同　余“续 2”

赛题精讲

例 1：数 1978^n 与 1978^m 的最末三位数相等，试求正整数 m 和 n，使得 n+m 取最小值，这里 $n>m\geq 1$.　　（第 20 届 IMO 试题）

【解】由已知 $1978^n\equiv 1078^m \pmod{1000}$，而 1000=8×125，所以

$$1978^n\equiv 1078^m \pmod 8 \quad ①$$

$$1978^n\equiv 1078^m \pmod{125} \quad ②$$

因 $n>m\geq 1$，且（1978^m，125）=1，则由②式知 $1978^{n-m}\equiv 1 \pmod{125}$ ③

又直接验证知，1978 的各次方幂的个位数字是以 8、4、2、6 循环出现的，所以只有 n－m 为 4 的倍数时，③式才能成立，因而可令 n－m=4k.由于. n+m=（ n－m）+2m=4k+2m，因而只需确定出 k 和 m 的最小值.

先确定 k 的最小值：因为 $1978^4=(79\times 25+3)^4\equiv 3^4\equiv 1 \pmod 5$，$1978^4\equiv 3^4\not\equiv 1 \pmod{25}$.故可令 $1978^4=5t+1$，而 $5\nmid t$，从而 $0\equiv 1978^{n-m}-1=1978^{4k}-1=(5k+1)^k-1\equiv \frac{k(k-1)}{2}\cdot(5t)^2+k\cdot 5t \pmod{125}$，显然，使上式成立的 k 的最小值为 25.

再确定 m 的最小值：因 $1978\equiv 2 \pmod 8$，则由①式知，$2^n\equiv 2^m \pmod 8$　④

由于 $n>m\geq 1$，④式显然对 m=1，2 不成立，从而 m 的最小值为 3.

故合于题设条件的 n+m 的最小值为 106.

【评述】比例中我们用了这样一个结论：1978 的各次方幂的个位数字是以 8，4，2，6 循环出现，即，当 r=1，2，3，4 时，$1978^p=1978^{4q+r}\equiv 8,4,2,6 \pmod{10}$.这种现象在数学上称为“模同期现象”.一般地，我们有如下定义：

整数列 $\{x_n\}$ 各项除以 m（m≥2，m∈N*）后的余数 a_n 组成数列 $\{a_n\}$.若 $\{a_n\}$ 是一个周期数列，则称 $\{x_n\}$ 是关于模 m 的周期数列，简称模 m 周期数列.满足 $a_{n+T}=a_n$（或 $a_{n+T}\equiv x_n$（modm））的最小正整数 T 称为它的周期.

例如，（1）$\{1978^n\}$ 是模 10 周期数列，周期为 4；（2）自然数列{n}是一个模 m（m≥2，m∈N*）周期数列，周期为 m；（3）任何一个整数等差数列都是一个模 m（m≥2，m∈N*）周期数列，周期为 m.

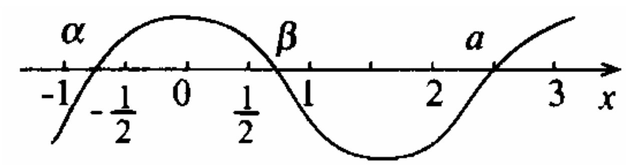
例 2：设 a 是方程 $x^3-3x^2+1=0$ 的最大正根，求证：17 可以整除$[a^{1788}]$与$[a^{1988}]$.其中$[x]$表示不超过 x 的最大整数. （第 29 届 IMO 预选题）

【证明】根据如下符号表可知，若设三根依次为$\alpha<\beta<a$，

则$-1<\alpha<-\frac{1}{2},\frac{1}{2}<\beta<1,$

x	-1	$-\frac{1}{2}$	$\frac{1}{2}$	1	$2\sqrt{3}$	3
$f(x)$符号	$-$	+	+	$-$	$-$	+

$2\sqrt{2}<a$,由于$f(-\alpha)=-2\alpha^3+(\alpha^3-2\alpha^2+1)=-2\alpha^3>0$,于是$-\alpha<\beta,|\alpha|<\beta.$



另一方面，由韦达定理知，

$\alpha^2+\beta^2=(\alpha+\beta)^2-2\alpha\beta=(3-a)^2+\frac{2}{a}=9+\frac{2-6a^2+a^3}{a}=9+\frac{-2a^3+a^3}{a}=1+(8-a^2)$

