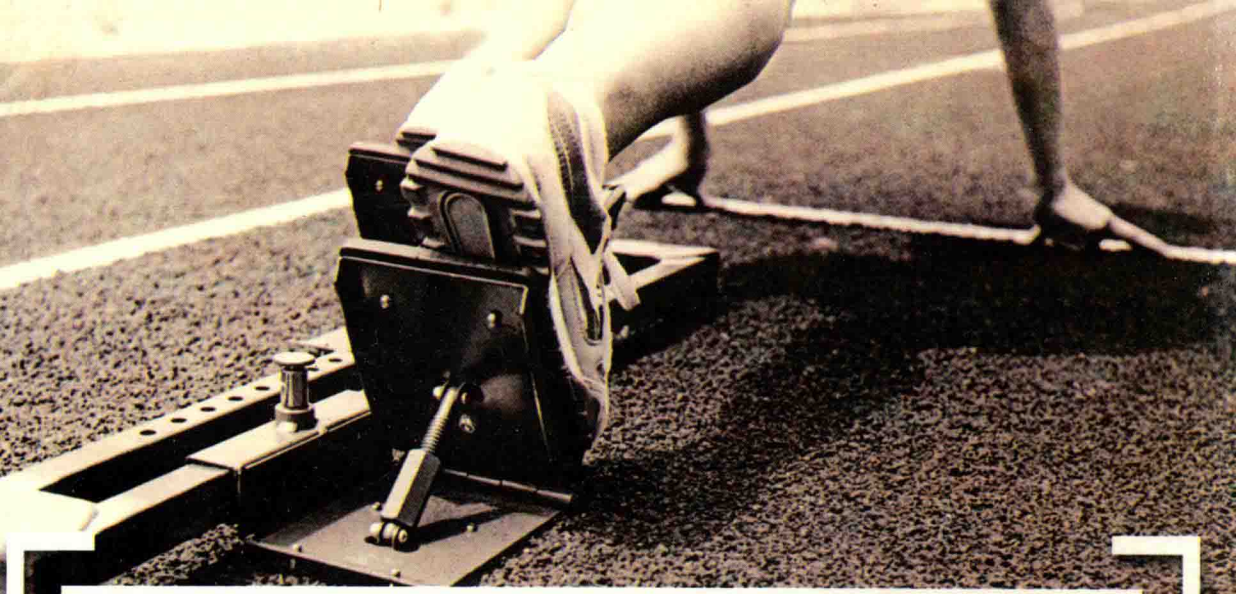

奥赛经典

分级精讲与测试系列

高一数学

◇沈文选/主编

湖南师范大学出版社

奥赛经典

分级精讲与测试系列

高一数学

◇沈文选/主编

编写

沈文选　羊明亮　吴仁芳

李善平　向昭红

湖南师范大学出版社

图书在版编目(CIP)数据

分级精讲与测试系列·高一数学 / 沈文选主编 .—长沙:湖南师范大学出版社,2004.5
(奥赛经典丛书)
ISBN 7-81081-420-6

Ⅰ.分… Ⅱ.沈… Ⅲ.数学课—初中—教学参考资料 Ⅳ.G634

中国版本图书馆 CIP 数据核字(2004)第 038742 号

分级精讲与测试系列·高一数学

沈文选 主编

◇丛书策划:陈宏平 廖建军 周玉波 何海龙
◇组稿编辑:何海龙
◇责任编辑:黄道见
◇责任校对:胡晓军
◇出版发行:湖南师范大学出版社
地址/长沙市岳麓山 邮编/410081
电话/0731.8853867 8872751 传真/0731.8872636
网址/www.hunnu.edu.cn/press
◇经销:湖南省新华书店
◇印刷:湖南航天长宇印刷有限责任公司

◇开本:730×960 1/16
◇印张:18.25
◇字数:378 千字
◇版次:2004 年 10 月第 1 版 2005 年 3 月第 2 次印刷
◇印数:5001—10000 册
◇书号:ISBN 7-81081-420-6/G·264
◇定价:17.00 元

目 录

第1讲　整除性问题

竞赛要点

数的整除性是初等数论的基础.高中数学竞赛大纲中,在这个基础上列出了要掌握的一些简单、常用的有关数论知识的要求,如欧几里得除法、费马小定理等.在大纲说明中,提出了在掌握欧几里得除法的同时,还应掌握辗转相除法.

定理1　设 a 和 b 是两个整数,$b\neq 0$,则存在惟一的一对整数 q 和 r,使得

$$a=qb+r(0\leqslant r<b) \tag{1-1}$$

成立.其中 q 称为用 b 除 a 所得的不完全商,r 叫做用 b 除 a 所得的余数.

上述定理是辗转相除法的根据,常称为带余除法定理,也称为欧几里得除法.特别地,当 $r=0$ 时,则说 b 整除 a,或 a 能被 b 整除,记为 $b\mid a$.否则就说 b 不能整除 a,或 a 不能被 b 整除,记为 $b\nmid a$.

整除具有许多非常重要的性质与结论:

定理2　设 a,b,c 是任意整数,则

(1) $a\mid a$. (1-2)

(2)当 $a\mid b,b\mid a$ 时,有 $a=b$ 或 $a=-b$. (1-3)

(3)当 $a\mid b,b\mid c$ 时,有 $a\mid c$. (1-4)

(4)当 $c\mid a,c\mid b$ 时,有 $c\mid(ma+nb)$,其中 m,n 为任意整数. (1-5)

(5)当 a 与 c 互素,且又①$a\mid bc$ 时,有 $a\mid b$;②$a\mid b,c\mid b$ 时,有 $ac\mid b$. (1-6)

定理3　k 个连续整数的积能被 $1\cdot 2\cdots k$ 整除,即当 a 为整数时,有 $1\cdot 2\cdots k\mid a\cdot(a+1)\cdots(a+k-1)$. (1-7)

定理4　(费马小定理)当 p 为素数时,对于任意整数 a,有 $p\mid(a^p-a)$. (1-8)

定理5　(威尔逊定理)当 p 为素数时,有

$$p\mid[1\cdot 2\cdot 3\cdots(p-1)-1]. \tag{1-9}$$

为了研究整除性问题,还要注意到下面的重要定理:

定理6　(算术基本定理)任何一个大于1的整数 a,都能惟一表示成它的质(素)因数的乘积(不计各因数的顺序),即有

$$a=p_1p_2\cdots p_n, \tag{1-10}$$

其中 $p_1\leqslant p_2\leqslant\cdots\leqslant p_n$,$p_i(i=1,2,\cdots,n)$ 为质(素)数.

如果把相同的质因数的积用指数形式表示,

则　$$a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_k^{\alpha_k}, \tag{1-11}$$

其中 $p_1<p_2<\cdots<p_k$,$p_i(i=1,2,\cdots,k)$ 为质数,$\alpha_1,\alpha_2,\cdots,\alpha_k$ 为正整数.

式(1-11)称为 a 的标准分解式.

定理7　设正整数 a 的标准分解式为(1-11),则正整数 d 是 a 的约数的条件是 d 的标准分解式为

$$d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}, \tag{1-12}$$

其中 $1 \leqslant \beta_i \leqslant \alpha_i (i = 1,2,\cdots,k)$. 反之亦真.

