经济转型与创新发展论丛

电子商务数学建模

刘英卓 著

南京大学出版社

经济转型与创新发展论丛

电子商务数学建模

刘英卓 著

南京大学出版社

图书在版编目(CIP)数据

电子商务数学建模 / 刘英卓著. —南京:南京大学出版社,2011.12

ISBN 978-7-305-08904-6

Ⅰ. ①电… Ⅱ. ①刘… Ⅲ. ①电子商务—数学模型 Ⅳ. ①F713.36

中国版本图书馆 CIP 数据核字(2011)第 195992 号

出版发行 南京大学出版社
社　　址 南京市汉口路 22 号　　邮　编 210093
网　　址 http://www.NjupCo.com
出 版 人 左　健

丛 书 名 经济转型与创新发展论丛
书　　名 电子商务数学建模
著　　者 刘英卓
责任编辑 王日俊　梁　颖　　编辑热线 025-83592193
照　　排 南京紫藤制版印务中心
印　　刷 南京大众新科技印刷有限公司
开　　本 880×1230　1/32　印张 6　字数 219 千
版　　次 2011 年 12 月第 1 版　2011 年 12 月第 1 次印刷
ISBN 978-7-305-08904-6
定　　价 26.00 元

发行热线 025-83594756
电子邮箱 Press@NjupCo.com
Sales@NjupCo.com(市场部)

前　言

在当前各个大学开展的电子商务学科建设中，已经形成了以《电子商务概论》、《网络支付与结算》、《电子商务安全》、《网站设计与网页制作》为主干课的课程群。针对电子商务专业的本科课程基础课又包括《运筹学》、《网络经济》、《管理学》等，以及作为大学生通识的《高等数学》、《大学英语》等。然而，电子商务学科的真正发展，应该有属于它自己的基石，电子商务专业学生需要属于自己学科的数学基础。文学家用各种文体来建模生活、社会、人生等方面；雕塑家用各种材料造型来建模想象和意境；歌唱家用声音来建模情感的抒发、情绪的变化；运动员用形体和运动建模人类的运动和生命的旋律；书画家用笔和纸在二维空间中创造出美，建模山川的秀丽、人生的壮阔。各行各业的研究者都在发挥自己的聪明才智，在各自的领域中建模着各自的研究对象。电子商务学科发展至今，已经不应该仅仅限于《电子商务概论》类概括性书籍的编撰，而应该向学科的定量性研究上发展。唯有如此，我们的电子商务学科才能真正立于众学科之林。首要的，我们电子商务研究者必须关注电子商务问题的数学建模。

大学学习的真正目的是培养人才。大学期间开了一门又一门课，这些课对大学生的知识量储备是必要的。但如何让这些课程内容在大学生的头脑中发酵、升华、进而得到质上的提高，才是大学真正应该追求的。简而言之，就是如何让大学生能够运用和实践这些课程所传授的知识，做到水乳交融、浑然一体。先哲们早以给出了答案：太极生两仪、两仪生四象；冰冻三尺，非一日之寒；学如春起之苗，不见其长，唯见其高……。讲授者讲解课程时要将本门知识与人生哲学相交融，从根本上建立课程与学生

内心中智慧之源的联系，这便是将具体的学科知识升华为学生自我的哲学观；而同时大学生作为学习者，应该在自己的哲学体系上，将五花八门的课程内容进行宏观上的融合、集成进自己的慧根。慧根是个佛家用语，它说明了学习的理解、领悟之源是学习者的哲学之根。作者觉得大学生阅读《科学的历程》、《万物简史》这样的书籍，对于在大学阶段建立成功的人生模型是非常有益的。

人类的进化就是学习的进化过程，在这个过程中，有一个主要的枝桠，那就是数学。古希腊毕达哥斯拉学派的“万物皆数”的观点，已经有无数的专家和学者关注过，“数”就是人类进化之源！现代各门学科，无论理科和文科以及它们的各种枝杈其实都是数和量的伸展与收缩，数量上尺度的不同，造就了从宏观到微观、从陆地到海洋、从海洋到天空、从地球到宇宙种种的不同。整个宇宙、乾坤都是用某种数在衡量，数量在伴随科学的发展。

