计算方法丛书·典藏版 —3

快速数论变换

孙琦　郑德勋　沈仲琦　著

科学出版社

计算方法丛书·典藏版 3

快速数论变换

孙 琦 郑德勋 沈仲琦 著

科学出版社

北京

内 容 简 介

本书主要介绍快速数论变换的理论、方法、应用及其最新进展.

数论变换是把数论应用到数字处理中而得到的一种计算方法. 其特点是: (1)没有舍入误差; (2)其中某些变换比快速傅里叶变换还快. 它不仅在数字处理中有用,还可以应用到多项式、大整数相乘等方面的计算中去.

本书可供计算数学工作者、大专院校有关专业教师、研究生、高年级学生等参考.

图书在版编目(CIP)数据

快速数论变换/孙琦, 郑德勋, 沈仲琦著. —北京: 科学出版社, 2015.11

(计算方法丛书)

ISBN 978-7-03-046407-1

Ⅰ. ①快… Ⅱ. ①孙… ②郑… ③沈… Ⅲ. ①数论—变换 Ⅳ. ①O156

中国版本图书馆 CIP 数据核字(2015)第 275757 号

责任编辑: 赵彦超 胡庆家 / 责任校对: 鲁 素

责任印制: 钱玉芬 / 封面设计: 王 浩

科学出版社 出版

北京东黄城根北街 16 号

邮政编码: 100717

http://www.sciencep.com

北京京华虎彩印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

1980 年 10 月第 一 版 开本: 850×1168 1/32

2016 年 1 月 印 刷 印张: 6 3/4

字数: 172 000

定价: 48.00 元

(如有印装质量问题, 我社负责调换)

《计算方法丛书》编委会

前　言

近年来，利用复数域上的离散傅里叶变换（DFT）对数字式信号进行处理，这种方法在雷达、通讯、遥感、物探、光学、医学等各方面都得到了有效的应用．特别是在1965年，Cooly和Tukey提出了快速计算离散傅里叶变换的算法——快速傅里叶变换（FFT），使得原来直接计算DFT的乘、加法次数的阶由$O(N^2)$降为$O(N\log_2 N)$，从而大大节省了计算量．这一方法促进了数字信号处理的发展，带来了更加广泛的应用．例如，FFT的提出，使得用DFT来计算两个长序列的卷积变得有实际意义了，而卷积运算在电子计算机科学和其他一些领域都有广泛的应用．

然而，在数字信号序列长度N很大的情况下，FFT的计算量仍嫌太大．于是人们努力寻求更快、更新的算法．

七十年代初，Rader，Agarwal，Burrus等人提出了构造整数模M剩余类环Z_M上的DFT，即数论变换，这种变换仍然具有循环卷积等特性，并可用类似FFT的快速演段来计算．这样，就可用数论变换来计算有理整数序列的卷积，与FFT比较，它具有更快的速度、没有舍入误差、不需要存贮三角函数等优点，其缺点是变换本身无物理意义（不能测量频率），以及序列长度要受运算字长的限制等．尽管如此，数论变换的提出，还是引起了人们的广泛注意，一方面是它的优点十分吸引人，更重要的一方面是数论变换把数论的方法带到了数字信号处理中，这从理论上和方法上讲，无疑是一个重要的进展．所以，自数论变换方法提出后，发展得很快，继之又提出了复数论变换和二次域上的某些变换等方法．

本书将系统介绍数论变换及其进一步推广的理论，以及这些理论所需要的数论基础知识．

应当指出，国外首先提出数论变换是重要的，其想法在数字信

号处理中也很有意义. 但是,因为数论变换的理论还在发展,数论变换的应用也还处在探索阶段,所以国外关于这方面工作的研究还不完善. 1976 年以来,我们在学习国外资料的基础上,开展了对数论变换的较系统的研究. 本书也总结了我们自己在这方面的工作:

1. 利用我们给出的 Z_M 上 DFT 存在的一组充分必要条件,可以求出 Z_M 上 DFT 的个数,以及得到所有这些变换的算法,并简化了 Z_M 上 DFT 的定义.