定理 8 设正整数 a 的标准分解式为式(1-11), a 的约数的个数记为 $T(a)$, 则

$$T(a) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1). \tag{1-13}$$

事实上, 由(1-11)与(1-12)式可知, a 的每个约数都对应着一个有序数组 $(\beta_1, \beta_2, \cdots, \beta_k)$. 反之, 每个数组 $(\beta_1, \beta_2, \cdots, \beta_k)$ 也对应着 a 的一个约数, 故 $T(a)$ 就等于有序数组 $(\beta_1, \beta_2, \cdots, \beta_k)$ 的个数, 但 β_i 可取 $0,1,2,\cdots,\alpha_i$, 共有 $\alpha_i + 1$ 种取法. 故有(1-13)式.

推论 当且仅当 $T(a)$ 为奇数时, a 为完全平方数.

定理 9 若 a 为合数, p 为 a 的除 1 以外的最小约数, 则 p 为质数且 $p \leqslant \sqrt{a}$.

事实上, 若 p 不是质数, 则 p 还有大于 1 的约数 q, 即 $q \mid p$, 而 $p \mid a$, 故 $q \mid a$, 即 q 为大于 1 又比 p 小的约数, 与 p 最小矛盾. 故 p 为质数.

又 p 为 a 的约数, 故存在整数 b, 使 $a = pb$, 即 b 也为 a 的约数. 于是 $b \geqslant p$, 从而 $a = pb \geqslant p^2$, 即 $p \leqslant \sqrt{a}$.

推论 如果 $\leqslant \sqrt{a}$ 的所有质数均不是 a 的约数, 则 a 为质数.

定理 10 设 p 为质数, $a_1, a_2, \cdots, a_n$ 为 n 个正整数, 若 $p \mid a_1 a_2 \cdots a_n$, 则必存在整数 $i, 1 \leqslant i \leqslant n, p \mid a_i$.

名题精析

例 1 (1)(1991 年高中联赛题)设 a 是正整数, $a < 100$, 并且 $a^3 + 23$ 能被 24 整除, 那么, 这样的 a 的个数为(　　).

A.4　　B.5　　C.9　　D.10

(2)(1985 年高中联赛题)在已知数列: 1,4,8,10,16,19,21,25,30,43 中, 相邻若干数之和能被 11 整除的数组共有_____组.

解 (1)选 B. 理由: 考虑使 $24 \mid (a^3 - 1)$ 成立的 a. $a^3 - 1 = (a-1)(a^2 + a + 1) = (a-1)[a(a+1) + 1]$. 因 $a(a+1) + 1$ 是奇数, 若要 $24 \mid (a^3 - 1)$, 必有 $2^3 \mid (a-1)$. 若 $a - 1$ 不能被 3 整除, 则 $3 \mid a(a+1)$, 从而 $a(a+1) + 1$ 不能被 3 整除. 因此, 若要 $24 \mid (a^3 - 1)$, 必有 $3 \mid (a-1)$, 这样就有 $24 \mid (a-1)$, 即 $a = 24k + 1$ $(k \in \mathbf{Z})$. 由 $24k + 1 < 100$, k 可能取的一切值为 0,1,2,3,4, 也就是这样的 a 有 1,25,49,73,95 五个.

(2)填 7. 理由如下: 由于是考虑被 11 整除的问题, 故可先把各项减去 11 的倍数, 使数字变小而便于运算, 由此可得如下数列: 1,4,−3,−1,5,−3,−1,3,−3,−1. 设 S_n 为它的前 n 项和, 则 $s_1 = 1$, $s_2 = 5, s_3 = 2, s_4 = 1, s_5 = 6, s_7 = 2, s_8 = 5, s_9 = 2, s_{10} = 1$. 其中相等的有 $s_1 = s_4 = s_{10} = 1, s_2 = s_8 = 5, s_3 = s_7 = s_9 = 2$. 从而 $s_4 - s_1, s_{10} - s_1, s_{10} - s_4, s_8 - s_2, s_7 - s_3, s_9 - s_3, s_9 - s_7$ 均能被 11 整除. 故共有 7 组数能被 11 整除.

例 2 (1994 年全俄竞赛题)已知自然数 a, b 使得 $\frac{a+1}{b} + \frac{b+1}{a}$ 是整数, 证明: a 与 b 的最大公约数不超过 $\sqrt{a+b}$.

证明 设 $(a, b) = d$, 则 $d \mid a$, $d \mid b$, 从而 $d^2 \mid ab$, $d^2 \mid a^2$, $d^2 \mid b^2$. 由题设 $\frac{a+1}{b} + \frac{b+1}{a} = \frac{a^2 + b^2 + a + b}{ab}$ 是整数, 知 $d^2 \mid (a^2 + b^2 + a + b)$. 注意到 $d^2 \mid a^2, d^2 \mid b^2$, 则 $d^2 \mid (a^2 + b^2)$, 从而 $d^2 \mid (a +$

$b)$,故 $d \leqslant \sqrt{a+b}$.

例 3 亚华商场销售某种货物,去年总收入为 36963 元,今年每件货物的售价(单价)不变,总收入为 59570 元.如果单价(以元为单位)是大于 1 的整数,问今年与去年各售这种货物多少件?

解 单价是 36963 与 59570 的最大公约数,由辗转相除法得出(36963,59570) = 37.

36963	1	59570
22607	1	36963
14356	1	22607
8251	1	14356
6105	1	8251
4292	2	6105
1813	1	2146
1665	5	1813
148	2	333
148	4	296
0		37

因为 37 的约数只有 1 与本身,所以 36963 与 59570 的大于 1 的公约数只有 37,即单价为 37 元.

于是,今年售出 $59570 \div 37 = 1610$ 件,去年售出 $36963 \div 37 = 999$ 件.

例 4 (1958 年匈牙利竞赛题)如果 a, b 都是整数,且 $91(a^2+ab+b^2)$,则 a, b 都能被 3 整除.

证明 由 $a^2+ab+b^2 = (a-b)^2+3ab$ 及 $91(a^2+ab+b^2)$,知 $3 \mid (a^2+ab+b^2)$.

又 $3 \nmid 3ab$,则 $3 \mid (a-b)^2$,即 $3 \mid (a-b)$,从而 $91(a-b)^2$,即知 $9 \nmid 3ab$,亦即 $3 \nmid ab$,这只有当 a, b 它们之中的一个能被 3 整除时才有可能.而 $3 \mid (a-b)$,故必有 $3 \mid a$ 和 $3 \mid b$ 同时成立.

注 此例的证明过程中反复运用了定理 2.

例 5 设 n 是正奇数,试证明:

$$18 \mid [1^n+2^n+\cdots+9^n-3(1^n+6^n+8^n)].$$

分析 注意到 $18 = 2 \times 9$,而 2 与 9 互质,所以只要能证明 $1^n+2^n+\cdots+9^n-3(1^n+6^n+8^n)$既能被 2 整除,同时也被 9 整除即可.在证明被 9 整除时,可借助因式分解公式(参见第 13 讲例 1):对于奇数 n,有

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

证明 显然 $1^n+2^n+\cdots+9^n$ 和 $3(1^n+6^n+8^n)$均是奇数,从而其差必为偶数,可知其差能被 2 整除.又由于 n 是正奇数,则知

1^n+8^n,2^n+7^n,3^n+6^n 和 4^n+5^n

都是 9 的整数倍.而 $1^n+2^n+\cdots+9^n-3(1^n+6^n+8^n)$可变形为 $9^n+(1^n+8^n)+(2^n+7^n)+(3^n+6^n)+(4^n+5^n)-3(1^n+8^n)-3\times 6^n$,可见每一项都能被 9 整除,从而结论获证.

