正交表的构造

杨子胥编

山东人民出版社

正交表的构造

杨子胥编

山东人民出版社出版
济南红卫印刷厂印刷
山东省新华书店发行

1978年8月第1版　1978年8月第1次印刷
统一书号：13099·77　定价：0.60元

前　言

正交试验法，在工农业生产和科学实验中，是一种帮助设计较为合理的实验方案的科学方法。它根据数学原理，利用一种规格化的表格——“正交表”，仅作较少次数的试验，便能得出较为明确可靠的结论。

为了让广大工农兵和科技人员掌握正交表的构造原理及其构造方法，使正交试验法进一步普及推广，在院党委的领导和大力支持下，根据自己多年的教学和推广正交试验法的实践，编写了《正交表的构造》这本书。本书共分五章，较系统地介绍了二水平正交表、$L_{t2}(t^m)$型正交表、$L_{t^u}(t^m)$型正交表、$L_{\lambda p^2}(p^{\lambda p+1})$型正交表等的构造原理及其构造方法；对造正交表时用到的代数基本知识也作了介绍；书后还附有正交表使用简介及常用正交表。可供广大工农兵、科技人员、大专院校师生阅读参考。

由于编者水平有限，书中难免有不当之处，恳请广大读者批评指正。

编　者　于山东师范学院聊城分院

一九七八年三月

目　录

第一章　代数基本知识

在构造各种类型的正交表时，需要用到代数方面的同余、群、有限域、向量空间、行列式及矩阵等基本知识，本章将分别加以介绍．讲述这些基本知识所涉及到的一些性质和定理，多数都作了详细证明，但也有一部分只列出结果，而没有证明．如需要了解这方面内容时，可查阅一般的高等代数或近世代数．

§1　同　余

同余，是在构造正交表时，要用到的最基本的概念之一．在介绍同余以前，先来熟悉一下有关整数的一些基本性质．

定义1　设a与b是两个整数，如果存在整数c，使

$$a=bc,$$

则称b整除a，或称a被b所整除，并且记为$b|a$．

当b不能整除a时，则记为$b\nmid a$．

当b整除a时，就称b是a的一个因数，而称a是b的一个倍数．

要判断一个正整数能不能整除另一个正整数，只需作普通除法，看是不是能除尽就可以了．能除尽时，就是能整除；否则，就是不能整除．但是，应该注意，现在是在整数范围内来讨论这一问题的．就是说，现在的讨论不仅包括正整数，

而且，还要包括负整数和零，范围已扩大了．虽然如此，但要判断一个整数能否整除另一个整数时，仍然归结到正整数的普通除法．

定理1 设a与b是两个整数，则$b\mid a$当且仅当$|b|\mid|a|$．即b整除a当且仅当b的绝对值整除a的绝对值．

证明：若$b\mid a$，可设

$$a=bc,\ c\text{为整数}.$$

两边取绝对值，可得

$$|a|=|b|\cdot|c|.$$

这就是说，$|b|\mid|a|$．

反之，若$|b|\mid|a|$，可设

$$|a|=|b|q,\ q\text{为整数}.$$

由此可得$q\geqslant 0$，于是有

$$|a|=|bq|.$$

由此可得

$$a=bq\text{ 或 }a=b(-q),$$

这就是说，$b\mid a$．（证完）

这个定理说明，要看是否$b\mid a$，只要看是否$|b|\mid|a|$．

例如，由于$4\mid 12$，所以便有

$$-4\mid 12,\quad 4\mid -12,\quad -4\mid -12;$$

又由于$4\nmid 18$，故便有

$$-4\nmid 18,\quad 4\nmid -18,\quad -4\nmid -18,$$

等等．

整数的整除有以下基本性质：

1.对任何整数 a，总有 $a|a$；

2.若 $c|b$，$b|a$，则必有 $c|a$；

3.若 $c|a$，$c|b$，则必有 $c|a\pm b$；

4.若 $b|a$，则对任意整数 c，必有 $b|ac$.

这些性质以后将经常用到，

定义 2 若整数 c 既是 a 的因数，也是 b 的因数，则称 c 为 a 与 b 的公因数.

a 与 b 的公因数中最大的，叫做 a 与 b 的最大公因数.

a 与 b 的最大公因数常用符号 (a,b) 表示.

由于 a 与 b、$-a$ 与 b、a 与 $-b$ 以及 $-a$ 与 $-b$ 四者都有完全相同的公因数，从而，它们就有相同的最大公因数.这样，就可以利用熟知的辗转相除法来求任意两整数的最大公因数.

关于整数的最大公因数，还有以下重要事实：

定理 2 设 d 是 a 与 b 的最大公因数，则存在二整数 s,t，使

$$as+bt=d.$$

这个定理不再证明了.