2. 为了缩短字长和进行二维滤波,需要引入二维的数论变换. Z_M 上的二维 DFT,国外只给出了一组含混不清的充分条件,我们给出了充分必要条件,以及全部变换的个数和算法. 用这个方法可立即得到一般 Z_M 上 m 维 ($m \geqslant 3$) DFT 的相应的结果. 而且,我们还简化了 Z_M 上的二维 DFT 的定义. 并对序列长度和运算字长之间的关系,作了较细致的讨论.

3. 求复整数序列的卷积,就需要复数论变换. 一般二次域 $R(\sqrt{m})$ 的整数剩余类环上 DFT 的构造问题,国外研究得很不充分,就是限定模 M 无平方因子的情况也未完全解决. 而我们对任意的正整数 $M > 1$,全部解决了 $R(\sqrt{m})$ 的模 M 整数剩余类环上的 DFT 的构造问题,包括 DFT 存在的充分必要条件,全部个数和算法. 对于分圆域(包括实分圆域)上的情况,我们也解决了.

4. 熟知,在复数域上具有循环卷积性质的可逆变换存在而且是唯一的,即 DFT. 但是在 Z_m 上如何呢? 我们的工作揭示了这两种情况的本质差别. 证明了在 Z_M 上存在非 DFT 型的有循环卷积性质的可逆变换 (CRT). 而且,进一步给出了在任意有单位元素的交换环 R 上的 CRT 存在的充分必要条件和具体构造. 同时还给出了二维的结果.

以上这些结果分别写进了第三章、第四章、第六章和第七章. 此外从学习数论变换及其推广的需要出发,我们在第一章和第五章还分别介绍了初等数论和代数数论的基础知识. 由于数论、代数、组合论等离散性数学已经深深地渗透到近代应用数学的各个

领域中，这些基础知识对于其他许多方面也是需要的.

通常把快速计算 DFT 的方法统称为快速变换. 作为计算方法的一个方面，其内容丰富，发展很快. 在第二章里我们除大致介绍一下 FFT 的实质外，还扼要介绍了某些新的快速变换，如素数幂变换和 WFTA 等. 第八章介绍了数论变换在其他方面的一些应用.

我们的工作始终是在柯召教授的热情指导下进行的. 在工作过程中还得到了中国科学院数学研究所、四机部 1014 所、四川大学无线电系等单位的有关同志的鼓励与支持，作者在此一并致以衷心地感谢.

限于水平，本书难免有缺点和错误，请读者批评指正.

作 者

一九七八年十二月

目　　录

第一章 初等数论

§1. 整数的分解

数论是研究数的规律，特别是整数的规律的数学分支. 整除是数论中的基本概念，本节从这个概念出发，引进带余除法和辗转相除法，证明了数论中最基本的定理——唯一分解定理以及介绍这个定理的一些应用.

1.1. 整除性 我们知道两个整数的和、差、积仍然是整数，但是用一个不等于零的整数去除另一个整数所得的商却不一定是整数，因此，我们引进整除的概念.

定义. 设 a, b 是任意两个整数，其中 $b \neq 0$，如果存在一个整数 q 使得等式

$$a = bq \tag{1}$$

成立，我们就说 b 整除 a 或 a 被 b 整除，记作 $b|a$，此时我们把 b 叫作 a 的因数，把 a 叫作 b 的倍数.

如果 (1) 里的整数 q 不存在，我们就说 b 不能整除 a 或 a 不能被 b 整除，记作 $b\nmid a$.

由整除的定义出发，下面几个性质是明显的.

(i) 如果 $b|a$，$c|b$，则 $c|a$.

(ii) 如果 $b|a$，则 $cb|ca$.

(iii) 如果 $c|a$，$c|b$，则对任意的整数 m，n，有 $c|ma+nb$.

以上三条性质中，我们总假定，$b \neq 0$，$c \neq 0$.

在一般的情形下，有下面的定理.