模型是通过对原型的形象化或模拟与抽象而得到的一种结构，人们借助模型来研究原型的功能特征和内在规律。数学模型广义含义是指凡是从现实原型概括出来的一切数学概念、公式、方程、定理、法则、理论体系等，狭义的解释是只有那种反映特定的具体事物内在规律性的数学结构。本书的电子商务数学建模取其广义含义。我们将电子商务的现实问题通过数学抽象分析，得到数学模型，再通过求解得到模型的解答，然后将模型的解答翻译成对电子商务现实问题的解答，最终在现实世界中实现模型的思想。

根据电子商务现实问题的不同，其数学模型的种类也有很大不同，既有理论模型和经验模型，又有微分方程模型和概率模型、离散型模型与连续模型、线性模型与非线性模型、确定性模型和随机性模糊模型等。在对现实的电子商务问题建模时，最重要的是要逆向思维，不拘一格地分析、研究，唯有如此，电子商务的问题才能得到精彩的解决。

本书写作的目的是为电子商务学科建立它在数学上的“源”

和“流”，让电子商务学习者、研究者拥有自己的学科立脚点。同时，深入挖掘电子商务学科的理论研究。电子商务涉及各种问题，大体上分为技术和商务应用两类。本书将这些问题划分到八个章节中，每一章阐述的是对应于专业课的典型问题的数学建模。这样安排的目的是为了方便读者阅读，那种不考虑读者的书是不负责任的。

由于本书作者水平有限，书中难免会存在错误、瑕疵和其他不足之处，请读者不吝提出。

目 录

第一章

电子商务安全中的数学模型

电子商务安全是实行电子商务的基础，电子商务的各个方面都离不开安全性的考虑，都渗透了安全。对典型的电子商务安全问题建立数学模型，对于深入研究电子商务学科意义重大。

电子商务安全是建立在密码学之上的。加密和解密的本质是对语言、文字的编码变换，这种变换反映到应用中就是将原来易于理解和解释的一种码变为另外一种你不熟悉和理解的码。例如，古埃及的象形文字主要是当时的账房先生用来表示所欠法老谷子的多少，对于现代人来说就是天书，将现代文字用它写出来就是一种加密。编码的过程就是加密（encryption），逆过程就是解密（decryption）。码的计算机表示就是 0 和 1 二进制的组合，为了符合人的习惯，二进制往往被转换成 10 进制，10 进制的数又组合起来，形成对字母、符号、文字的表示，就是 ASCII、gb2313、gbk、UTF－8 等。这些本质都是数字，数字间的变换就是加密和解密，加密的强度是与数论难题相关的。

第一节　加密中的数学难题

人们在对明文进行正向加密时希望加密的算法能够很容易进行下去，得到密文；加密算法要保证对加密者方便，并尽可能增加攻击者的难度，而对于合法的解密者由于其掌握一个窍门解密是不成为问题的。攻击者不知道这个窍门，从而需要在一个空间内搜寻该窍门，这个窍门的解空间越大，破译的难度就会越大。所以，加密函数具有一种单向性，该单向性源自数学上的难题。

一、大数分解问题

将大合数分解成素因子乘积（大数分解）是数论中一个最基本、最古老的问题，它在历史上曾经吸引了包括费马、欧拉、勒让德和高斯在内的大批数学家花费大量的时间和精力去研究。素数在数论中占有特殊的地位，把合数分解成素因子的乘积是算术基本定理的构造性方面的需要。

大数分解具有很大的应用价值，这一点在电子商务安全课程中学习 RSA 算法应深有体会。但也正是因为 RSA 算法的诞生，才使得人们不再认为大数分解仅仅是数学家的游戏，而可以由一国元首用来操控未来战争中核弹的按钮密码。

在 RSA 算法中，利用了破解者仅知道加密过程而未被告知解密过程则不可能对电文进行解密。这就是大数分解的单向性事实：能够很容易地将两个大素数乘积求出，反过来，要分解一不大整数（譬如 200 位）则几乎不可能，RSA 体制的建立与破译就等价于素数判别与大数分解问题。