注 利用乘法公式或因式分解公式是讨论整除性的一种重要方法,对于任意正整数,还有乘法公式:$a^n-b^n = (a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1})$.

例 6 (1956 年北京市竞赛题)证明:$n^3+\frac{3}{2}n^2+\frac{1}{2}n-1$ 对任何正整数 n 都是整数,并且用 3 除时余 2.

证明 $n^3+\frac{3}{2}n^2+\frac{1}{2}n-1=\frac{n(n+1)(2n+1)}{2}-1$.由于$\frac{1}{2}n(n+1)$是整数,所以原式对任何整数 n 都是整数.

又 $n^3+\frac{3}{2}n^2+\frac{1}{2}n-1=\frac{2n(2n+1)(2n+2)}{8}-3+2$,由于 $2n(2n+1)(2n+2)$可被 3 整除,而 3 与 8 互质,因而$\frac{2n(2n+1)(2n+2)}{8}$可被 3 整除,故结论获证.

注 (1)此例一方面经过变形出现连续整数的乘积,再利用 n 个连续整数之积必可被 n 整除;另一方面还用到了整除性质的定理 2 中的(5).

(2)此例也可以运用整值多项式的性质来证.

如果一个多项式 $p(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 的所有系数 $a_0,a_1,\cdots,a_{n-1},a_n$ 都是整数,则称它为整系数多项式,如果多项式 $p(x)$在 x 取整数时,所得到的多项式值也是整数,则称 $p(x)$为整值多项式.很显然,整系数多项式一定是整值多项式.

结论 1 设 $p(x)$是一个 n 次多项式.如果在相邻的 $n+1$ 个整数点上,$p(x)$的值为整数,那么它在所有整数点上的值都是整数,也即 $p(x)$为整值多项式.

结论 2 设 $p(x)$是 n 次多项式.如果在相邻的 $n+1$ 个整数点上,$p(x)$的值均为整数,并且能被整数 m 整除,那么对任何整数 x,$p(x)$的值均是整数,而且都能被 m 整除.

例 6 另证 考虑一个新的多项式 $F(n)=\frac{f(n)+1}{3}$.我们可以证明 $F(n)$是一个整值多项式:令 $n=1,2,3,4$,得 $F(1)=0,F(2)=1,F(3)=5,F(4)=14$.而 $F(n)$是一个三次多项式,由上述结论知 $F(n)$是整值多项式,从而 $f(n)$的每一个值被 3 除时余 2.

例 7 (1994 年全俄竞赛题)整数 x,y,z 满足$(x-y)(y-z)(z-x)=x+y+z$.证明:$x+y+z$能被 27 整除.

证明 只要证明:x,y,z 除以 3 时余数都相同,那么,$x+y+z=(x-y)(y-z)(z-x)$就能被 27 整除,若 x,y,z 除以 3 时的余数相异,则$(x-y)(y-z)(z-x)$就不能被 3 整除,而 $x+y+z$ 能被 3 整除.所以,x,y,z 中至少有两个数除以 3 时余数相同,而此时 $x+y+z$ 能被 3 整除.因此,第三个数在除以 3 时也有相同的余数.

例 8 证明:大于 3 的两个孪生素数所夹的那个自然数能被 6 整除.

证明 如果 p 是大于 3 的素数,则 p 只可能是 $3m+1$ 和 $3n+2$ 形式的数(其中 m 和 n 均是正整数).此时 $p^2-1=(3m+1)^2-1=3(3m^2+2m)$,或者 $p^2-1=(3n+2)^2-1=3(3n^2+4n+1)$,可见 $3|(p^2-1)$.

又由于 $p>3$ 是素数,所以有 $p=2k+1(k>1$ 是整数),于是 $p^2-1=(2k+1)^2-1=4k(k+1)$,因此,$8|(p^2-1)$,从而 $24|(p^2-1)$.

如果 $a-1$ 和 $a+1$ 是一对大于 3 的孪生素数,题目要求证明 a 是 6 的倍数.由上面的讨论,有

$24|[(a-1)^2-1]$和 $24|[(a+1)^2-1]$,

而 $[(a+1)^2-1]-[(a-1)^2-1]=4a$.

所以 $24|4a$,故有 $6|a$.

例 9 设 n 为正整数,下式:

$$2^1+3^5+4^9+5^{13}+\cdots+n^{4n-7}-\frac{1}{2}(n^2+n-2)$$

的值的个位数字是多少?

解 先证 n^5-n 能被 5 整除.事实上,

$$n^5-n=n(n^2+1)(n+1)(n-1)=n(n^2-4+5)(n+1)(n-1)$$
$$=n(n-1)(n+1)(n-2)(n+2)+5n(n+1)(n-1).$$

上式第一个加项是 5 个连续整数之积,能被 5 整除,故 n^5-n 能被 5 整除.

又 n^5-n 是偶数,所以 n^5-n 能被 10 整除.

其次,$n^{4k+1}-n=n(n^{4k}-1)$能被 $n(n^4-1)$整除,即能被 10 整除.因而形式为 n^{4k+1}的数与 n 具有相同的个位数.因此,所要求的式子的个位数与数$(2+3+4+\cdots+n)-\frac{1}{2}(n^2+n-2)$的个位数字相同.但$(2+3+4+\cdots+n)-\frac{1}{2}(n^2+n-2)=[\frac{n(n+1)}{2}-1]-\frac{n^2+n-2}{2}=0$.所以,所给表示式的个位数字为 0.

注 (1)对于 $10|(n^5-n)$可运用费马小定理证明:因 5 为素数,从而有 $5|(n^5-n)$,又 n^5-n 是偶数,故 $10|(n^5-n)$.

(2)对于 $10|(n^{4k+1}-n)$,我们有更一般的结论:

设 n,k,m 都是正整数,则 $10|(n^{4k+m}-n^m)$.

事实上,$n^{4k+m}-n^m=n^m(n^{4k}-1)$

$$=n^m(n^4-1)[(n^4)^{k-1}+(n^4)^{k-2}+\cdots+1]$$
$$=n(n-1)(n+1)(n^2+1)\cdot n^{m-1}(n^{4k-4}+n^{4k-8}+\cdots+1)$$
$$=n(n-1)(n+1)[(n^2+5n+6)-(5n+5)]\cdot n^{m-1}(n^{4k-4}+n^{4k-8}+\cdots+1)$$
$$=[(n-1)\cdot n\cdot(n+1)(n+2)(n+3)-5(n-1)n(n+1)^2]\cdot n^{m-1}\cdot(n^{4k-4}+n^{4k-8}+\cdots+1)$$

注意到 k 个连续整数之积总可被 $1\cdot2\cdot\cdots\cdot k$ 整除,则知 $10|(n-1)\cdot n(n+1)(n+2)(n+3)$,$10|5\cdot(n-1)n(n+1)^2$,从而

$10|(n^{4k+m}-n^m)$.

例 10 试证:对任意正整数 n,在 n^2 和 $n^2+n+3\sqrt{n}$之间一定能找到 3 个正整数,使得其中两个的乘积能被第 3 个整除.

证明 先从特殊情形入手来寻求规律.

当 $n=1$ 时,在 1 与 5 之间有三个数 2,3,4,显然有 $2|3\times4$.

当 $n=2$ 时,在 4 和 $6+3\sqrt{2}$之间有 6,8,9(或 5,8,10),显然有 $6|8\times9$(或 $5|8\times10$).