定理 1. 设 a，b 是两个整数，其中 $b>0$，则存在两个唯一的整数 q 及 r，使得

$$a = bq + r, \quad 0 \leqslant r < b \tag{2}$$

成立.

证. 作整数序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots,$$

则 a 必在上述序列的某两项之间,即存在一个整数 q 使得

$$qb \leqslant a < (q+1)b$$

成立. 令 $a - qb = r$, 则 (2) 成立.

设 q_1, r_1 是满足 (2) 的另一对整数,因为

$$bq_1 + r_1 = bq + r,$$

于是

$$b(q - q_1) = r_1 - r,$$

故

$$b|q - q_1| = |r_1 - r|.$$

由于 r 及 r_1 都是小于 b 的正整数,所以上式右边是小于 b 的. 如果 $q \neq q_1$, 则上式左边 $\geqslant b$, 这是不可能的. 因此 $q = q_1$, $r = r_1$. 证完.

我们把 (2) 中的 q 叫做 a 被 b 所除得的不完全商, r 叫做 a 被 b 除所得到的余数,常记 $\langle a \rangle_b = r$.

1.2. 最大公因数与辗转相除法 我们用带余数除法, 研究整数的最大公因数的存在问题和实际求法.

定义. 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数. 若整数 d 是它们之中每一个的因数,那么 d 就叫作 $a_1, a_2, \cdots, a_n$ 的一个公因数. 整数 $a_1, a_2, \cdots, a_n$ 的公因数中最大的一个叫作最大公因数,记作 $(a_1, a_2, \cdots, a_n)$, 若 $(a_1, a_2, \cdots, a_n) = 1$, 我们说 $a_1, a_2, \cdots, a_n$ 互素. 我们有下面的定理.

定理 1. 设 a, b, c 是任意三个不全为零的整数,且

$$a = bq + c,$$

其中 q 是整数,则 $(a, b) = (b, c)$.

证. 因为 $(a, b)|a$, $(a, b)|b$, 则有 $(a, b)|c$, 因而 $(a, b) \leqslant (b, c)$, 同法可证 $(b, c) \leqslant (a, b)$, 于是得到 $(a, b) = (b, c)$. 证完.

因为显然有 $(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$ 和

$b>0$，$(0,b)=b$，所以下面我们只讨论两个正整数的最大公因数的求法，即辗转相除法，并借此推出最大公因数的若干性质。

设 a，b 是任意两个正整数，由带余除法，有下列等式：

$$\begin{aligned}
&a=bq_1+r_1, \quad 0<r_1<b,\\
&b=r_1q_2+r_2, \quad 0<r_2<r_1,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&r_{n-2}=r_{n-1}q_n+r_n, \quad 0<r_n<r_{n-1},\\
&r_{n-1}=r_nq_{n+1}+r_{n+1}, \quad r_{n+1}=0,
\end{aligned} \tag{1}$$

因为

$$b>r_1>r_2>r_3>\cdots\cdots,$$

故经有限次带余除法后，总可以得到一个余数是零，即 (1) 中 $r_{n+1}=0$。

现在我们证明定理 2.

定理 2. 若 a，b 是任意两个正整数，则 (a,b) 就是 (1) 中最后一个不等于零的余数，即 $(a,b)=r_n$。

证. 由定理 1 即得

$$\begin{aligned}
r_n&=(0,r_n)=(r_n,r_{n-1})=\cdots=(r_2,r_1)\\
&=(r_1,b)=(a,b),
\end{aligned}$$

证完。

我们从 (1) 中顺次由第一个等式解出 $r_1=a-bq_1$ 后代入第二个式子得 $r_2=-aq_2+b(1+q_1q_2)$，再代入第三个式子解出 r_3，然后代入第四个式子，这样作下去，最后可得

$$r_n=ma+nb,$$

这里的 m，n 是两个整数. 于是得到定理 3.

定理 3. 若 a，b 是任意两个正整数，则存在两个整数 m，n 使得

$$(a,b)=ma+nb.$$

定理 4. 若 $a\neq 0$，$a|bc$，$(a,b)=1$，则 $a|c$.

