从阶与原根谈起

武炳杰

（复旦大学数学科学学院09级，200433）

中图分类号：O156　　文献标识码：A　　文章编号：1005-6416(2012)01-0006-05

（本讲适合高中）

整除与同余问题一直是数学竞赛的热点与难点．本文旨在从阶出发，用原根串起一系列性质与定理，以此来解决近年来一些国内外的数学竞赛题．

定义1　设 $m\geqslant1,(a,m)=1$，使得

$a^x\equiv1(\bmod m)$

成立的最小正整数 x 称为 a 关于模 m 的阶（或指数），并用 $\operatorname{ord}_m(a)$ 表示．

定理1　对于正整数 x，

$\operatorname{ord}_m(a)\mid x\Leftrightarrow a^x\equiv1(\bmod m)$．

推论1　$\operatorname{ord}_m(a)\mid\varphi(m)$，其中，$\varphi(m)$ 是欧拉函数，表示小于 m 且与 m 互质的正整数的个数．

推论2　若 $a^{k_1}\equiv1(\bmod m),a^{k_2}\equiv1(\bmod m)$，则 $a^{(k_1,k_2)}\equiv1(\bmod m)$．

下面是两道利用以上性质解决的典型数论问题．

例1　对于质数 p，若对无限多个正整数 k，存在一个正整数数列 $n_1,n_2,\cdots,n_k$ 满足：

(1)当 $i=1,2,\cdots,k$ 时，$n_i\geqslant\frac{p+1}{2}$；

(2)当 $i=1,2,\cdots,k$ 时，$p^{n_i}-1$ 是 n_{i+1} 的倍数，且 $\frac{p^{n_i}-1}{n_{i+1}}$ 与 n_{i+1} 互质，$n_{k+1}=n_1$，且对于 $k=1$ 不成立．

此时，称 p 是“漂亮质数”．

证明：2不是漂亮质数，但所有奇质数是漂亮质数．[1]

（第23届韩国数学奥林匹克(2010)）

【分析】可以利用阶的极小性通过设出最小质因子产生矛盾来解决此问题．

证明　显然，$n_i\geqslant3$ 且均为奇数．

记 $q(q\geqslant3)$ 是 $n_1n_2\cdots n_k$ 的最小质因子，不妨设 $q\mid n_2$．

由推论1知 $\operatorname{ord}_q(2)\mid(q-1)$，故

$\operatorname{ord}_q(2)<q$．

但由 $q\mid(2^{n_1}-1)$ 及定理1得

$\operatorname{ord}_q(2)\mid n_1$，

这与 q 的最小性矛盾．

所以，2不是漂亮质数．

证明“所有奇质数是漂亮质数”略．

例2　是否存在 $n\in\mathbf{N}_+$，使得

$103\mid n,2^{2n+1}\equiv2(\bmod n)$

成立？[2]

（2010，印度国家队选拔考试）

【分析】注意到，103是质数，可以通过费马小定理来找出一些有关 $2n$ 的性质．

解　不存在．

若存在，由费马小定理得

$2^{102}\equiv1(\bmod 103)$．

而由题意及推论2知

$2^{2n}\equiv1(\bmod 103)$，

$2^{(102,2n)}\equiv1(\bmod 103)$．

注意到，$102=2\times3\times17$，且当

$(102,2n)=2,3,6$

时，经检验知不正确．

所以，$17\mid(102,2n)$．从而，$17\mid n$．

进一步有 $2^{2n}\equiv1(\bmod 17)$．

而由费马小定理知

$2^{16}\equiv1(\bmod 17)$．

收稿日期：2011-08-03　修回日期：2011-11-24

则再由推论 2 知

$$2^{(2n,16)}\equiv 1(\bmod 17).$$

同理，由于 2^2、$2^4\not\equiv 1(\bmod 17)$，则必有 $8\mid(2n,16)$，进一步知 $4\mid n$，得

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

矛盾.

下面引入原根.

事实上，它是某些剩余系的本质刻画.

定义 2　若 $\mathrm{ord}_m(a)=\varphi(m)$，则将 a 称作模 m 的一个原根.

定理 2（原根定理）　若 p 是奇质数，则模 p 的原根是存在的.

证明　设模 p 的简化剩余系 $\{1,2,\cdots,p-1\}$ 中元素模 p 阶的集合为 $\{\gamma_1,\gamma_2,\cdots,\gamma_r\}$，取其最小公倍数 $\gamma=[\gamma_1,\gamma_2,\cdots,\gamma_r]$.