当 $(a,b)=1$，即 a 与 b 的最大公因数是 1 时，则称 a 与 b 互质.

由定理 2 不难推出，二整数 a 与 b 互质的充分与必要条件是，存在二整数 s 与 t，使

$$as+bt=1.$$

定义 3 设 p 是一个大于 1 的整数，如果 p 没有 1 及 p 以外的正因数，则称 p 是一个素数（或质数）；否则，称 p 是一个合数.

由此可见，当 a 是一个合数时，a 必定可以写成两个大于 1 且小于 a 的整数的乘积.

素数有无限多.200以内的素数有46个，它们是：

2、3、5、7、11、13、17、19、23、29、31、37、41、43、47、53、59、61、67、71、73、79、83、89、97、101、103、107、109、113、127、131、137、139、149、151、157、163、167、173、179、181、191、193、197、199.

显然，2是素数中唯一的一个偶数；其余的素数全是奇数，以后常称其为奇素数.

素数以及互质有以下重要性质：

1.若$a|bc$，但$(a, b)=1$，则必有$a|c$.

证明：因为$(a, b)=1$，故存在二整数s与t，使

$$as+bt=1.$$

两边乘以c，得

$$acs+bct=c.$$

由于$a|acs$及假设$a|bc$，从而，根据整除性质知，

$$a|(acs+bct)=c.$$

即有$a|c$.　　（证完）

2.设p是一个素数，则对任一整数a，或者$(p,a)=1$，或者$p|a$.

证明：设$(p,a)=d$，则有$d|p$.

但由于p是一个素数，故只有

$$d=1 \quad 或 \quad p.$$

当$d=1$时，有$(p,a)=1$；当$d=p$时，则有$p|a$.（证完）

3.设p是一个素数，若$p|ab$，则必有$p|a$或$p|b$.

证明：因为p是一个素数，当$p\nmid a$时，则由性质2知，必有$(p, a)=1$，从而又由性质1知，

$$p|b.$$　　（证完）

对性质3可进一步推广：若素数 $p|ab\cdots c$，则 p 至少可整除 a，b，…，c 中的一个.

4.若 $a|c$，$b|c$，但 $(a, b)=1$，则必有 $ab|c$.

证明：因为 $a|c$，故可设

$$c=ad,\ d\text{是整数}.$$

又因为 $b|c$，从而 $b|ad$.但由假设 $(a, b)=1$，从而由性质1知，$b|d$.设

$$d=bq,\ q\text{是整数}.$$

从而有

$$c=ad=(ab)q.$$

即有 $ab|c$.　　（证完）

对性质4可进一步推广：若 $a_1|c$，$a_2|c$，…，$a_n|c$，但 a_1, a_2，…，a_n 两两互质，则必有

$$a_1a_2\cdots a_n|c.$$

以上四个基本性质，也是以后经常用到的.

定理3　（唯一分解定理）任意一个合数都可以分解成素数的乘积，并且，这种分解基本上是唯一的.

证明：设 a 是一个合数，并且

$$a=b_1b_2,\ \text{其中}\ 1<b_1,\ b_2<a.$$

若 b_1, b_2 已是素数，则分解便已完成；若 b_1 与 b_2 中有一个或两个都不是素数，而为合数，于是，可继续进行分解.

由于这种分解中的因数一次比一次小，但又都大于1，因此总会遇到不能再分解的时候.而这种不能再分解的因数，当然都是素数.这就是说，每一个合数都一定可以分解成素因数的乘积.

其次，设

$$a=p_1p_2\cdots p_r,\quad a=q_1q_2\cdots q_s$$

都是a的素因数分解式，要证明必有$r=s$，并且，在适当调换素因数的次序后，可以有

$$p_i=q_i,\ i=1,\ 2,\ \cdots,r.$$

事实上，因为有

$$p_1p_2\cdots p_r=q_1q_2\cdots q_s,\qquad (1)$$

从而，$q_1\mid p_1p_2\cdots p_r$. 但由于q_1是素数，故q_1必整除$p_1,p_2,\cdots,p_r$中的一个.经适当调换素因数的次序后，不妨假定

$$q_1\mid p_1,$$

那么，由于p_1也是素数，故必有$q_1=p_1$.

这样，在（1）的两边可消去p_1，便得

$$p_2p_3\cdots p_r=q_2q_3\cdots q_s.\qquad (2)$$

同理，由$q_2\mid p_2p_r\cdots p_r$，可类似地推得$p_2=q_2$. 再从(2)式两边消去p_2，等等.

如此继续下去，便可把两种分解中的素数一对对地消去，而且不可能一边消完，而另一边还剩有素数（因为素数及其乘积不可能等于1）.这就是说，必有$r=s$，而且由上可知

$$p_1=q_1,\ p_2=q_2,\ \cdots,\ p_r=q_r.\qquad (证完)$$

在一个整数的素因数分解式中，有些素数可能是相同的；如果我们把相同的素因数合并成方幂，比方假定为

$$a=p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m},$$

其中$p_1,p_2,\cdots,p_m$为互不相同的素数，而$k_1,k_2,\cdots,k_m$为正整数；则我们称这种分解为a的典型分解式.