当 $n=10$ 时,在 100 与 $110+3\sqrt{10}$之间有 $a=104=8\times13$,$b=108=9\times12$,$c=117=9\times13$,显然 $c|ab$.在这种情形下,我们对 a,b,c 的表示做一点变形,可以发现规律:

$a=(10-2)(10+2+1)$,

$b=(10-2+1)(10+2)$,

$c=(10-2+1)(10+2+1)$.

由此,一般地,在 n^2 与 $n^2+n+3\sqrt{10}$之间,有

$a=(n-x)(n+x+1)=n^2+n-x^2-x$,

$b=(n-x+1)(n+x)=n^2+n-x^2+x$,

$c=(n-x+1)(n+x+1)=n^2+2n+1-x^2$.

其中 $n>2$,且 x 是整数.显然,$c \mid ab$.

设 x 是满足 $x^2+x<n$ 的最大整数,那么 $c<n^2<a<b<c$,剩下只需证明:$c<n^2+n+3\sqrt{n}$,即 $n^2+2n+1-x^2<n^2+n+3\sqrt{n}$,亦即 $x^2>n-3\sqrt{n}+1$.

用反证法,假设 $x^2 \leqslant n-3\sqrt{n}+1$,则 $x<\sqrt{n}-\frac{3}{2}$,亦即 $x+1<\sqrt{n}-\frac{1}{2}$.但在这种情况下,有

$$(x+1)^2+(x+1)<(\sqrt{n}-\frac{1}{2})^2+(\sqrt{n}-\frac{1}{2})=(n-\sqrt{n}+\frac{1}{4})+(\sqrt{n}-\frac{1}{2})<n,$$

这与 x 的选择矛盾.故 $x^2>n-3\sqrt{n}+1$ 获证.

例 11 (IMO-26 预选题)求出最小正整数 n,使其恰有 144 个正约数,并且其中有 10 个连续整数.

解 任意 10 个连续整数中,必有 2^3,3^2,5,7 的倍数,因此,n 必是 $2^3 \cdot 3^2 \cdot 5 \cdot 7$ 的倍数.所以 n 的素因数分解必是 $2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 7^{\alpha_4} \cdots p_s^{\alpha_s}$,其中 $\alpha_1 \geqslant 3, \alpha_2 \geqslant 2, \alpha_3 \geqslant 1, \alpha_4 \geqslant 1$.

由于约数的个数是

$T(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1)=144$.

而 $(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)(\alpha_4+1) \geqslant 4 \times 3 \times 2 \times 2=48$,

因此,$(\alpha_5+1)\cdots(\alpha_s+1) \leqslant 3$,即知 $s=5, 0 \leqslant \alpha_5 \leqslant 2$.于是,$n$ 的形式是 $n=2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \cdot 7^{\alpha_4} \cdot 11^{\alpha_5}$,其中 $\alpha_1 \geqslant 3, \alpha_2 \geqslant 2, \alpha_3 \geqslant 1, \alpha_4 \geqslant 1, 0 \leqslant \alpha_5 \leqslant 2$.

在满足 $(\alpha_1+1)(\alpha_2+1)(\alpha_3+1)(\alpha_4+1)(\alpha_5+1)=144$ 的数组 $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ 中进行试算,可得(5,2,1,1,1)使 n 最小.于是最小的 $n=2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11=110880$.

注 此利用到了整数的素因数分解及约数个数的定理,而注意到 n 要有 10 个连续的约数,则 n 必须是 $2^3 \cdot 3^2 \cdot 5 \cdot 7$ 的倍数,是解决问题的关键.

例 12 (CMO-11 试题)设 $S=\{1,2,\cdots,50\}$,求最小的自然数 k,使 S 的任一 k 元子集中都存在两个不同的数 a 与 b,满足 $(a+b) \mid ab$.

分析 可先找出所有满足 $(a+b) \mid ab$ 的数对 (a,b),然后再讨论至少要取多少个数才能保证一定有一个这样的数对被取到即是解.

解 设 $a, b \in S, a<b$,满足 $(a+b) \mid ab$,令 $(a,b)=d, a=a_1 d, b=b_1 d$,则 $(a_1, b_1)=1$,且 $1 \leqslant a_1<b$,于是

$a+b=d(a_1+b_1), ab=d^2 a_1 b_1$

故 $d(a_1+b_1) \mid d^2 a_1 b_1$.即 $(a_1+b_1) \mid d(a_1+b_1)$.

但 $(a_1+b_1, a_1)=1, (a_1+b_1, b_1)=1$,则

$(a_1+b_1) \mid d$.

而 $(a_1+b_1)^2 \leqslant d(a_1+b_1)=a+b \leqslant 99$,

故 $3 \leqslant a_1+b_1 \leqslant 9$.

(ⅰ)若 $a_1+b_1=3$,则 $a_1=1, b_1=2$,d 可取 3,6,9,12,15,18,21,24,相应的 $(a,b)=(3,6),(6,12),(9,18),(12,24),(15,30),(18,36),(21,42),(24,48)$;

(ⅱ)若 $a_1+b_1=4$,则 $a_1=1, b_1=3$,d 可取 4,8,12,16,相应的 $(a,b)=(4,12),(8,24),(12,36),(16,48)$;

(ⅲ)若 $a_1+b_1=5$,则 $a_1=1, b_1=4$,d 可取 5,10,相应的 $(a,b)=(5,20),(10,40)$;或 $a_1=2, b_1=$

3，d 取 5,10,15，相应的$(a,b)=(10,15),(20,30),(30,45)$；

(ⅳ)若 $a_1+b_1=6$，则 $a_1=1,b_1=5$，d 可取 6，相应的$(a,b)=(6,30)$；

(ⅴ)若 $a_1+b_1=7$，则 $a_1=1,b_1=6$，d 可取 7，相应的$(a,b)=(7,42)$；或 $a_1=2,b_1=5$，d 可取 7，相应的$(a,b)=(14,35)$；或 $a_1=3,b_1=4$，d 可取 7，相应的$(a,b)=(21,28)$；

(ⅵ)若 $a_1+b_1=8$，则 $a_1=3,b_1=5$，d 可取 8，相应的$(a,b)=(24,40)$；

(ⅶ)若 $a_1+b_1=9$，则 $a_1=4,b_1=5$，d 可取 9，相应的$(a,b)=(36,45)$.

以上共找出 23 对数(a,b)满足$(a+b)\mid ab$，且 $1\leqslant a<b\leqslant 50$.但其中只有 24 个不同的数.用 24 个点表示这 24 个数，如果某两数组成上述 23 对数中的某一对，就在表示该数的点间连一条线，这样就得到图 1-1(图中共 24 个点，连 23 条线).图中最多可取到两两不连线的点 12 个.例如取 4,8,16,3,5,9,40,36,15,14,28,7 这 12 个点.与图中未画出的 26 个数，共得 38 个数，这 38 个数组成的 S 的子集中没有任一对数能满足$(a+b)\mid ab$.

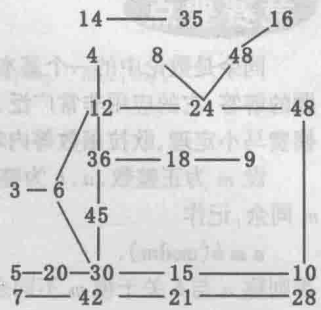

图 1-1

但如取出 S 中任意不少于 39 个元组成的集合 T，则图中至少要取出 13 个数，必有两数可连线，即这两数满足$(a+b)\mid ab$.把图中 1-1 中24 个数分成 12 个数对：(3,6)，(4,12)，(5,20)，(7,42)，(8,24)，(9,18)，(10,40)，(14,35)，(15,30)，(16,48)，(21,28)，(36,45).若取出的 S 的子集元素不少于 39 个，则至多 11 个元未取出，于是上述 12 个数对中至少有一个数对中的两数都被取出，从而就一定有满足$(a+b)\mid ab$ 的数对.