下面证明有一根 g，其阶为 γ 且 $\gamma=p-1$.

作标准质因数分解

$$\gamma=q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_k^{\alpha_k}.$$

由最小公倍数的性质，知对每个 $s(1\leqslant s\leqslant k)$ 有一个 $\gamma_i=aq_s^{\alpha_s}$，而有一整数 x 的阶为 γ_i，取 $x_s=x^a$.

易知，$\mathrm{ord}_p(x^a)=q_s^{\alpha_s}$.

故剩余系中存在 k 个数 $x_1',x_2',\cdots,x_k'$，模 p 的阶分别为 $q_i^{\alpha_i}(i=1,2,\cdots,k)$.

于是，令 $g=x_1'x_2'\cdots x_k'$.

注意到，阶函数的可乘性，即若

$$(\mathrm{ord}_p(m),\mathrm{ord}_p(n))=1,$$

则　$\mathrm{ord}_p(mn)=\mathrm{ord}_p(m)\cdot\mathrm{ord}_p(n)$.

所以，$\mathrm{ord}_p(g)=\gamma$.

另一方面，因为 $1,2,\cdots,p-1$ 中任一数的阶均在 $\{\gamma_1,\gamma_2,\cdots,\gamma_r\}$ 中出现过，所以，$x^\gamma\equiv 1(\bmod p)$ 对 $x=1,2,\cdots,p-1$ 成立. 于是，至少有 $p-1$ 个解. 而 $x^n\equiv 1(\bmod p)$ 不可能有超过 n 个不同的解，否则设

$$x\equiv\alpha_i(\bmod p)\ (i=1,2,\cdots,n+1),$$

$$x^n-1\equiv c(x-\alpha_1)\cdots(x-\alpha_n)(\bmod p),$$

其中，c 是常数，且 $p\nmid c$.

将 $x=\alpha_{n+1}$ 代入知

$$0\equiv c(\alpha_{n+1}-\alpha_1)\cdots(\alpha_{n+1}-\alpha_n)(\bmod p).$$

因此，一定有一个 $j(1\leqslant j\leqslant n)$，使得

$$\alpha_{n+1}\equiv\alpha_j(\bmod p),$$

这与有 $n+1$ 个不同解矛盾.

所以，$\gamma\geqslant p-1$.

而由定理 1 及最小公倍数的性质，知 $\gamma\mid(p-1)$，故 $\gamma=p-1$，即

$$\mathrm{ord}_p(g)=p-1.$$

下面给出一个原根作为循环群生成元的直接运用的例子，即解高阶同余方程.

例 3　已知 $x\in\mathbf{N}_+$，若 $x^7\equiv 1(\bmod 29)$，求 x 模 29 的值.

解　易验证 2 为模 29 的原根.

因为 $x^7\equiv 1(\bmod 29)$ 至多有 7 个解，而检验知 2^4、2^8、2^{12}、2^{16}、2^{20}、2^{24}、2^{28} 恰好为方程不同的解，所以，方程恰好是这 7 个解，所求即为前面 7 个数模 29 的值.

下面再给出一个利用原根阶的特殊性来解决整除问题的例子.

例 4　设 $n(n\geqslant 2)$ 为正整数. 证明：

$$n\left|\left(\sum_{k=1}^{n-1}k^{n-1}+1\right)\right.\Leftrightarrow\text{对 } n \text{ 的任意质因数 } p,$$

$$p\left|\left(\frac{n}{p}-1\right),(p-1)\right|\left(\frac{n}{p}-1\right).$$ [3]

（2005，丝绸之路数学竞赛）

证明　设 $n=Ap$（p 为质数）.

若 $(p-1)\mid(n-1)$，由费马小定理易知

$$\sum_{k=1}^{n-1}k^{n-1}\equiv(n-1)-(A-1)\equiv -A(\bmod p).$$

若 $(p-1)\nmid(n-1)$，由定理 2 知可取 p 的一个原根 r.