证. 若 $c\neq 0$，由 $(a,b)=1$ 知存在两个整数 m，n 使 $ma+nb=1$，故 $mac+nbc=c$，由 $a|bc$，知 $a|c$，若 $c=0$，结论显然成立. 证完.

例. 求 323 和 221 的最大公因数.

$$
\begin{array}{r|l}
323 & 221 \\
\cline{2-2}
221 & 1 \\
\cline{1-2}
221 & 102 \\
\cline{2-2}
204 & 2 \\
\cline{1-2}
102 & 17 \\
\cline{2-2}
102 & 6 \\
\cline{1-2}
0 &
\end{array}
$$

$$
\begin{aligned}
323 &= 221 \times 1 + 102, \\
221 &= 102 \times 2 + 17, \\
102 &= 17 \times 6, \\
&\text{故 } (323, 221) = 17.
\end{aligned}
$$

再从第一个式子解出 102 代入第二个式子得

$$17 = (-2) \times 323 + 3 \times 221,$$

即得定理 3 中的 $m = -2$, $n = 3$.

现在来研究两个以上整数的最大公因数. 不妨假设 $a_1, a_2, \cdots, a_n$ 是任意 n 个正整数. 令

$$(a_1, a_2) = d_2, \quad (d_2, a_3) = d_3, \cdots, \quad (d_{n-1}, a_n) = d_n,$$

于是有下面的定理.

定理 5. 若 $a_1, a_2, \cdots, a_n$ 是 n 个正整数,则

$$(a_1, a_2, \cdots, a_n) = d_n.$$

证. 由 1.1. 节中的 (ii) 知,

$$d_n \mid a_n, \quad d_n \mid d_{n-1},$$

但

$$d_{n-1} \mid a_{n-1}, \quad d_{n-1} \mid d_{n-2},$$

故

$$d_n \mid a_{n-1}, \quad d_n \mid d_{n-2},$$

由此类推,最后得到

$$d_n \mid a_n, \quad d_n \mid a_{n-1}, \cdots, \quad d_n \mid a_1,$$

便有 $d_n \leqslant (a_1, a_2, \cdots, a_n)$, 另一方面,设 $(a_1, a_2, \cdots, a_n) = d$, 由 1.1. 节中的 (ii) 和定理 3 可得

$$d \mid d_2, \quad d \mid d_3, \cdots, \quad d \mid d_n,$$

故

$$d \leqslant d_n,$$

于是得到

$$(a_1, a_2, \cdots, a_n) = d_n.$$

证完.

1.3. 最小公倍数

定义. 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数 ($n \geqslant 2$)，若 m 是这 n 个数中每一个数的倍数，则 m 就叫作这 n 个数的一个公倍数. 在 $a_1, a_2, \cdots, a_n$ 的一切公倍数中的最小正数叫作最小公倍数，记作 $[a_1, a_2, \cdots, a_n]$.

因为乘积 $a_1a_2\cdots a_n$ 就是 $a_1, a_2, \cdots, a_n$ 的一个公倍数，故最小公倍数是存在的.

由于任何正整数都不是零的倍数，故讨论整数的最小公倍数时，总假定这些整数都不是零.

和最大公因数一样，显然有 $[a_1, a_2, \cdots, a_n] = [|a_1|, |a_2|, \cdots, |a_n|]$，所以只需对正整数讨论它们的最小公倍数.

我们先研究两个正整数的最小公倍数.

定理 1. 设 a, b 是任意两个正整数，则 (i) a, b 的所有公倍数就是 $[a, b]$ 的所有倍数；(ii) $[a, b] = \dfrac{ab}{(a, b)}$.

证. 设 m 是 a, b 的任一公倍数，$m = ak = bk'$，令

$$a = a_1(a, b) \quad 和 \quad b = b_1(a, b),$$

代入上式得 $\qquad a_1k = b_1k'$,

由于 $\qquad (a_1, b_1) = 1$,

故 $\qquad b_1 | k$.

