$ 的末三位数.

解 注意到，

$2\,013\equiv3(\mathrm{mod}\ 5)$，$2\,013^2\equiv-1(\mathrm{mod}\ 5)$，

$2\,013^4\equiv1(\mathrm{mod}\ 5)$，$2\,013\equiv13(\mathrm{mod}\ 25)$，

$2\,013^2\equiv-6(\mathrm{mod}\ 25)$，$2\,013^4\equiv11(\mathrm{mod}\ 25)$，

$2\,013^8\equiv-4(\mathrm{mod}\ 25)$，$2\,013^{12}\equiv6(\mathrm{mod}\ 25)$，

$2\,013^{20}\equiv1(\mathrm{mod}\ 25)$.

因为 $2\,013\equiv1(\mathrm{mod}\ 4)$，$2\,013^{20}\equiv1(\mathrm{mod}\ 4)$，所以，$2\,013^{20}\equiv1(\mathrm{mod}\ 100)$.

故 $2\,013^{2\,013}\equiv2\,013^{20\times100+13}\equiv2\,013^{13}\equiv13^{13}$

$\equiv(10+3)^{13}\equiv10C_{13}^{12}\cdot3^{12}+3^{13}$

$\equiv3^{12}\times133\equiv(80+1)^3\times33\equiv241\times33$

$\equiv41\times33\equiv53(\mathrm{mod}\ 100)$.

由 $2\,013^{20}\equiv13^{20}\equiv(10+3)^{20}$

$\equiv C_{20}^{19}\cdot10\times3^{19}+3^{20}\equiv3^{19}\times203$

$\equiv(3^5)^3\times3^4\times78$

$\equiv-7^3\times81\times78\equiv51(\mathrm{mod}\ 125)$，

得 $2\,013^{40}\equiv(1+50)^2\equiv101(\mathrm{mod}\ 125)$，

$2\,013^{80}\equiv(1+100)^2\equiv-49(\mathrm{mod}\ 125)$.

故 $2\,013^{100}\equiv1(\mathrm{mod}\ 125)$.

由 $2\,013\equiv5(\mathrm{mod}\ 8)$，$2\,013^2\equiv1(\mathrm{mod}\ 8)$，

得 $2\,013^{100}\equiv(\mathrm{mod}\ 1\,000)$.

由 $2\,013^{2\,013}=100k+53$，得

$2\,013^{2\,013^{2\,013}}\equiv2\,013^{100k+53}\equiv2\,013^{53}$

$\equiv(2\,000+13)^{53}\equiv13^{53}\equiv(10+3)^{53}$

$\equiv C_{53}^2\cdot10^2\times3^{51}+C_{53}^1\cdot10\times3^{52}+3^{53}$

$\equiv3^{51}\times399(\mathrm{mod}\ 1\,000)$.

又 $3^7\equiv187(\mathrm{mod}\ 1\,000)$，

$3^{10}\equiv187\times27\equiv49(\mathrm{mod}\ 1\,000)$，

$3^{17}\equiv187\times49\equiv163(\mathrm{mod}\ 1\,000)$，

$3^{51}\equiv163^3\equiv747(\mathrm{mod}\ 1\,000)$，

所以，$3^{51}\times399\equiv53(\mathrm{mod}\ 1\,000)$.

综上，所求末三位数为053.

例5 求所有奇素数 p，使得 $p\mid\sum_{k=1}^{103}k^{p-1}$.

解 若 $p>103$，则对 $1\leqslant k\leqslant103$，有

$k^{p-1}\equiv1(\mathrm{mod}\ p)$，

$\sum_{k=1}^{103}k^{p-1}\equiv103(\mathrm{mod}\ p)$.

故 $p\leqslant103$.

设 $103=pq+r(0\leqslant r<p)$，即在 $1\sim103$ 中共有 q 个数是 p 的倍数. 所以，

$\sum_{k=1}^{103}k^{p-1}\equiv103-q\equiv pq+r-q$

$\equiv r-q\equiv0(\mathrm{mod}\ p)$

$\Leftrightarrow r\equiv q(\mathrm{mod}\ p)$.

若 $p>q$，则 $r=q$，$103=pq+r=(p+1)r$.

由103为素数，得 $p=102$，$r=1$，矛盾.

若 $p\leqslant q$，则

$103=pq+r\geqslant p^2\Rightarrow p=3,5,7$.