由 $(r,p)=1$，知 $\{r,2r,\cdots,(p-1)r\}$ 仍是一个模 p 的简化剩余系. 故

$$\sum_{k=1}^{p-1}k^{n-1}\equiv\sum_{k=1}^{p-1}(rk)^{n-1}\equiv r^{n-1}\sum_{k=1}^{p-1}k^{n-1}(\bmod p).$$

因为 $(p-1)\nmid(n-1)$，则由定理 1 知

$$r^{n-1}\not\equiv 1(\bmod p).$$

所以，$\sum\limits_{k=1}^{p-1}k^{n-1}\equiv 0(\bmod p)$.

同理，$\sum\limits_{k=(s-1)p+1}^{sp-1}k^{n-1}\equiv 0(\bmod p)\ (s=2,3,\cdots,A)$.

累和得$\sum_{k=1}^{n-1}k^{n-1}\equiv 0 \pmod p$.

综上,当$n \left| \left(\sum_{k=1}^{n-1}k^{n-1}+1\right)\right.$成立时,

要么$(p-1)\mid(n-1)$,$p\mid(-A+1)$;

要么$(p-1)\nmid(n-1)$,$p\mid 1$.

第二种情形显然不可能.

所以,只有$(p-1)\mid(n-1)$,$p\mid(A-1)$.

而$n-1=(p-1)A+(A-1)$,故

$(p-1)\mid(A-1)$,$p\mid(A-1)$.

反过来,若

$p\mid(A-1) \Rightarrow p\nmid A \Rightarrow p^2\nmid n$,

又$(p-1)\mid(A-1)$

$\Rightarrow (p-1)\mid(A-1)p=n-1-(p-1)$

$\Rightarrow (p-1)\mid(n-1)$,

从而,$\sum_{k=1}^{n-1}k^{n-1}+1\equiv 1-A\equiv 0 \pmod p$.

因为$p^2\nmid n$及p的任意性,所以,

$n \left| \left(\sum_{k=1}^{n-1}k^{n-1}+1\right)\right.$.

事实上,利用原根还能很好地去理解二次剩余中的问题.

定义3 定义勒让德符号$\left(\frac{a}{p}\right)$:

(1)当$p\mid a$时,$\left(\frac{a}{p}\right)=0$.

(2)当$(p,a)=1$时,若$x^2\equiv a \pmod p$在简化剩余系中有解,则$\left(\frac{a}{p}\right)=1$,并称$a$为$p$的二次剩余;

若$x^2\equiv a \pmod p$无解,则$\left(\frac{a}{p}\right)=-1$,并称$a$为$p$的二次非剩余.

引理 设p是一个奇质数.则恰有$\frac{p-1}{2}$个模p的二次剩余,且恰有$\frac{p-1}{2}$个模p的二次非剩余.

例5 求有序整数对(a,b)的个数,使得

$x^2+ax+b=167y$

有整数解(x,y),其中,$1\leqslant a$、$b\leqslant 2\,004$.[4]

(2004,新加坡数学奥林匹克)

【分析】类似于一般的二次方程问题,可以通过配方化为二次剩余的问题.

解 若$x^2+ax+b\equiv 0 \pmod{167}$,则配方得

$a^2-4b\equiv(2x+a)^2 \pmod{167}$.

因此,固定a后,a^2-4b是模167的二次剩余.

故由引理知,b可取$\frac{167-1}{2}+1=84$个模167的值.

而$\frac{2\,004}{167}=12$,则每个a对应84×12个b,共有

$2\,004\times 84\times 12=2\,020\,032$

个有序整数解.

由引理能引出重要的欧拉准则.

定理3(欧拉准则) 设p为奇质数.则

$a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right) \pmod p$.

证明 取p的一个原根为g,故剩余系$\{1,2,\cdots,p-1\}$可表示为

$\{g,\cdots,g^{p-2},g^{p-1}=1\}$.

而由引理知恰好有$\frac{p-1}{2}$个二次剩余.

注意到,$g^{2k}\left(1\leqslant k\leqslant\frac{p-1}{2}\right)$的指数为偶数,一定是二次剩余.故恰好是$g$的所有偶数次幂为二次剩余,奇数次幂为二次非剩余.

于是,当$\left(\frac{a}{p}\right)=1$时,

$a^{\frac{p-1}{2}}\equiv(g^{2k})^{\frac{p-1}{2}}\equiv 1 \pmod p$;

当$\left(\frac{a}{p}\right)=-1$时,

$a^{\frac{p-1}{2}}\equiv(g^{2k+1})^{\frac{p-1}{2}}\equiv g^{\frac{p-1}{2}}\equiv -1 \pmod p$.