$\because a^2>(2\sqrt{2})^2=8,\therefore \alpha^2+\beta^2<1.$

为了估计$[a^{1788}]$、$[a^{1988}]$，先一般考察$[a^n]$，为此定义：

$u_n=\alpha^n+\beta^n+a^n.(n=0,1,2,\cdots)$

直接计算可知：$u_0=3,u_1=2+\beta+a=3.u_2=\alpha^2+\beta^2+a^2=9,$以及$u_{n+3}=3u_{n+2}-n(n\geq 0).$

又因$0<\alpha^n+\beta^n<1(\because|\alpha|<\beta,$即$\alpha^n+\beta^n>0,$又$\alpha+\beta=3-\alpha<2-2\sqrt{2}<1,$当$n\geq 2$时，$\alpha^n+\beta^n\leq|\alpha|^n+\beta^n<\alpha^2+\beta^2<1),$则$a^n=u_n-(\alpha^n+\beta^n)=u_n-1-[1-(\alpha^n+\beta^n)].$

$\therefore [a^n]=u_n-1.(n=1,2,\cdots)$

由此知，命题变为证明：$u_{1788}-1$和$u_{1988}-1$能被 17 整除.

现考察$\{u_n\}$在模 17 的意义下的情况：

$u_0\equiv 3,u_1\equiv 3,u_2\equiv 9,u_3\equiv 7,u_4\equiv 1,u_5\equiv 11,u_6\equiv 9,u_7\equiv 9,u_8\equiv 16,u_9\equiv 5,u_{10}\equiv 6,u_{11}\equiv 2,$

$u_{12}\equiv 1,u_{13}\equiv 14,u_{14}\equiv 6,u_{15}\equiv 0,u_{16}\equiv 3,u_{17}\equiv 3,u_{18}\equiv 9,\cdots\cdots$

可见，在模 17 意义下，$\{u_n\}$是 16 为周期的模周期数列，即$u_{n+16}\equiv u_n(\bmod 17)$.由于$1788\equiv 12(\bmod 16),1988\equiv 4(\bmod 16)$,故$u_{1788}\equiv u_{12}\equiv 1(\bmod 17),u_{1988}\equiv u_4\equiv 1(\bmod 17)$,故$u_{1788}-1\equiv 0,u_{1988}-1\equiv 0(\bmod 17)$.命题得证.

例 3：求八个整数$n_1,n_2,\cdots,n_8$满足：对每个整数 k（－1985<k<1985），有八个整数a_1，a_2，…，a_8∈{－1，0，1}，使得$k=a_1n_1+a_2n_2+\cdots+a_8n_8$.　　（第 26 届 IMO 预选题）

【解】令数集$G=\{k\mid k=a_1+a_2\cdot 3+a_3\cdot 3^2+\cdots+a_{n+1}\cdot 3^n,a_i\in\{-1,0,1\},i=1,2,\cdots,n+1\}$.

显然　$\max G=1+3+3^2+\cdots+3^n=\dfrac{3^{n+1}-1}{2}\xlongequal{\text{记}}$H,

$$mixG=1-3-3^2-\cdots-3^n=-H.$$

且 G 中的元素个数有$3^{n+1}=2H+1$个.又因 G 中任意两数之差的绝对值不超过 2H，所以 G 中的数对模 2H+1 不同余.因此，G 的元素恰好是模 2H+1 的一个绝对值最小的完系，于是，凡满足$-H\le k\le H$的任意整数都属于 G，且可惟一地表示为：$a_1+a_2\cdot 3+a_3\cdot 3^2+\cdots+a_{n+1}\cdot 3^n$形式.

当 n=7 时，H=3280>1985，而 n=6 时，H=1043<1985.故 $n_1=1$，$n_2=3$，…，$n_8=3^7$为所求.

例 4：设 n 为正整数，整数 k 与 n 互质，且 0<k<n.令 M={1，2，…，n－1}，给 M 中每个数染上黑、白两种颜色中的一种，染法如下：(i）对 M 中每个 i，i 与 n－i 同色；(ii）对 M 中每个 i，$i\neq k$,i 与$|k-i|$同色.求证：M 中所有的数必为同色.　　（第 26 届 IMO 试题）

【证明】因$(k,n)=1$,又 0，1，…n－1 是模 n 的一个完全剩余系，所以 0，k，2k，…，（n－1）k 也是模 n 的一个完全剩余系.若设$jk\equiv r_j(\bmod n)$(其中$1\le r_j\le n-1,j=1,2,\cdots,n-1$),则 M={$r_1,r_2,\cdots,r_{n-1}$}.下只需证$r_{j+1}$与$r_j(1\le j\le n-2)$.因为，若如此，当 r_1 的颜色确定后，M 中所有都与 r_1 同色.