（一）幂运算

在 RSA 算法中要计算 $a^m \bmod n$，如果根据定义，先计算 $a \bmod n$，再依次计算 $a^k \bmod n = (a \bmod n) \cdot (a^{k-1} \bmod n) \bmod n$，则至少需要 m 次乘法才能得到 $a^m \bmod n$，而 m 经常是很大很大，这时计算量也就很大，于是需要有更好的计算 $a^m \bmod n$ 的方法。在此，考虑 a＝n×商＋余数，即 $a \bmod n$＝余数，则 $a^2 \bmod n = (n \times 商 + 余数)^2 \bmod n = 余数^2 \bmod n = (a \bmod n)^2 \bmod n$。注意到当 a 的幂为 2 的幂数时，就可以利用已经计算出的低幂次求模结果来逐渐求出高幂次取模结果。所以，当要计算 $a^m \bmod n$ 时，先将 m 用二进位制表示，设 $m = (a_{k-1} \cdots a_2 a_1)$，$a_i = 0$ 或 1，$i = 0, 1, \cdots k-1$。再将使 $a_i = 1$ 对应的余数 r_i 连乘起来，取模 n，则得 $a^k \bmod n$（这里连乘是指每乘一个数取一次模 m，然后用所得的结果再与另一乘数相乘）。

因此，RSA 算法中 a^m mod n 的计算，先将 m 表示为二进制形式：b_k，b_{k-1}，$\cdots b_0$。然后应用快速指数实现算法。

```
c=0; d=1;
for i=k down to 0 do
 {
        c=2×c;
        d= (d×d) mod n;
        if  b_i=1
        then {
c=c+1;
d= (d×a) mod n
             }
}
return d;
```

d 最终为所求的加密结果，c 的最终值为 m。

练习：计算 3^{107} (mod 134)。

(二) 辗转相除法

RSA 算法中要计算私钥 d，使 d * e=1 mod f (n)；由前面几步，e 和 f (n) 是已知的，现在求 d，然而 d * e=1 mod f (n) 实质上有两个未知数，即 d * e=f (n) ×商+1，“商”未知，同时要求 d 和“商”必须为整数。那么这个整数的二元一次方程到底有没有整数解，又如何求出 d 的整数解。

引理 令 (a, b) 表示 a 和 b 的最大公约数，(a, b) 具有如下性质：

(1) 存在整数 x，y，使得 (a, b) =ax+by；

(2) 对任意两个整数 x，y，必有 (a, b) | (ax+by)；

(3) 如果任一整数 e，e | a，e | b，则 e | (a, b)。

定理 1 二元一次方程 ax+by=c 有整数解的充要条件是(a, b) | c。

证明 必要性。假定 ax+by=c 有整数解，设为 x_0，y_0，则 $ax_0+by_0=c$，但 (a, b) | a，(a, b) | b，故 (a, b) | c，条件的必要性得证。

充分性。若 (a, b) | c，则 $c=c_1$ (a, b)，其中 c_1 是整

数。由引理存在两个整数 s，t 满足方程：

$as+bt=(a,b)\Rightarrow as\,c_1+bt\,c_1=(a,b)\,c_1=c$。

令 $x_0=sc_1$，$y_0=tc_1$，即 $ax_0+by_0=c$。所以 $ax+by=c$ 有整数解 x_0，y_0。证毕。

练习 判定 $10x-7y=17$；$117x+21y=38$ 是否有整数解。

根据定理 1 验证 RSA 算法中的等式 $d*e=1 \bmod f(n)$ 是否有解。

由 $d*e=1 \bmod f(n)\Rightarrow ed-f(n)\times 商=1$，其中 d 和“商”为未知数，其有整数解的充分必要条件为 $(e,f(n))\mid 1$，显然任何数都能够整除 1，故 RSA 算法中的等式 $d*e=1 \bmod f(n)$ 一定有整数解。

如果想顺利求出 d 的整数解，还需要用到辗转相除法，它最初是公元前由欧几里得提出来的，所以也叫做欧几里得算法，人们用它来求最大公因数。该算法表述如下：

设给定 m，n（m＞n），令 $r_0=m$，$r_1=n$，gcd 表示求最大公因数函数符号，$r_i=r_{i-2} \bmod r_{i-1}$，$i=2,\cdots k$，则：

$r_k=\gcd(r_{k-1},r_k)=\gcd(r_{k-2},r_{k-1})=\cdots=\gcd(r_2,r_3)=\gcd(r_1,r_2)=\gcd(r_0,r_1)=\gcd(m,n)$。