综上所述，$k=39$.

注 此例所采用的解题方法称为构造法.

过关测试

1. 求证：对于任意整数 x，$f(x)=\frac{1}{6}x^3+\frac{5}{6}x$ 都是整数.

2. 设 x 为正整数，求证：$8640\mid(x^9-6x^7+x^5-4x^3)$.

3. 设 n 为整数，求证：$27301\mid(n^{13}-n)$.

4.(1984 全苏竞赛题)有 n 个整数，其积为 n，其和为零.求证：$4\mid n$，反之也成立.

5. 设 p 和 q 是孪生素数，求证：$(p+q)\mid(p^p+q^q)$.

6. 证明：在十进制中，任何一个五位平方数不能用五个相异的偶数(或奇数)的数字来表示.

7. 设 k 是正奇数，求证：$(1+2+\cdots+n)\mid(1^k+2^k+\cdots+n^k)$.

8. 求出所有形如$\overline{30x070y03}$能被 37 整除的自然数.

9. 证明：对每一个不小于 3 的自然数 n，都存在一个自然数 a_n，它可以表示为自己的 n 个互不相同的正约数的和.

10.(1999 年莫斯科竞赛题)整数 a,b,c 使$\frac{a}{b}+\frac{b}{c}+\frac{c}{a}$和$\frac{a}{c}+\frac{c}{b}+\frac{b}{a}$均为整数.求证：$|a|=|b|=|c|$.

11.(《中等数学》2003 年第 5 期训练题)试求出正整数 k 的最小可能值，使得下述命题成立：对于任意的 k 个整数 $a_1,a_2,\cdots,a_k$(允许相等)，必定存在相应的 k 个整数 $x_1,x_2,\cdots,x_k$(也允许相等)，且 $|x_i|\leqslant 2(i=1,2,\cdots,k)$，$|x_1|+|x_2|+\cdots+|x_k|\neq 0$，使得 2003 能整除 $x_1a_1+x_2a_2+\cdots+x_ka_k$.

第2讲 同余及应用

竞赛要点

同余是数论中的一个基本概念,它是整除概念的拓广与发展.同余的引入简化了数论中许多问题的解答,它的应用非常广泛.竞赛大纲中明确地提出了要掌握同余、非负最小完全剩余系概念,掌握费马小定理、欧拉函数等内容.

设 m 为正整数,a,b 为整数(以下均同),若用 m 去除 a,b 所得的余数相同,则称 a 与 b 关于模 m 同余,记作

$$a\equiv b(\mathrm{mod}m). \tag{2-1}$$

否则称 a 与 b 关于模 m 不同余,记作 $a\not\equiv b(\mathrm{mod}m)$,其中 m 称为模,(2-1)式又称作同余式.

定理1 整数 a,b 对模 m 同余的充要条件是

$$m\mid(a-b)(\text{即 } a-b=qm). \tag{2-2}$$

定理2 同余具有如下基本性质(与等式的性质相同或相近):

(1)$a\equiv a(\mathrm{mod}m)$;(反身性) (2-3)

(2)若 $a\equiv b(\mathrm{mod}m)$,则 $b\equiv a(\mathrm{mod}m)$(对称性); (2-4)

(3)若 $a\equiv b(\mathrm{mod}m),b\equiv c(\mathrm{mod}m)$,则 $a\equiv c(\mathrm{mod}m)$(传递性); (2-5)

(4)若 $a\equiv b(\mathrm{mod}m),c\equiv d(\mathrm{mod}m)$,则 $a\pm c\equiv b\pm d(\mathrm{mod}m)$; (2-6)

(5)若 $a\equiv b(\mathrm{mod}m),c\equiv d(\mathrm{mod}m)$,则 $ac\equiv bd(\mathrm{mod}m)$; (2-7)

(6)若 $a\equiv b(\mathrm{mod}m),n\in\mathbf{N}^+$,则 $a^n\equiv b^m(\mathrm{mod}m)$; (2-8)

(7)若 $ac\equiv bc(\mathrm{mod}m),c\neq 0$,则 $a\equiv b\left(\mathrm{mod}\dfrac{m}{(c,m)}\right)$; (2-9)

即只有在 c 与模 m 互质[$(c,m)=1$]时,才能在同余式两边消去 c,而不需要改变模.

(8)若 $a\equiv b(\mathrm{mod}m),m=qn,n\in\mathbf{N}^+$,则 $a\equiv b(\mathrm{mod}n)$; (2-10)

(9)若 $a\equiv b(\mathrm{mod}m_i),i=1,2,\cdots,k$,$m_i$ 的最小公倍数记为$[m_1,m_2,\cdots,m_k]$,则 $a\equiv b(\mathrm{mod}[m_1,m_2,\cdots,m_k])$. (2-11)

关于模 m 同余的一切数的集合,叫做以 m 为模的剩余类(或同余类).在 m 个以 m 为模的相异的剩余类中,各取一个数,所得的 m 个数,叫做模 m 的一个完全剩余系,简称完系.$0,1,2,\cdots,m-1$ 称为模 m 的非负最小完全剩余系或简化剩余系.

定理3 设$(a,m)=1,b$ 是任意整数,若 $x_0,x_1,\cdots,x_{m-1}$ 是模 m 的一个完全剩余系,则 ax_0+b,$ax_1+b,\cdots,ax_{m-1}+b$ 也是模 m 的一个完全剩余系.

对于正整数 m,以 $\varphi(m)$ 表示在 $0,1,\cdots,m-1$ 这 m 个数中与 m 互素的数的个数,则称 $\varphi(m)$ 为欧拉函数.

定理4 (欧拉定理)设 $m>1$ 且为整数,$(a,m)=1$,则

$$a^{\varphi(m)}\equiv 1(\mathrm{mod}m). \tag{2-12}$$

特别地，若$(a,p)=1$，则 $a^{p-1}\equiv 1(\mathrm{mod}p)$. (2-13)

定理5 设正整数 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\varphi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k}). \tag{2-14}$$

定理6 (孙子定理)设正整数 $m_1,m_2,\cdots,m_k$ 两两互质，则对于任意给定的整数 $a_1,a_2,\cdots,a_k$，同余方程组

$$x\equiv a_i(\mathrm{mod}m_i),(i=1,2,\cdots,k) \tag{2-13}$$

一定有解，并且它的全部解可以写成

$$x=a_1b_1m_2m_3\cdots m_k+a_2b_2m_1m_3\cdots m_k+\cdots+a_kb_km_1m_2\cdots m_{k-1}+lm_1m_2\cdots m_{k-1}m_k,$$

其中 b_i 满足 $\frac{m_1m_2\cdots m_k}{m_i}\cdot b_i\equiv 1(\mathrm{mod}m_i),(i=1,2,\cdots,k)$，$l$ 为任一整数.

名题精析

例1 给出一个数能否被11整除的判别方法.

解 因为 $1\equiv 1(\mathrm{mod}11),10\equiv -1(\mathrm{mod}11)$,

$10^2\equiv(-1)^2=1(\mathrm{mod}11),10^3\equiv(-1)^3=-1(\mathrm{mod}11),\cdots\cdots$

$10^n\equiv(-1)^n(\mathrm{mod}11)$.