最后一式是由于

$g^{p-1}\equiv 1 \pmod p \Rightarrow g^{\frac{p-1}{2}}\equiv \pm 1 \pmod p$,

而g为原根且阶为$p-1$,所以,只能

$g^{\frac{p-1}{2}}\equiv -1 \pmod p$.

正是由于模 p 的每个二次剩余能由 p 的一个原根的幂刻画，因此，很容易发现勒让德符号具有可乘性.

例 6 设 p 是满足 $p\equiv 1 \pmod 4$ 的奇质数. 计算 $\sum_{k=1}^{p-1}\left\{\frac{k^2}{p}\right\}$ 的值（$\{x\}=x-[x]$，$[x]$ 表示不超过实数 x 的最大整数）.[5]

（第 5 届中国香港数学奥林匹克（2002））

【分析】首先利用前面叙述的二次剩余的性质求出分子所有的可能值，再利用取小数函数的性质，将和为整数的配成一对，求出对数即可.

解 因为 $p\equiv 1 \pmod 4$，由定理 3 知

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}\equiv 1 \pmod p,$$

所以，-1 是模 p 的二次剩余.

由 $\left(\frac{-b}{p}\right)=\left(\frac{b}{p}\right)\left(\frac{-1}{p}\right)$，知 b 为二次剩余的充要条件为 $p-b$ 也是二次剩余. 而由引理，知所有二次剩余为 $\left\{1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2\right\}$，故在模 p 的意义下，此集合等价于

$$\{a_1,p-a_1,\cdots,a_{\frac{p-1}{4}},p-a_{\frac{p-1}{4}}\}.$$

当 $1\leqslant a_i$、$p-a_i<p$ 时，

$$\left\{\frac{a_i}{p}\right\}+\left\{\frac{p-a_i}{p}\right\}=1.$$

故所求和式的值为 $\frac{p-1}{4}$.

由欧拉准则，知当 $p\equiv 1 \pmod 4$ 时，-1 是模 p 的二次剩余；当 $p\equiv 3 \pmod 4$ 时，-1 是模 p 的二次非剩余. 利用这个性质可得到以下两个推论.

推论 3 如果整数 $(a,b)=1$，则 a^2+b^2 的质因子都是 $4k+1$ 的形式.

证明 设 p 是一个质因子. 则

$a^2+b^2\equiv 0 \pmod p$.

由 $(a,b)=1$，知 $(a,p)=1$.

设 c 是 a 的模 p 的逆. 则

$ac\equiv 1 \pmod p$.

故 $(ac)^2+(bc)^2\equiv 1+(bc)^2\equiv 0 \pmod p$.

进一步知 -1 是模 p 的二次剩余.

所以，p 是 $4k+1$ 形式的质数.

推论 4 存在无穷多个 $4k+1$ 形质数.

证明 假设只有有限个 $p_1,p_2,\cdots,p_k$. 令 $p=(2p_1p_2\cdots p_k)^2+1$，取 p 的任一质因子 q.

显然，q 是奇数且与 $p_1,p_2,\cdots,p_k$ 均互质.

但 $p=(2p_1p_2\cdots p_k)^2+1\equiv 0 \pmod q$，于是，$-1$ 是模 q 的二次剩余.

进一步知 q 也是一个 $4k+1$ 形质数.

所以，假设错误，原命题成立.

例 7 在整数集内，求

$$x^{2010}-2006=4y^{2009}+4y^{2008}+2007y$$

的解.[6]

（2009，马其顿数学奥林匹克）

【分析】设法因式分解后通过前述的平方和性质来证明无整数解.

证明 原方程等价于

$$x^{2010}+1=(4y^{2008}+2007)(y+1).$$

注意到，上式左边为平方和，所以，由推论 3 知只有 $4k+1$ 形质因子.

而 $4y^{2008}+2007\equiv 3 \pmod 4$，故原方程无解.

例 8 证明：有无穷多个正整数 n，使得 $(n^2+1)\mid n!$；也有无穷多个正整数 n，使得 $(n^2+1)\nmid n!$.[7]

（2008，罗马尼亚数学奥林匹克）

【分析】设法取一些特殊的 n，将 n^2+1 因式分解为两个一次式的乘积，再进一步讨论两个一次式的最大公约数，即可构造出无穷多个符合题意的数.