例如，由于

$$600=2\times2\times2\times3\times5\times5,$$

将相同的素因数合并后，即得600的典型分解式如下：

$$600 = 2^3 \cdot 3 \cdot 5^2.$$

关于整数的性质暂时讨论到这里．下面再来讨论同余的概念．

设m为任意一个固定的大于1的整数，则任意整数a都可以唯一地表示为

$$a = mq + r,$$

其中q与r都是整数，并且$0 \leqslant r < m$．

我们分别称q与r为a除以m所得的商和余数．

当a是一个正整数时，可以用通常的除法，求出a除以m所得的商和余数．但是，当a是负整数时，如何求其商和余数呢？方法如下：

由于此时$-a$是正整数，故可按通常除法，求出$-a$除以m所得的商和余数q，r，使

$$-a = mq + r, \quad 0 \leqslant r < m.$$

当$r = 0$时，有

$$a = m(-q),$$

从而，$m \mid a$，即此时a除以m所得的商是$-q$，余数是0．

当$r \neq 0$时，有

$$a = m(-q-1) + (m-r), \quad 0 < m-r < m.$$

即此时的商和余数分别为$-q-1$与$m-r$．

例如，当取$m = 6$时，由于有

$$19 = 6 \cdot 3 + 1,$$

所以有

$$-19 = 6 \cdot (-4) + 5.$$

即-19除以6所得的商是-4，余数是5．

定义4 若二整数a与b用m除，所得的余数相同，就称a与b对模m同余，并且记为

$$a \equiv b \pmod{m}.$$

例如，42与50，用8除所得的余数相同，都是2，所以42与50对模8同余，用上面的符号表示

$$42 \equiv 50 \pmod{8}.$$

又如，-19与23用6除所得的余数也相同，都是5，故有

$$-19 \equiv 23 \pmod{6}.$$

关于同余，以下三个基本性质显然是成立的（均对同一模数m而言）：

1.对任何整数a，都有$a \equiv a$；

2.若$a \equiv b$，则有$b \equiv a$；

3.若$a \equiv b$，$b \equiv c$，则有$a \equiv c$.

根据定义，要判断两个正整数是不是同余，可以用同一模数去除，看它们的余数是否相同，相同则同余，不相同则不同余.而对于负整数，也可以按照上面求商和余数的方法来判断.

但是，一般来讲，按照下面定理所指出的方法来判断则更方便一些.

定理4 对模m来说，二整数a与b同余的充分与必要条件是

$$m \mid a-b.$$

证明： 设

$$a = mq_1 + r_1, \quad 0 \leqslant r_1 < m,$$

$$b = mq_2 + r_2, \quad 0 \leqslant r_2 < m,$$

两式相减，得

$$a - b = m(q_1 - q_2) + (r_1 - r_2).$$

若a与b同余，即有$r_1=r_2$，从而由上式知，$m|a-b$.

反之，设$m|a-b$，同样由上式知，有

$$m|r_1-r_2.$$

但由于$0\leqslant r_1, r_2<m$,所以，只有$r_1=r_2$，即a与b对模 m 同余. （证完）

例如，由于

$$9|27=16-(-11),$$

根据定理 4，就有 $16\equiv -11\ (mod\ 9)$.

特别，由定理 4 可推出以下的同余性质（均对同一模数m而言）：

1.若$a\equiv b$，则$ka\equiv kb$，即同余式两边可同乘任一整数.

证明：因为$a\equiv b$，所以由定理 4，得$m|a-b$.

从而，由整除性质知，

$$m|k(a-b)=ka-kb.$$

即$m|ka-kb$，于是有$ka\equiv kb$. （证完）

2. 若$ka\equiv kb$，且$(k, m)=1$，则$a\equiv b$.

证明：因为$ka\equiv kb$,故由定理 4,得$m|k(a-b)$. 但由于$(k,m)=1$,故由互质的性质1知,$m|a-b$,从而有$a\equiv b$.(证完)

这个性质说明，在同余式两边不能随便约去同一个数.

例如，虽然有

$$12\equiv 6\ (mod\ 3),$$

但是却有 $2\not\equiv 1\ (mod\ 3)$.

即不能约去 6，因为 6 与 3 不互质.

3.若$a_1\equiv b_1$，$a_2\equiv b_2$，则有$a_1\pm a_2\equiv b_1\pm b_2$，$a_1a_2\equiv b_1b_2$.