例 求 $107x+37y=25$ 的一切整数解。

解 首先判断出这个方程有解，下面用辗转相除法求它。

由方程得：$37y=25-107x\Rightarrow y=(25-107x)/37=-2x+(25-33x)/37$，令 $y_1=(25-33x)/37$，则 y_1 应当是一个整数，于是得到一个新的不定方程 $37y_1=25-33x$，又 $33x=25-37y_1\Rightarrow x=(25-37y_1)/33=-y_1+(25-4y_1)/33$，仿照上面，令 $x_1=(25-4y_1)/33$，又得到一个新的不定方程：$33x_1+4y_1=25$。又 $4y_1=25-33x_1\Rightarrow y_1=(25-33x_1)/4=6-8x+(1-x_1)/4$。

令 $y_2=(1-x_1)/4$，这就得到 $x_1+4y_2=1$，由此不难看出 $x_1+4y_2=1$ 的一切解是 $x_1=1-4t$，$y_2=t$（$t=0,\pm1,\pm2,\cdots$）。

将这个结果逆向回代，得到：$y_1=-2+33t$，$x_1=1-4t$，x

$=3-37t$，$y=-8-107t$（$t=0$，±1，±2，…）。

从这个例子可以看出，解的过程就是对整个不定方程辗转相除，依次化为等价的不定方程，直到出现一个变量系数为±1为止。

二、椭圆曲线的数学基础

（一）离散对数问题

模指数运算是频繁地用于密码学中的一种单向函数，即单向性反映在计算下面这个表达式很容易：

$a^x \bmod n=b$

而其逆运算是求解 x，即 $x=\log_a(n\times? +b)$，其中“?”可以被看成商，因为在模运算中，a^x 可以看成被除数，n 为除数，b 为余数。要求解 x，这是一个难题。要注意：被除数、除数、余数都是整数空间的概念。所以，只有满足要求的整数才是合法的解。既然有这个整数空间的限制，就决定了并不是所有的离散对数都有解。

例如：$3^x=7 \bmod 13$ 无解，而 $3^x=15 \bmod 17$ 的解为 6。

（二）有限域上的离散对数

密码的设计主要考虑利用的是有限域上的离散对数单向函数的逆向解难题，这里的有限是指将无限的空间进行人为的范围限定或构造出适合的空间，在这个人为构造空间上再利用数学上的群来描述空间粒子的关系。主要可供利用的有三种群：

（1）素数域的乘法群：GF（p）；

（2）特征为 2 的有限域上的乘法群：$GF(2^n)$；

（3）有限域 F 上的椭圆曲线群：EC（F）。

定义 1 生成元

如果 p 是一个素数，且 g 小于 p，对于从 0 到 p−1 的每一个 b，都存在某个 a，使得 $g^a=b \pmod p$，那么 g 是模 p 的生成元，或者叫做 g 是 p 的本原元。

例 1 $p=11$，可以取 $g=2$，b 的取值在 0 到 10 之间，都可

以满足生成元的定义。

定理 1 生成元判断定理

如果 p 是一个素数，且 q_1，q_2，…q_n 是 p－1 的素因子，要检验一个小于 p 的数 g 是否是模 p 的生成元，对所有的 q_1，q_2，…q_n 计算：

$$g^{(p-1)/q_i} \ (\mathrm{mod}p),\ i=1,\ \cdots n$$

如果对某个 q_i，其结果为 1，则对应的 g 不是一个生成元；如果对任何 q_i，结果不等于 1，则 g 是生成元。

有限域就是这样一种空间，它的 p 是一个素数或一个大素数的幂，其专有名字是伽罗瓦域，记作 GF（p）。在伽罗瓦域上，非零元的加、减、乘、除均有定义。有一个加法单位元 0，乘法单位元 1，每个非零元都有唯一的逆元（如果 p 不是素数，这点不成立）。交换律、结合律、分配率在其上都成立。

GF（p）上的运算大量地用于密码方面。它给数一个限制范围，除法将不会有任何舍入错误。密码设计者为了使密码算法更加复杂，也使用模 n 次不可约多项式的算术运算，它的系数是模 q 的整数，q 是素数。这些域称为 GF（q^n）。所有的运算都模 p（x），p（x）是n 次不可约多项式。例如 GF（2^3）有以下元素：0，1，x，x＋1，x^2，x^2+1，x^2+x，x^2+x+1。