当 $p=3$ 时，$q=34\equiv1=r(\mathrm{mod}\ 3)$；

当 $p=5$ 时，$q=20\equiv2(\mathrm{mod}\ 3)$，$2\neq r=3$；

当 $p=7$ 时，$q=14\equiv2(\mathrm{mod}\ 3)$，$2\neq r=5$.

故 $p=3$ 为所求.

例6 求所有的素数 p，使得

$$p^3\mid\sum_{k=1}^{p-1}(C_p^k)^2.$$

解 显然，$p\neq2,3$.

当 $p\geqslant5$ 时，注意到，

$p-1\equiv-1(\mathrm{mod}\ p)$，

$p-2\equiv-2(\mathrm{mod}\ p)$，

……

$k\equiv k-p(\mathrm{mod}\ p)(k=1,2,\cdots,p)$.

将各式相乘得

$$\frac{(p-1)!}{(k-1)!}\equiv\pm(p-k)!(\mathrm{mod}\ p),$$

即 $C_{p-1}^{k-1}\equiv\pm1(\mathrm{mod}\ p)$.

对于 $k(1\leqslant k\leqslant p-1)$，存在 $r_k(1\leqslant r_k\leqslant p-1)$，使得 $kr_k\equiv1(\mathrm{mod}\ p)$，且当 k 取遍 $1,2,\cdots,p-1$ 时，r_k 也取遍 $1,2,\cdots,p-1$.

又 $C_p^k=\frac{p}{k}C_{p-1}^{k-1}$，得

$$p^3\mid\sum_{k=1}^{p-1}(C_p^k)^2\Leftrightarrow p\mid\sum_{k=1}^{p-1}\frac{(C_{p-1}^{k-1})^2}{k^2}.$$

而 $\sum_{k=1}^{p-1}\frac{(C_{p-1}^{k-1})^2}{k^2}\equiv\sum_{k=1}^{p-1}\frac{(C_{p-1}^{k-1})^2}{k^2}(kr_k)^2$

$$\equiv\sum_{k=1}^{p-1} r_k^2\equiv\sum_{k=1}^{p-1} k^2$$

$$\equiv\frac{p(p-1)(2p-1)}{6}(\mathrm{mod}\ p).$$

当素数 $p\geqslant 5$ 时,由

$(p-1)(2p-1)\equiv 1-p^2\equiv 0(\mathrm{mod}\ 3)$,

得 $6\mid(p-1)(2p-1)$.

因此,$p\left|\sum_{k=1}^{p-1}\frac{(C_{p-1}^{k-1})^2}{k^2}\right.$.

故所有不小于 5 的素数为所求.

例 7 求所有的素数对 (p,q),使得

$pq\mid(p^p+q^q+1)$.

解 若 $p=q$,则 $p^2\nmid(2p^p+1)$.

不妨设 $p<q$.

若 $p=2$,由

$2q\mid(q^q+5)\Rightarrow q\mid 5\Rightarrow q=5$.

所以,$(p,q)=(2,5)$.

当 p、q 均为奇素数时,由

$pq\mid(p^p+q^q+1)\Rightarrow p^p\equiv -1(\mathrm{mod}\ q)$

$\Rightarrow p^{2p}\equiv 1(\mathrm{mod}\ q)\Rightarrow \delta_q(p)\in\{2,2p\}$.

若 $\delta_q(p)=2$,则

$p^2\equiv 1(\mathrm{mod}\ q)\Rightarrow p\equiv 1(\mathrm{mod}\ q)(p<q)$

$\Rightarrow p=1$,

矛盾.

于是,$\delta_q(p)=2p$.

由 $p^{q-1}\equiv 1(\mathrm{mod}\ q)\Rightarrow 2p\mid(q-1)$

$\Rightarrow q\equiv 1(\mathrm{mod}\ p)$.

但 $0\equiv p^p+q^q+1\equiv 2(\mathrm{mod}\ p)$,矛盾.

综上,$(p,q)=(2,5),(5,2)$.

例 8 证明:方程

$x^{2\,014}=4y^{2\,013}+4y^{2\,012}+2\,011y+2\,010$

无整数解.

证明 先证明一个引理.

引理 若 x 是任意整数,则 x^2+1 的每个奇素因子为 $4k+1$ 型.