由于$(j+1)k\equiv r_{j+1}(\bmod n)$,则$r_j+k\equiv r_{j+1}(\bmod n)$，因此，

(1)若$r_j+k<n$,则$r_{j+1}=r_j+k$，于是,由条件(i)知，$k-r_{j+1}=n-r_j$与$n-(n-r_j)=r_j$

同色.又由条件（ii）知，$k-r_{j+1}$与$|k-r_{j+1}-k|=r_{j+1}$同色，故r_{j+1}与r_j同色.

综上所述可知，r_{j+1}与r_j同色.命题得证.

例 5：设 a 和 m 都是正整数，a>1.证明：$m\mid\varphi(a^m-1)$.

【证明】实上，显然a与a^m-1互素，且a模a^m-1的阶是 m，所以由模阶的性质③导出$m\mid\varphi(a^m-1)$.

例 6：设 p 是奇素数，证明：$2p-1$的任一素因子具有形式$2px+1, x$是正整数.

【证明】设 q 是 2^p-1 的任一素因子，则 q≠2.设 2 模 q 的阶是 k，则由$2^p\equiv1(\bmod q)$知 k|p，故 k=1 或 p（因 p 是素数，这是能确定阶 k 的主要因素）.显然 k≠1，否则$2^1\equiv1(\bmod q)$，这不可能，因此 k=p.

现在由费马小定理$2^{q-1}\equiv1(\bmod q)$推出$k\mid q-1$,即$p\mid q-1$.因 p、q 都是奇数，故 q－1=2px（x 是个正整数），证毕.

例 7：设 m,a,b 都是正整数，m>1，则$m^a-1,m^b-1)=m^{(a,b)}-1$.

【证明】记$d=(m^a-1,m^b-1)$.由于（a,b）|a 及（a,b）|b，易知$m^{(a,b)}-1\mid m^a-1$及$m^{(a,b)}-1\mid m^b-1$，故$m^{(a,b)}-1\mid d$，

另一方面设 m 模 d 的阶是 k，则由

$m^a\equiv1(\bmod d), m^b\equiv1(\bmod d)$

推出，k|a 及 k|b，故 k|（a，b）.因此$m^{(a,b)}\equiv1(\bmod d)$,即$d\mid m^{(a,b)}-1$.

综合两方面可知，$d=m^{(a,b)}-1$.证毕.

例 8：设 n，k 是给定的整数，n>0，且 k（n－1）是偶数.证明：存在x,y,使得$(x,n)=(y,n)=1$,是$x+y\equiv k(\bmod n)$.

【证明】我们先证明，当 n 为素数幂 p^α 时结论成立.实际上，我们能证明，存在 x,y，使 $p\nmid xy$，且$x+y=k$.

如 p=2，则条件表明 k 为偶数，可取 $x=1, y=k-1;$如$p>2,$则$x=1, y=k-1$或$x=1, y=k-2$中有一对满足要求.

一般情形下，设 $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ 是 n 的标准分解，上面已证明，对每个 p_i，均有整数 x_i，y_i，使 $p_i \nmid x_iy_i$，且 $x_i+y_i=k(1,2,\cdots,r)$. 现在孙子定理表明，同余方程组

$$x\equiv x_1(\operatorname{mod} p_1^{\alpha_1}),\cdots,x\equiv x_r(\operatorname{mod} p_r^{a_r})$$ 有解 x，同样

$$y\equiv y_1(\operatorname{mod} p_1^{\alpha_1}),\cdots,y\equiv y_r(\operatorname{mod} p_r^{a_r})$$

也有解 y.现在易证 x,y 符合问题中的要求：因 $p_i \nmid x_iy_i$，故 $p_i \nmid xy$（i=1，⋯，r），于是（xy，n）=1.又 $x+y=x_i+y_i=k(\operatorname{mod} p_i^{\alpha_1})(i=1,\cdots,r),$故$x+y\equiv k(\operatorname{mod} n).$

例 9：设 n 为任意的正整数.证明：一定存在 n 个连续的正整数解，使其中任何一个都不是质数的整数幂. （第 30 届 IMO 试题）

【证明】取 2n 个两两不同的质数 $p_1,p_2,\cdots,p_n$和$q_1,q_2,\cdots,q_n$.同余方程组 $x\equiv -i(\operatorname{mod} p_iq_i),$ $i=1,2,\cdots,n$.由于 $p_1q_1,p_2q_2,\cdots,p_nq_n$ 两两互质，根据孙子定理必有解，取为正整数 N，则 n 个连续正整数 N+1，N+2，⋯，N+n 都至少含有两个不同的质因数，因而它们中的任一个都不是质数的整数幂.证毕.