因此

$$m = ak = a(b, t) = \frac{ab}{(a, b)}t, \tag{1}$$

其中 t 满足等式 $k = b_1t$，反之，当 t 为任一整数时，$\dfrac{ab}{(a, b)}t$ 为 a, b 的一个公倍数，故 (1) 可以表示 a, b 的一切公倍数. 令 $t = 1$，即得最小的正数，故 $[a, b] = \dfrac{ab}{(a, b)}$. 即证明了 (ii)；又由 (1)，(i) 亦得证.

现在讨论两个以上整数的最小公倍数. 设 $a_1, a_2, \cdots, a_n$ 是 n 个正整数，令

$$[a_1, a_2] = m_2,\quad [m_2, a_3] = m_3, \cdots, [m_{n-1}, a_n] = m_n, \quad (2)$$

我们有定理 2.

定理 2. 若 $a_1, a_2, \cdots, a_n$ 是 $n(n \geqslant 2)$ 个正整数，则

$$[a_1, a_2, \cdots, a_n] = m_n.$$

证. 由 (2) 知，$m_i | m_{i+1}$，$i = 2, 3, \cdots, n-1$，且 $a_1 | m_2$，$a_i | m_i$，$i = 2, \cdots, n$，故 m_n 是 $a_1, a_2, \cdots, a_n$ 的一公倍数，又设 m 是 $a_1, a_2, \cdots, a_n$ 的任一公倍数，则 $a_1 | m$，$a_2 | m$，故由定理 1 的(i)，$m_2 | m$. 又 $a_3 | m$，同理可得 $m_3 | m$，依此类推，最后得 $m_n | m$. 因此 $m_n \leqslant |m|$. 故

$$m_n = [a_1, a_2, \cdots, a_n].$$

我们已经讲了最大公因数的求法，因此上面两个定理给出了最小公倍数的求法.

1.4. 素数，唯一分解定理 在正整数里，1 的因数就只有它本身. 任一个大于 1 的整数都至少有两个正因数，即 1 和它本身.

定义. 一个大于 1 的整数，如果它的正因数只有 1 和它本身，就叫作素数，否则就叫作复合数.

本节的主要目的就是要证明任何一个大于 1 的整数，如果不论次序，能唯一地表示成素数的乘积.

定理 1. 设 a 是任一大于 1 的整数，则 a 的除 1 以外的最小正因数 q 是素数，并且当 a 是复合数时，$q \leqslant \sqrt{a}$.

证. 假定 q 不是素数，由定义，q 除 1 和它本身外还有一正因数 q_1，因而 $1 < q_1 < q$，但 $q | a$，所以 $q_1 | a$，这与 q 是最小正因数矛盾，故 q 是素数.

当 a 是复合数时，则 $a = a_1 q$，且 $q \leqslant a_1$，故 $q \leqslant \sqrt{a}$. 证完.

定理 2. 若 p 是一素数，a 是任一整数，则有 $p | a$ 或 $(p, a) = 1$.

证. 因为 $(p, a) | p$，故 $(p, a) = 1$ 或 $(p, a) = p$. 即 $(p, a) = 1$ 或 $p | a$. 证完.

定理3. 若 p 是素数，$p|ab$，则 $p|a$ 或 $p|b$.

证. 若 $p\nmid a$，则由定理2知 $(p, a)=1$，由§1.2定理4知 $p|b$. 证完.

定理4（唯一分解定理）. 任一大于1的整数能表示成素数的乘积，即整数 $a>1$，

$$a=p_1p_2\cdots p_n, \quad p_1\leqslant p_2\leqslant\cdots\leqslant p_n, \tag{1}$$

其中 $p_1, p_2, \cdots, p_n$ 是素数，并且若

$$a=q_1q_2\cdots q_m, \quad q_1\leqslant q_2\leqslant\cdots\leqslant q_m, \tag{2}$$

其中 $q_1, q_2, \cdots, q_m$ 是素数，则 $m=n$, $q_i=p_i$ $(i=1, 2, \cdots, n)$.