证明 设 p 为 x^2+1 的一个奇素因子,即 $p\mid(x^2+1)$. 则 $(p,x)=1$,且 $x^2\equiv -1(\mathrm{mod}\ p)$.

所以,$(x^2)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}}\equiv x^{p-1}\equiv 1(\mathrm{mod}\ p)$.

从而,$\frac{p-1}{2}=2k(k\in\mathbf{N}_+)$,即 $p=4k+1$.

回到原题.

原方程即

$x^{2\,014}+1=4y^{2\,013}+4y^{2\,012}+2\,011y+2\,011$

$=(y+1)(4y^{2\,012}+2\,011)$.

由 $x^{2\,014}+1$

$=(x^2+1)[(x^2)^{1\,006}-(x^2)^{1\,005}+\cdots+(x^2)^2-(x^2)+1]$,

且 $(x^2)^{1\,006}-(x^2)^{1\,005}+\cdots+(x^2)^2-(x^2)+1\equiv 1(\mathrm{mod}\ 4)$,

但 $4y^{2\,012}+2\,011\equiv 3(\mathrm{mod}\ 4)$,矛盾.

故原方程无整数解.

例 9 求与数列 $\{a_n\}$ 满足

$a_n=2^n+3^n+6^n-1(n\in\mathbf{Z}_+)$

中所有项均互素的所有正整数.

解 显然,$(1,a_n)=1$.

设 $m(m>1)$ 是与 $\{a_n\}$ 中所有项均互素的正整数,p 为 m 的一个素因数.

若 $p>3$,则由费马小定理得

$2^{p-1}\equiv 1(\mathrm{mod}\ p)$,$3^{p-1}\equiv 1(\mathrm{mod}\ p)$,

$6^{p-1}\equiv 1(\mathrm{mod}\ p)$.

记 $2^{p-1}=mp+1$,$3^{p-1}=np+1$,

$6^{p-1}=tp+1(m,n,t\in\mathbf{Z}_+)$.

则 $a_{p-2}=2^{p-2}+3^{p-2}+6^{p-2}-1$

$=\frac{mp+1}{2}+\frac{np+1}{3}+\frac{tp+1}{6}-1$

$=\frac{3mp+2np+tp}{6}=p\cdot\frac{3m+2n+t}{6}$.

因为 a_{p-2} 为整数,$(p,6)=1$,所以,

$6\mid(3m+2n+t)$,$p\mid a_{p-2}$.

这与 $(m,a_{p-2})=1$ 矛盾.

若 $p=2$ 或 3,则 $a_2=48=2^4\times 3\Rightarrow p\mid a_2$,也矛盾.

故与数列 $\{a_n\}$ 中所有项均互素的正整数只有 1.

例 10 证明:不存在正整数 k、m,使得

$k!+48=48(k+1)^m$. ①

证明 (1)若 $k+1$ 为合数,则

$(k+1)\mid k!$,$(k+1)\mid 48$.

由 $48\mid k!\Rightarrow k\geqslant 6\Rightarrow k=7,11,23,47$,

检验知均非解.

(2)若 $k+1$ 为素数,由威尔逊定理知

$k!\equiv -1(\bmod k+1) \Rightarrow (k+1)\mid(k!+1)$.

又由式①得$(k+1)\mid 47 \Rightarrow k=46$.

于是,方程为

$$46!+48=48\times 47^m \Rightarrow \frac{46!}{48}+1=47^m.$$

两边取模4得 $1\equiv(-1)^m(\bmod 4)$.

所以,m 为偶数. 令 $m=2m_1$.

则$(47^{m_1}+1)(47^{m_1}-1)=\frac{46!}{48}$.

由 $23^2\mid\frac{46!}{48}$,$47^{m_1}+1\equiv 2(\bmod 23)$,得

$23^2\mid(47^{m_1}-1)$.

因为$47^{m_1}=(46+1)^{m_1}\equiv 46m_1+1(\bmod 23^2)$,所以,

$23^2\mid(47^{m_1}-1)\Leftrightarrow 23^2\mid 46m_1\Leftrightarrow 23\mid m_1$.

则 $m=2m_1\geqslant 46$,

$48\times 47^m\geqslant 48\times 47^{46}>48\times 46!>46!+48$,矛盾.

综上,不存在正整数 k、m 满足式①.