证明：因为$a_1\equiv b_1$，$a_2\equiv b_2$，故有

$$m|a_1-b_1,\quad m|a_2-b_2.$$

从而，根据整除性质，有

$$m|[(a_1-b_1)+(a_2-b_2)],\ m|[(a_1-b_1)-(a_2-b_2)].$$

即$m|[(a_1+a_2)-(b_1+b_2)]$，$m|[(a_1-a_2)-(b_1-b_2)]$，从而有

$$a_1+a_2\equiv b_1+b_2,\ a_1-a_2\equiv b_1-b_2.$$

其次，由于$a_1\equiv b_1$，$a_2\equiv b_2$，故由同余性质1，可得$a_1a_2\equiv b_1a_2$与$b_1a_2\equiv b_1b_2$，从而有$a_1a_2\equiv b_1b_2$．（证完）

4．若$a+b\equiv c$，则$a\equiv c-b$，即普通移项规则对同余式成立．

证明：因为$a+b\equiv c$，$b\equiv b$，从而由同余性质3知，$a\equiv c-b$．（证完）

5．若$a\equiv b$，则有$a+ms\equiv b+mt$．就是说，在同余式两边可以任意加上或减去模数的整倍数．

证明：由$a\equiv b$可得$m|a-b$，从而可得

$$m|[(a+ms)-(b+mt)],$$

于是，由定理4可得$a+ms\equiv b+mt$．（证完）

6．若$a\equiv 0$，则$m|a$；反之也成立．

这个性质可由定理4直接推出．

从上面的讨论可以看出，同余式的这些性质和通常等式的性质，可以说基本上是相同的．但是，我们也应该注意到它们的区别，特别是性质2、5与6．这在今后的讨论中要经常用到．

§2 群的初步知识

在普通代数里，我们计算的对象是数，计算的方法也多半是普通的加减乘除．但是，在数学以及其他的一些学科中，却也常常遇到一些计算的对象不一定是数，而计算的方法也不一定是普通的加减乘除．例如，我们所熟知的多项式加法与乘法运算就属于这种情形；在构造各种类型的正交表时，也将经常遇到这种情形．因此，从这一节开始，将陆续介绍这些内容．

先来介绍代数运算的概念．

定义1 设M是至少包含一个元素的集合，如果有一个法则，它对于M中任意两个有次序的元素a与b，在M中总有一个唯一确定的元素c与之对应，则称这个法则为集合M的一个代数运算。

代数运算可用一个记号，例如"$\circ$"来表示，并且把a与b所对应的元素c记为$a\circ b$，即

$$a\circ b=c,$$

这就是说，对于M中任意两个有次序的元素a与b，通过运算"$\circ$"，可以"算"出一个元素c，而这个c又必须属于集合M.

例1 令M是全体有理数（或全体实数、复数）的集合，则数的普通加法、减法与乘法都是M的代数运算．这是因为，有理数相加、相减、相乘的结果均仍为有理数．

例2 令$M=\{1,\ 2,\ 3,\ 4\cdots\cdots\}$，即全体正整数的集合．

当然，数的普通加法与乘法也都是它的代数运算，因为

正整数相加、相乘的结果均仍为正整数.但是，应该注意，由于正整数相减得到的结果不一定是正整数，因此，普通减法不是正整数集合的代数运算.

下面，我们将给出正整数集合的另一个代数运算.

对任意两个正整数a，b，规定：

$$a \bigcirc b = a^b.$$

则这个法则"$\bigcirc$"是正整数集合M的一个代数运算.这是因为，对任意两个正整数a与b，通过"$\bigcirc$"所得到的结果a^b也是一个正整数.例如，有

$$1 \bigcirc 2 = 1^2 = 1，\ 2 \bigcirc 1 = 2^1 = 2，\ 3 \bigcirc 4 = 3^4 = 81,$$

等等.

例3 令$M = \{0，\ 1，\ 2，\ 3，\ 4\}$.

显然，数的普通加法不是这个集合的一个代数运算，因为，例如1，4虽然属于M（今后写成$1 \in M$，$4 \in M$），但是，$1 + 4 = 5$却不属于M（今后记为$5 \notin M$）.

现在，对这个集合M规定一个新的运算规则，使它成为M的一个代数运算.

设a，$b \in M$，我们规定：

$a \oplus b =$（$a+b$）除以5所得的余数.

由于任何整数除以5，所得的余数只能是0，1，2，3，4中的一个，所以这个法则是这个集合的一个代数运算.

例如，根据这个法则可得

$1 \oplus 1 = 2$，$1 \oplus 2 = 3$，$1 \oplus 3 = 4$，$1 \oplus 4 = 0$，$2 \oplus 2 = 4$，$2 \oplus 3 = 0$，$2 \oplus 4 = 1$，$3 \oplus 3 = 1$，$3 \oplus 4 = 2$，$4 \oplus 4 = 3$，

等等.