于是对于数 $A=\overline{a_na_{n-1}\cdots a_1a_0}=a_0+a_1\times 10+\cdots+a_n\times 10^n\equiv$

$a_0-a_1+a_2-\cdots+(-1)^na_n\equiv(a_0+a_2+a_4+\cdots)-(a_1+a_3+a_5+\cdots)(\mathrm{mod}11)$

因此，数 A 能否被11整除，就取决于$(a_0+a_2+\cdots)-(a_1+a_3+\cdots)$能否被11整除，从而得到判别方法：将一个自然数 A 的奇数数位的数字和与偶数数位的数字和相减，当且仅当这个差被11整除时，A 被11整除.

例2 证明：形如11,111,1111,…的数中无平方数.

证明 偶数 $2n$ 的平方是 $4n^2$，奇数 $2n+1$ 的平方为 $(2n+1)^2=4n^2+4n+1$. 所以 $(2n)^2\equiv 0(\mathrm{mod}4),(2n+1)^2\equiv 1(\mathrm{mod}4)$，即平方数除以4，余数为0或1. 而 $11\equiv 111\equiv 1111\equiv\cdots\equiv 3(\mathrm{mod}4)$. 所以，形如11,111,1111,…的数中无平方数.

例3 (1994年澳大利亚竞赛题)证明：对任意整数 x，$\frac{1}{5}x^5+\frac{1}{3}x^3+\frac{7}{15}x$ 是一个整数.

证明 令 $f(x)=15(\frac{1}{5}x^5+\frac{1}{3}x^3+\frac{7}{15}x)=3x^5+5x^3+7x$.

由费马小定理，知 $x^5\equiv x(\mathrm{mod}5),x^3\equiv x(\mathrm{mod}3)$.

于是 $3x^5+5x^3+7x\equiv 3x+7x\equiv 0(\mathrm{mod}5)$,

$3x^5+5x^3+7x\equiv 5x+7x\equiv 0(\mathrm{mod}3)$.

$(3,5)=1$，故 $3x^5+5x^3+7x\equiv 0(\mathrm{mod}15)$，即 $f(x)$ 是15的倍数，从而 $\frac{1}{15}f(x)=\frac{1}{5}x^5+\frac{1}{3}x^3+\frac{7}{15}x$ 是整数.

例4 (1992年友谊杯国际竞赛题)证明：若 n 为大于1的自然数，则 2^n-1 不能被 n 整除.

证明 若 n 为偶数，则 2^n-1 为奇数，显然 $n\nmid(2^n-1)$.

若 n 为奇质数，由费尔马小定理，必有 $2^n\equiv 2(\mathrm{mod}n)$，于是 $2^n-1\equiv 1(\mathrm{mod}n)$，即 $2\nmid(2^n-1)$.

若 n 为奇合数，设 p 为 n 的最小的质因子，则由费尔马小定理，知 $2^{p-1}\equiv 1(\mathrm{mod}p)$. 若 k 是使 $2^k\equiv 1(\mathrm{mod}p)$ 成立的最小自然数，则 $k\mid(p-1)$. 于是 $2\leqslant k\leqslant p-1$，这说明 k 不是 n 的约数，即 $k\nmid n$.

设 $n=kq+r$（q 为整数，$0<r<k$），则 $2^n\equiv 2^r\not\equiv 1(\mathrm{mod}p)$（否则与 k 的最小性矛盾）. 这就是说 $2^n-1\not\equiv 0(\mathrm{mod}p)$，$p\nmid(2^n-1)$，从而 $n\nmid(2^n-1)$. 综上，命题获证.

例 5 求数 7^{99} 被 2550 除所得的余数.

解 注意到 $2550=50\times 51$，而 50 与 51 互质，故先求出 7^{99} 分别被 50 和 51 除所得的余数.

$$7^{99}=7\times 7^{98}=7\times 49^{49}\equiv 7\times(-2)^{49}\equiv -14\times(-2)^{4\times 12}\equiv -14\times 16^{12}$$
$$\equiv -14\times 256^6\equiv -4\times 1^6\equiv -14(\mathrm{mod}51)$$
$$7^{99}=7\times 49^{49}\equiv 7\times(-1)^{49}\equiv -7(\mathrm{mod}50)$$

记 $x=7^{99}$，则 $\begin{cases}x\equiv -14(\mathrm{mod}51),\\ x\equiv -7(\mathrm{mod}50).\end{cases}$ （*）

于是，$\begin{cases}50x\equiv -14\times 50(\mathrm{mod}2550),\\ 51x\equiv -7\times 51(\mathrm{mod}2550).\end{cases}$

再由两式相减得 $x\equiv -7\times 51-(-14)\times 50\equiv 343(\mathrm{mod}2550)$，即 7^{99} 被 2550 除后余数为 343.

注 对于（*）式也可运用定理 6 求解.

例 6 （IMO－30 试题）求证：对任何正整数 n，存在 n 个相继的正整数，它们都不是素数的正整数幂.

分析 如果能证明存在 n 个相继正整数，它们中的每一个都能被至少两个不同素数的乘积整除，显然这 n 个相继正整数就都不是素数的正整数幂.

证明 取 $2n$ 个不同的素数 $p_1,p_2,\cdots,p_n;q_1,q_2,\cdots,q_n$，则由定理 6，同余方程组

$$\begin{cases}x\equiv -1(\mathrm{mod}p_1q_1),\\ x\equiv -2(\mathrm{mod}p_2q_2),\\ \cdots\cdots\\ x\equiv -n(\mathrm{mod}p_nq_n).\end{cases}$$

有解. 设此解为 m，则 $m+1,m+2,\cdots,m+n$ 是 n 个相继正整数，它们中的每一个都至少含有两个不同的素因数，因而，每一个都不是素数的正整数幂.

例 7 （1969 年普特南竞赛题）设 n 为自然数，$n+1$ 能被 24 整除. 求证：n 的全体约数的和也能被 24 整除.

证明 由 $24\mid(n+1)\Leftrightarrow\begin{cases}n\equiv -1(\mathrm{mod}3),\\ n\equiv -1(\mathrm{mod}8).\end{cases}$

设 $d\mid n$，则 $d\equiv 1$ 或 $2(\mathrm{mod}3)$，$d\equiv 1,3,5$ 或 $7(\mathrm{mod}8)$.

再由 $d\cdot\dfrac{n}{d}=n\equiv -1(\mathrm{mod}3)$ 或 $(\mathrm{mod}8)$，即知仅有下列几种可能情形出现：

$d\equiv 1,\dfrac{n}{d}\equiv 2(\mathrm{mod}3)$，反之亦然；

$d\equiv 1,\dfrac{n}{d}\equiv 7(\mathrm{mod}8)$，反之亦然；

$d\equiv 3,\dfrac{n}{d}\equiv 5(\mathrm{mod}8)$，反之亦然.

上列各种情形都符合

$d+\frac{n}{d}\equiv 0(\mathrm{mod}3)$及$(\mathrm{mod}8)\Rightarrow d+\frac{n}{d}\equiv 0(\mathrm{mod}24)$.

因为$d\neq\frac{n}{d}$,所以n的约数两两互异.这就证明了n的全体约数的和能被24整除.