证. 我们用数学归纳法首先证明(1)式成立，当 $a=2$ 时(1)式显然成立. 假定对于一切小于 a 的正整数(1)式都成立，此时若 a 是素数，则(1)式对 a 成立，若 a 是复合数，则有两个正整数 b, c 满足条件

$$a=bc, \quad 1<b\leqslant c<a.$$

由假定 b 和 c 分别能表示成素数的乘积，故 a 能表成素数的乘积，即(1)式成立. 由归纳法即知对任一大于1的正整数，(1)式成立. 若对 a 同时有(1)，(2)两式成立，则

$$p_1p_2\cdots p_n=q_1q_2\cdots q_m. \tag{3}$$

由定理3知有 p_k, q_i 使得 $p_1|q_i$, $q_1|p_k$，但 q_i, p_k 都是素数，所以 $p_1=q_i$, $q_1=p_k$，又 $p_k\geqslant p_1$, $q_i\geqslant q_1$，故同时有 $p_1\geqslant q_1$ 和 $q_1\geqslant p_1$，因而 $p_1=q_1$，由(3)式得 $p_2\cdots p_n=q_2\cdots q_m$. 同理可得 $p_2=q_2$, $p_3=q_3$. 依此类推，最后得 $m=n$. 证完.

这个定理告诉我们，任一大于1的正整数 a 能够唯一地写成

$$a=p_1^{\alpha_1}\cdots p_k^{\alpha k}, \quad \alpha_i>0 \quad (i=1, 2, \cdots, k), \tag{4}$$

其中 $p_i<p_j$, $(i<j)$ 是素数.

(4)叫做 a 的标准分解式.

于是，当 $d|a$, $d>0$，由(4) d 可以表示成

$$d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta k}, \quad \alpha_i\geqslant\beta_i\geqslant 0 \quad (i=1, 2, \cdots, k) \tag{5}$$

的形式，反之 d 可以表示成(5)的形式时，一定有 $d|a$, $d>0$.

作为唯一分解定理的一个简单而直接的应用，我们有：

设 a，b 是任意两个正整数，且

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad \alpha_i \geqslant 0 \quad (i = 1, 2, \cdots, k),$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad \beta_i \geqslant 0 \quad (i = 1, 2, \cdots, k),$$

则

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \quad \gamma_i = \min(\alpha_i, \beta_i) \quad (i = 1, \cdots, k),$$
$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}, \quad \delta_i = \max(\alpha_i, \beta_i) \quad (i = 1, \cdots, k),$$

符号 $\min(\alpha_i, \beta_i)$ 表示 α_i，β_i 中较小的数，$\max(\alpha_i, \beta_i)$ 表示 α_i，β_i 中较大的数.

对于任意整数 x，y 显然有

$$x + y = \max(x, y) + \min(x, y).$$

由此，我们又可得出 § 1.3 定理 1 的结果：

$$[a, b] = \frac{ab}{(a, b)}.$$

上面从理论上证明了任意一个大于 1 的正整数有唯一的标准分解，但在实际计算中，还没有一个简单而有效的方法去判断哪些正整数是素数，也没有一个简单而有效的方法求出一个正整数的标准分解式. 但另一方面，我们根据素数的定义及其性质，可以造出素数表来以供使用.

任给一个正整数 N，可以按照下述方法求出一切不超过 N 的素数，把不超过 N 的一切正整数按大小顺序排成一串

$$1, 2, 3, 4, \cdots, N,$$

首先划去 1，第一个留下的是 2，它是一个素数：

$$\not{1}, 2, 3, 4, \cdots, N,$$

其次从 2 起，划出除 2 以外的 2 的一切倍数，

$$\not{1}, 2, \not{3}, \not{4}, \not{5}, \not{6}, \not{7}, \not{8}, \not{9}, \not{10}, \cdots, N,$$

在 2 的后面第一个未划去的是 3，它不是 2 的倍数，因此是一个素数. 然后划去的数是 $3m$ $(m = 2, 3, \cdots)$，