练 习 题

1. 证明:对任意的正整数 n,$3^n+2\times 17^n$ 不是5的倍数,并求最小的正整数 n,使得

$11\mid(3^n+2\times 17^n)$.

提示:注意到,

$3^{2k}+2\times 17^{2k}\equiv(-1)^k+2\times 2^{2k}$

$\equiv 3(-1)^k(\bmod 5)$,

$3^{2k+1}+2\times 17^{2k+1}\equiv 3(-1)^k+4(-1)^k$

$\equiv 2(-1)^k(\bmod 5)$.

故 $3^n+2\times 17^n$ 不是5的倍数.

又 $3^n+2\times 17^n\equiv 3^n+2\times 6^n$

$\equiv 3^n(1+2^{n+1})\equiv 0(\bmod 11)$

$\Leftrightarrow 11\mid(1+2^{n+1})$,

故 $n_{\min}=4$.

2. 对任意的正整数 $n(n\geqslant 1)$,b 的素因数均大于 n. 证明:

$n!\mid a(a+b)(a+2b)\cdots[a+(n-1)b]$.

提示:因为 b 的素因数均大于 n,所以,

$(b,n!)=1$,$bb^{-1}\equiv 1(\bmod n!)$,

$(b^{-1})^n a(a+b)(a+2b)\cdots[a+(n-1)b]$

$\equiv(ab^{-1})(ab^{-1}+1)(ab^{-1}+2)\cdots[ab^{-1}+(n-1)]$

$\equiv 0(\bmod n!)$.

又$(b^{-1},n!)=1$,则

$n!\mid a(a+b)(a+2b)\cdots[a+(n-1)b]$.

3. 已知 p 为素数. 证明:存在一个素数 q,使得对任意的正整数 n,$q\nmid(n^p-p)$.

提示:因为

$$\frac{p^p-1}{p-1}=p^{p-1}+\cdots+p^2+p+1\equiv p+1(\bmod p^2),$$

所以,$\frac{p^p-1}{p-1}$ 中至少有一个素因子 q(即 $q\mid(p^p-1)$)满足 $p^2\nmid(q-1)$.

若存在正整数 n 使得 $n^p\equiv p(\bmod q)$,则

$n^{p^2}\equiv p^p\equiv 1(\bmod q)$.

由费马小定理得 $n^{q-1}\equiv 1(\bmod q)$.

由 $p^2\nmid(q-1)\Rightarrow(p^2,q-1)\mid p$.

所以,$n^p\equiv 1(\bmod q)$.

又 $n^p\equiv p(\bmod q)$,故

$p\equiv 1(\bmod q)$,

$1+p+p^2+\cdots+p^{p-1}\equiv p(\bmod q)$.

由 q 是 $1+p+p^2+\cdots+p^{p-1}$ 的一个素因子,知 $p\equiv 0(\bmod q)$,与 $p\equiv 1(\bmod q)$ 矛盾.

4. 已知 p 为奇素数. 证明:

$$\sum_{k=1}^{p-1}k^{2p-1}\equiv\frac{p(p+1)}{2}(\bmod p^2).$$

提示:由 $p-1$ 为偶数得

$$\sum_{k=1}^{p-1}k^{2p-1}=\sum_{k=1}^{\frac{p-1}{2}}[k^{2p-1}+(p-k)^{2p-1}].$$

注意到,

$k^{2p-1}+(p-k)^{2p-1}$

$=p^{2p-1}-C_{2p-1}^1p^{2p-2}k+\cdots+C_{2p-1}^{2p-2}pk^{2p-2}$

$\equiv C_{2p-1}^1pk^{2p-2}\equiv -pk^{2p-2}(\bmod p^2)$.

由费马小定理知 $k^{p-1}\equiv 1(\bmod p)$.

故 $k^{2p-2}\equiv 1(\bmod p)\Rightarrow k^{2p-2}=pm+1$

$\Rightarrow pk^{2p-2}=-p(pm+1)\equiv -p(\bmod p^2)$.

故$\sum_{k=1}^{p-1}k^{2p-1}\equiv\sum_{k=1}^{\frac{p-1}{2}}(-p)\equiv -\frac{p(p-1)}{2}$

$\equiv p^2-\frac{p(p-1)}{2}\equiv\frac{p(p+1)}{2}(\bmod p^2)$.