例8 (2003年全国高中联赛加试题)设三角形的三边长分别是整数l,m,n,且$l>m>n$.已知$\{\frac{3^l}{10^4}\}=\{\frac{3^m}{10^4}\}=\{\frac{3^n}{10^4}\}$,其中$\{x\}=x-[x]$,而$[x]$表示不超过$x$的最大整数.求这种三角形周长的最小值.

解 由题设可知$\frac{3^l}{10^4}-[\frac{3^l}{10^4}]=\frac{3^m}{10^4}-[\frac{3^m}{10^4}]=\frac{3^n}{10^4}-[\frac{3^n}{10}]$,于是

$$3^l\equiv 3^m\equiv 3^n(\mathrm{mod}10^4)\Leftrightarrow\begin{cases}3^l\equiv 3^m\equiv 3^n(\mathrm{mod}2^4), & ①\\ 3^l\equiv 3^m\equiv 3^n(\mathrm{mod}5^4). & ②\end{cases}$$

由于$(3,2)=(3,5)=1$,则由①可知$3^{l-n}\equiv 3^{m-n}\equiv 1(\mathrm{mod}2^4)$.

设u是满足$3^u\equiv 1(\mathrm{mod}2^4)$的最小正整数,则对任意满足$3^v\equiv 1(\mathrm{mod}2^4)$的正整数$v$,有$u\mid v$,即$u$整除$v$.事实上,若$u\nmid v$,则由带余除法可知,存在非负整数$a$及$b$,使得$v=au+b$,其中$0<b\leqslant u-1$.从而,可推出$3^b\equiv 3^{b+au}\equiv 3^v\equiv 1(\mathrm{mod}2^4)$,而这显然与$u$的定义矛盾.所以,$u\mid v$.

注意到$3\equiv 3(\mathrm{mod}2^4)$,$3^2\equiv 9(\mathrm{mod}2^4)$,$3^3\equiv 27\equiv 11(\mathrm{mod}2^4)$,$3^4\equiv 1(\mathrm{mod}2^4)$.从而,可设$m-n=4k$,其中$k$为正整数.

同理,由②推出$3^{m-n}\equiv 1(\mathrm{mod}5^4)$.故$3^{4k}\equiv 1(\mathrm{mod}5^4)$.

下面求满足$3^{4k}\equiv 1(\mathrm{mod}5^4)$的正整数$k$.

因为$3^{4k}-1=(1+5\times 2^4)^k-1\equiv 0(\mathrm{mod}5^4)$,即

$$5k\times 2^4+\frac{k(k+1)}{2}\times 5^2\times 2^8+\frac{k(k-1)(k-2)}{6}\times 5^3\times 2^{12}\equiv$$

$$5k+5^2k[3+(k-1)\times 2^7]+\frac{k(k-1)(k-2)}{3}\times 5^3\times 2^{11}\equiv 0(\mathrm{mod}5^4). \quad (*)$$

从而 $k=5t$,并代入上式得

$t+5t[3+(5t-1)\times 2^7]\equiv 0(\mathrm{mod}5^2)$.

所以,$t\equiv 0(\mathrm{mod}5^2)$.

从而,$k=5t=5^3s$,其中s为正整数,故$m-n=500s$,s为正整数.

同理,可证$l-n=500r$,r为正整数.

由于$l>m>n$,所以,$r>s$.

于是,三角形三边为$500r+n$,$500s+n$和n.故有$n>500(r-s)$,因此,当$s=1$,$r=2$,$n=501$时,三角形周长最小,其值为$(1000+501)+(500+501)+501=3003$.

注 $(*)$式中,运有前一式我们应用到的公式:$(a+b)^k=a^k+k\cdot a^{k-1}\cdot b+\frac{k(k-1)}{2}\cdot a^{k-2}\cdot b^2+\frac{k(k-1)(k-2)}{6}\cdot a^{k-3}\cdot b^3+\frac{k(k-1)(k-2)(k-3)}{24}\cdot a^{k-4}\cdot b^4+\cdots+b^k$,其中$a=1$,$b=5\times 2^4$.

例9 (IMO-40预选题)设n,k是正整数,且n不能被3整除,$k\geqslant n$.证明:存在正整数m,使得m可被n整除,且它的各位数字之和是k.

证明 设$n=2^a5^bp$,其中a,b是非负整数,且$(p,10)=1$.只要证明存在正整数M满足$p\mid M$,且M的各位数字之和等于k.实际上,只要设$m=M\cdot 10^c$,其中c为a,b中较大的一个,即$c=\max\{a,$

b|.

因为$(p,10)=1$,由定理4(欧拉定理),知存在正整数$d\geqslant 2$,使得$10^d\equiv 1(\mathrm{mod}p)$.

对于每个非负整数i,j,有

$10^{id}\equiv 1(\mathrm{mod}p)$,$10^{id+1}\equiv 10(\mathrm{mod}p)$.

设$M=\sum_{i=1}^{u}10^{id}+\sum_{j=1}^{v}10^{jd+1}$,其中如果$u$或$v$是0,则对应的和为0.

由于$M\equiv u+10v(\mathrm{mod}p)$,设$\begin{cases}u+v=k,\\ p\mid(u+10v),\end{cases}\Rightarrow\begin{cases}u+v=k,\\ p\mid(k+9v).\end{cases}$ (*)

因为$(p,3)=1$,则$k,k+9,k+18,\cdots,k+9(p-1)$模$p$的剩余之一一定是零.于是,存在某个正整数$v_0$,且$0\leqslant v_0<p$,满足(*)式.

设$u_0=k-v_0$,则由u_0,v_0所确定的M满足前面所要求的条件.

例10 (数学通报问题1256)求$7^{7^{\cdot^{\cdot^{\cdot 7}}}}$($n$个7,$n\geqslant 3$)的末四位数.

分析 即求满足$7^{7^{\cdot^{\cdot^{\cdot 7}}}}\equiv a(\mathrm{mod}10000)$的$a$.

解 因$7^4\equiv 1(\mathrm{mod}100)$,有对正整数$x$,$7^{4x}\equiv 1(\mathrm{mod}100)$.

又 $7\equiv -1(\mathrm{mod}4)$,故$7^7\equiv(-1)^7\equiv -1(\mathrm{mod}4)$.

因而 $7^{7^{\cdot^{\cdot^{\cdot 7}}}}$($n-1$个7,$n-1\geqslant 2$)$\equiv(-1)(\mathrm{mod}4)$.

于是可设$7^{7^{\cdot^{\cdot^{\cdot 7}}}}$($n-1$个7,$n-1\geqslant 2$)$=4x+3$,$x\in\mathbf{N}^+$,则

$7^{7^{\cdot^{\cdot^{\cdot 7}}}}\equiv 7^{4x+3}\equiv 7^3\equiv 43(\mathrm{mod}100)$.

从而可设 $7^{7^{\cdot^{\cdot^{\cdot 7}}}}$($n$个7,$n\geqslant 3$)$=7^{100m+43}$,$m\in\mathbf{N}^+$, ①

而 $7^4\equiv 2401(\mathrm{mod}10000)$,则

$7^8\equiv 4801(\mathrm{mod}10000)$,$7^{16}\equiv 9601(\mathrm{mod}10000)$,

$7^{32}\equiv 9201(\mathrm{mod}10000)$,$7^{64}\equiv 8401(\mathrm{mod}10000)$.

则 $7^{32}\cdot 7^{64}=7^{96}\equiv 7601(\mathrm{mod}10000)$.

故 $7^{100}=7^4\cdot 7^{96}\equiv 2401\cdot 7601\equiv 1(\mathrm{mod}10000)$.