1985 年，Neal Koblitz 和 V. S. Miller 把椭圆曲线的研究成果应用到密码学中，分别独立提出在公钥密码系统中使用椭圆曲线的思想。

实数域上的椭圆曲线是连续的，并不适合用于加密。必须把椭圆曲线变成离散的点，把它定义在有限域上，顾名思义，有限域是一种只由有限个元素组成的域。

域的概念是从有理数，实数的运算中抽象出来的，域中的元素同有理数一样，有自己的加法、乘法、除法、单位元（1），零元（0），并满足交换率、分配率。我们可以形象地将数学上的群、环、域建模成一种小宇宙，它们当中的元素逐渐形成某种联系，进而产生互相依存的关系。

例 一个简单的有限域 Fp，这个域只有有限个元素，它的

定义如下：

Fp 中只有 p（p 为素数）个元素 0，1，2 … p－2，p－1；

Fp 的加法（a＋b）法则是 a＋b≡c（mod p）；即，（a＋c）÷p 的余数和 c÷p 的余数相同。

Fp 的乘法（a×b）法则是 a×b≡c（mod p）；

Fp 的除法（a÷b）法则是 a/b≡c（mod p），即 $a\times b^{-1}\equiv c$（mod p）（b^{-1}也是一个 0 到 p－1 之间的整数，但满足 $b\times b^{-1}\equiv 1$（mod p），具体求法可以参考初等数论）。

Fp 的单位元是 1，零元是 0。

并不是所有的椭圆曲线都适合加密。$y^2=x^3+ax+b$ 是一类可以用来加密的椭圆曲线，也是最为简单的一类。

考虑如下等式：

$$\mathbf{K}=kG$$

其中，K，G 为 Ep（a，b）上的点，k 为小于 n（n 是点 G 的阶）的整数。

不难发现，给定 k 和 G，根据加法法则，计算 **K** 很容易；但给定 **K** 和 G，求 k 就相对困难了。这就是椭圆曲线加密算法采用的难题。把点 G 称为基点，k（k＜n，n 为基点 G 的阶）称为私有密钥，**K** 称为公开密钥。

密码学中，描述一条 Fp 上的椭圆曲线，常用到六个参量：

T＝（p，a，b，G，n，h）。

p、a、b 用来确定一条椭圆曲线，G 为基点，n 为点 G 的阶，h 是椭圆曲线上所有点的个数 m 与 n 相除的整数部分。

这几个参量取值的选择，直接影响了加密的安全性。

第二节　古典加密学的数学变换

古典密码学是在计算机出现前，密码学由基于字符的密码算法构成，不同的密码算法是字符之间互相换位或者互相替代，置换与替代是古典密码学的主要方法。

一、加密中的置换应用

在古典加密学中，主要采用的是置换的手段来对明文进行加密。所谓的置换，其实就是位置的变换。要定位位置，在物理上采用空间的概念，如一维空间、二维空间、三维空间、多维空间。一维空间的置换最简单，进行明文加密仅仅是前后位置关系的变化。二维空间的置换除了行的变化，还有列的变化，而三维空间的置换又进一步增加了深度的变化，多维空间的置换则在所选定的各维上进行相应的变换。要描述明文在每一维上的变化，就要给该维分配一个变量，如 x、y、z；r、ρ、θ 等。

在古典密码学中，采用的置换主要是指在一维空间中进行的置换，即将文字符号仅仅作前后位置的调整，得到的密文就是一组乱序的字母符号。

例如置换：$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\3 & 6 & 1 & 4 & 5 & 2\end{pmatrix}$。这个置换将原文的位置关系进行了前后移动，原来排第一的，现在排在第三位，原来排第六位的，现在排第二位。这个置换还很眼熟，原来它就是双绞线线序的一种排列。还有很多例子，请同学们想一想自己有没有和人玩过猜手指头的游戏。

二、加密中的矩阵应用

在古典密码学中，比如 Playfair 密码、Hill 密码和其他一些对照表进行加密的方法，它们的本质上都是在二维空间中进行对明文的置换。二维空间需要两个变量描述位置，即行和列，整个二维平面就是点（x，y）的集合，任何处于二维空间中的东西都可以用点阵来建模。例如，图像、文字、符号等都可以建模成数学上的矩阵。矩阵的定义是将数域 P 中 m·n 个数排成 m 行，n 列的长方阵（将第 i 行，第 j 列的元素记为 a_{ij}），再加上括号，即：