证明 对于第一个命题：

当 $n=2k^2$ 时，

$$n^2+1=(2k^2-2k+1)(2k^2+2k+1).$$

因 $(2k^2-2k+1,2k^2+2k+1)$

$$=(2k^2-2k+1,4k)=1,$$

而 $2k^2-2k+1<2k^2=n$，所以，$2k^2-2k+1$ 是 $n!$ 的因子.

取 $k=5m+1$，则

$2k^2+2k+1=5(10m^2+6m+1)$.

而 $5<10m^2+6m+1<2(5m+1)^2=n$，故乘积是 $n!$ 的因子.

所以，有无穷多个 n 使得 $(n^2+1)\mid n!$.

对于另一个命题，由于 -1 是 $4k+1$ 形质数 p 的二次剩余，故存在 $n(1\leqslant n\leqslant p-1)$，使得 $p\mid(n^2+1)$，$n<p$，因此，$p\nmid n!$.

这样，每个 $4k+1$ 形质数 p 就能找到一个 n 满足命题.

由推论 4，知这样的质数有无穷多个，所以，这样的 n 也有无穷多个.

练 习 题

1. 试求所有的质数对 (p,q)，使得

$pq\mid(p^p+q^q+1)$. ①

(2007，韩国数学奥林匹克)

提示：将式①看成同余式，利用推论 2 解得 $(2,5)$，$(5,2)$

2. 求所有的质数 p、q、r，使得

$p^3=p^2+q^2+r^2$

成立.

(第 22 届伊朗数学奥林匹克(第二轮))

提示：首先 $p=2$ 无解.

因为 $q^2+r^2\equiv0\pmod p$，所以，由定理 4 知，有 $p\mid q$，$p\mid r$ 或者 p 为 $4k+1$ 形质数.

可得，$p=q=r=3$.

3. 设 $q=2p+1$（p、$q>0$ 且都是质数）. 证明：存在 q 的一个倍数，在十进制中的各位数码之和不超过 3.

(2009，巴西数学奥林匹克)

提示：先证 10 模 q 的阶为 p.

由定理 3，知 10 是 q 的二次剩余. 再作 q 的二次剩余集合

$A=\{0\}\cup\{10^k\pmod q),0\leqslant k<p\}$，

$B=\{q-1\}\cup\{-1-10^k\pmod q),0\leqslant k<p\}$.

这两个集合有交集，将这两个交的元素相减得到的是一个 q 的倍数，且可发现数码和不超过 3.

4. (1)求所有的质数 p，使得 $\frac{7^{p-1}-1}{p}$ 为完全平方数；

(2)求所有的质数 p，使得 $\frac{11^{p-1}-1}{p}$ 为完全平方数.

(2009，土耳其数学奥林匹克)

提示：若存在正整数 x 和质数 p 满足 $px^2=q^{p-1}-1$，则总存在整数 y、z 满足下列两种情形之一：

(1) $q^{\frac{p-1}{2}}-1=2py^2$，$q^{\frac{p-1}{2}}+1=2z^2$；

(2) $q^{\frac{p-1}{2}}-1=2y^2$，$q^{\frac{p-1}{2}}+1=2pz^2$.

由定理 3，知当 $q=7$ 时，$p=3$；

当 $q=11$ 时，不存在 p.

5. 有无穷多个 $8k-1$ 形质数，$8k+5$ 形质数.

提示：若有有限多个 $p_1,p_2,\cdots,p_k$，仿照推论 4 的证明，对 $8k-1$ 形证

$p=(p_1p_2\cdots p_k)^2-2$

有满足的质因子，对 $8k+5$ 形证

$p=(p_1p_2\cdots,p_k)^2+4$

有满足的质因子.

参考文献：

[1] 第 23 届韩国数学奥林匹克(2010)[J]. 中等数学，2011(增刊).

[2] 2010 印度国家队选拔考试[J]. 中等数学，2011(增刊).

[3] 2005 丝绸之路数学竞赛[J]. 中等数学，2006(增刊).

[4] 2004 新加坡数学奥林匹克[J]. 中等数学，2005(增刊).

[5] 第 5 届中国香港数学奥林匹克(2002)[J]. 中等数学，2004(增刊).

[6] 2009 马其顿数学奥林匹克[J]. 中等数学，2010(增刊).

[7] 2008 罗马尼亚数学奥林匹克[J]. 中等数学，2010(增刊).

从阶与原根谈起