$7^{100m}\equiv 1(\mathrm{mod}10000)$. ②

所以,由①、②得 $7^{7^{\cdot^{\cdot^{\cdot 7}}}}\equiv 7^{100m+43}\equiv 7^{43}(\mathrm{mod}10000)$. ③

又 $7^{40}=7^{32}\cdot 7^8\equiv 9201\cdot 4801\equiv 4001(\mathrm{mod}10000)$,易知$7^3=343$,所以$7^{43}=7^3\cdot 7^{40}\equiv 343\cdot 4001\equiv 2343(\mathrm{mod}10000)$. ④

由③、④得,$7^{7^{\cdot^{\cdot^{\cdot 7}}}}$的末四位数是2343.

例11 对任意正整数n,k,令$s=1^n+2^n+\cdots+k^n$.求s被3除所得的余数.

解 (ⅰ)当n为奇数时,不妨设$n=2l-1$,$l\in\mathbf{N}^+$.对$m\in\mathbf{N}^+$,如果3$\nmid m$,则$m^2\equiv 1(\mathrm{mod}3)$,即$m^{2l}\equiv 1(\mathrm{mod}3)$,亦即$m^{2l-1}\equiv m^{2(l-1)+1}\equiv m(\mathrm{mod}3)$;

如果$3\mid m$,则$m^{2l-1}\equiv 0\equiv m(\mathrm{mod}3)$.

于是,当n为奇数时,对$m\in\mathbf{N}^+$,总有$m^n\equiv m(\mathrm{mod}3)$,从而$s\equiv 1+2+\cdots+k\equiv(1+2+3)+(4+5+6)+\cdots(\mathrm{mod}3)$.

设$t\in\mathbf{N}^+$,则当$k=3t+3$或$k=3t+2$时,就有$s\equiv 0(\mathrm{mod}3)$.

当$k=3t+1$时,就有$s\equiv(1+2+3)+\cdots+[(k-3)+(k-2)+(k-1)]+k\equiv 1(\mathrm{mod}3)$.

(ⅱ)当 n 为偶数时,对 $m\in\mathbf{N}^+$,由(ⅰ)知,$3\nmid m\Rightarrow m^2\equiv 1(\mathrm{mod}3)$;$3\mid m\Rightarrow m^2\equiv 0(\mathrm{mod}3)$.于是

$s\equiv(1+1+0)+(1+1+0)+\cdots(\mathrm{mod}3)$.

设 $t\in\mathbf{N}^+$,则当 $k=3t+3$ 时,$(1+1+0)$共有 $t+1$ 组,故

$s\equiv(t+1)(1+1+0)\equiv 2t+2(\mathrm{mod}3)$;

当 $k=3t+2$ 时,$(1+1+0)$共有 t 组,且$(k-1)^n\equiv k^n\equiv 1(\mathrm{mod}3)$,故 $s\equiv 2t+1+1\equiv 2t+2(\mathrm{mod}3)$;

当 $k=3t+1$ 时,$(1+1+0)$共有 t 组,且 $k^n\equiv 1(\mathrm{mod}3)$,故 $s\equiv 2t+1(\mathrm{mod}3)$.

综合(ⅰ),(ⅱ)知,当 n 为正奇数时,$s\equiv\begin{cases}0,k=3t+3\text{ 或 }3t+2\\1,k=3t+1\end{cases}(\mathrm{mod}3)$;

当 n 为正偶数时,$s\equiv\begin{cases}2t+2,k=3t+3\text{ 或 }3t+2\\2t+1,k=3t+1\end{cases}(\mathrm{mod}3)$.

例 12 (IMO-34 预选题)对于正整数 n,如果对于任何整数 a,只要 $n\mid(a^n-1)$,就有 $n^2\mid(a^n-1)$,则称 n 具有性质 p.求证:(1)每个质数 n 都具有性质 p;(2)有无穷多个合数也都具有性质 p.

证明 (1)设 $n=p$ 为质数,且 $p\mid(a^p-1)$,于是$(a,p)=1$.但 $a^p\equiv a(\mathrm{mod}p)$,即 $p\mid(a^p-a)$.

而 $a^p-a=a^p-1-(a-1)$,故得 $p\mid(a-1)$,即 $a\equiv 1(\mathrm{mod}p)$,于是 $a^i\equiv 1(\mathrm{mod}p)(i=0,1,2,\cdots,p-1)$.故

$1+a+a^2+\cdots+a^{p-1}\equiv 0(\mathrm{mod}p)$.

于是 $p^2\mid(a-1)(a^{p-1}+a^{p-2}+\cdots+a^2+a+1)$,即 $p^2\mid(a^p-1)$.

(2)若 $n\mid(a^n-1)$,则$(n,a)=1$,故 $a^{\varphi(n)}\equiv 1(\mathrm{mod}n)$.

又 $a^n\equiv 1(\mathrm{mod}n)$,故 $a^{(n,\varphi(n))}\equiv 1(\mathrm{mod}n)$.

此时,如果$[n,\varphi(n)]=1$,则有 $a\equiv 1(\mathrm{mod}n)$,如(1)所证,必有 $n^2\mid(a^n-1)$.问题转化为求出无穷多个合数 n,使$[n,\varphi(n)]=1$.

如果 n 的标准分解式中,任一质因数 p 的次数$\geqslant 2$,则$[n,\varphi(n)]\neq 1$,故为简单计,取 $n=pq(p,q$ 为不等的质数且$p\geqslant 5)$,则 $\varphi(n)=(p-1)(q-1)$.因此,必须 $p\nmid(q-1)$,$q\nmid(p-1)$.现取 $p-2$ 的质因数 q,则因 $q\mid(p-2)$,故 $q\nmid(p-1)$,从而 $q\nmid p$.同时 $p\nmid(q-1)$.此时,必有$[n,\varphi(n)]=1$.从而 $n=pq$ 具有性质 p.

再取一个大于 pq 的质数,则按上法又可得一个具有性质 p 的合数.仿此下去,即可得无穷多个具有性质 p 的合数.

例 13 (第 28 届美国奥林匹克题)设 p 是素数,$p>2$,a,b,c,d 是不能被 p 整除的整数,并且满足对于任意一个不能被 p 整除的整数 r 均有

$$\left\{\frac{ra}{p}\right\}+\left\{\frac{rb}{p}\right\}+\left\{\frac{rc}{p}\right\}+\left\{\frac{rd}{p}\right\}=2.$$

证明 $a+b,a+c,a+d,b+c,b+d,c+d$ 这六个数中至少有两个数能被 p 整除.其中$\{x\}=x-[x]$.

证明 因 $p\nmid d$,所以 $0,d,2d,\cdots,(p-1)d$ 构成了关于 p 的完全剩余系,其中必有 $R\in\{1,2,\cdots,p-1\}$,使得 $Rd\equiv p-1(\mathrm{mod}p)$.

设 $Ra\equiv A(\mathrm{mod}p)$,$Rb\equiv B(\mathrm{mod}p)$,$Rc\equiv C(\mathrm{mod}p)$,$Rd\equiv D(\mathrm{mod}p)$,$(A,B,C,D\in\{1,2,\cdots,p-1\})$.

不妨设 $A\leqslant B\leqslant C\leqslant D$,假设 $A\neq 1$,由于对任意 r,$p\nmid r$,都有$\left\{\frac{ra}{p}\right\}+\left\{\frac{rb}{p}\right\}+\left\{\frac{rc}{p}\right\}+\left\{\frac{rd}{p}\right\}=2$.