数学名著译丛

代数数理论讲义

〔德〕E. 赫克 著

科学出版社
www.sciencep.com

数学名著译丛

代数数理论讲义

〔德〕E. 赫 克 著
王 元 译

科 学 出 版 社
北 京

内 容 简 介

本书向读者介绍了构成代数数论理论框架的一般问题的一个理解.从数学特别是算数的发展中引出结论,并用群论的术语与方法来给出关于有限与无限阿贝尔群的必要定理,导致了形式上与概念上相当的简化;给出了任意代数数域中最一般二次互反律一个新的证明,并给出了相对二次类域存在性的证明.

本书可供高等学校数学系数论与代数专业的研究生及高年级学生阅读,也可作为数论研究人员的科研参考书.

图书在版编目(CIP)数据

代数数理论讲义/(德)赫克(Hecke,E)著;王元译.—北京:科学出版社,2005

(数学名著译丛)

ISBN 7-03-013282-3

Ⅰ.代… Ⅱ.①赫…②王… Ⅲ.代数数论 Ⅳ.O156.2

中国版本图书馆 CIP 数据核字(2004)第 040585 号

责任编辑:刘嘉善 范庆奎/责任校对:包志虹

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

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2005 年 1 月第 一 版 开本:850×1168 1/32

2005 年 1 月第一次印刷 印张:8 1/2

印数:1—4 000 字数:220 000

定价:28.00 元

(如有印装质量问题,我社负责调换〈环伟〉)

序

这本书是根据我在巴塞尔、哥庭根与汉堡的若干次讲课材料写成的，其目的在于向没有任何数论预备知识的读者介绍构成代数数论理论框架的一般问题一个理解. 前七章没有包含本质上新的东西；包括其形式在内，我从数学，特别是算术的发展中引出结论，并用群论的术语与方法来给出关于有限与无限阿贝尔群的必要定理. 这将导致形式上与概念上相当的简化. 对于熟悉这个理论的人，有些章节或许仍然会感兴趣，例如阿贝尔群基本定理的证明（§8），我用戴德金的原始构造方法处理相对判别式理论（§36，38），及不用截塔函数决定类数（§50）.

最后一章，即第八章将引导读者至近代理论之高峰. 这一章将给出任意代数数域中最一般二次互反律一个新的证明，其中用到西塔函数. 它比至今所知道的证明本质上要简短得多. 尽管这一方法至今还不能作推广，但它可以给初学者在代数数域中出现的各种新概念一个全貌，从而可使较高的互反定理变得较易接受. 作为互反定理的推论，在本书的结尾，我们将给出相对二次类域存在性的证明.

作为预备知识，我们仅要求读者具备初等微积分与代数知识，对于最后一章，则要求有复函数论知识.

我谨向班克、汉布尔革与奥斯特罗夫斯基先生表示感谢，他们为本书指误并作了不少建议. 早在大战之前，出版社即坚持从事了本书的出版工作，谨致谢意. 为使本书可能面世，他们不顾环境的极端困难. 对于他们的辛劳，应致特殊感谢.

E. 赫克

汉堡，数学讨论班，1923 年 3 月

目　录

第一章　有理数论概要

§1. 可除性、最大公因子、模、素数及数论的基本定理

我们暂时假定，算术的对象为全体整数，即 $0, \pm 1, \pm 2, \cdots$，它们间有加法、减法、乘法与除法（不是总有的）. 高等算术中用的研究方法类似于实数与复数的方法. 进而言之，在推导出它的定理时，我们也用到属于数学其他一些领域的分析方法，例如微积分与复函数论. 由于本书的后面部分将讨论这些方面，我们将假定读者熟知全体复数构成的数域，其中四种运算（除去用 0 除以外）可以无限制地进行，复数域在代数概要及微积分中已作了较细致地讲授. 在这一域中，1 是满足方程

$$1 \cdot a = a$$

对所有数 a 成立的一个特别的数. 其他的整数都是由 1 经过加法与减法而得来的，如果再经过除法运算则得到有理数集合，即整数商的全体. 以后，从 §21 开始，“整数”的概念将有一个本质的推广.

在这个导引部分，我们将给出有理算术的基本知识，简要地说，它们是关于整数的可除性性质.

由两个有理整数 a, b 总能得到形如 $a+b, a-b$ 及 $a \cdot b$ 的整数，而 a/b 则不一定是整数. 若 a/b 为整数，即 a 与 b 具有这一特别性质，则我们用记号 $b \mid a$ 来表示，或者说：b 整除 a，或 b 一致进入 a，或 b 是 a 的一个因子（因数），或 a 是 b 的倍数. 每一个整数 $a(\neq 0)$ 都有寻常因子 $\pm a, \pm 1$；a 与 $-a$ 有相同的因子，能够整除每一个数的整数仅为两个“单位”1 与 -1. 一个非零的整数 a，由于它的因子的绝对值不超过 $|a|$，所以它只有有限多个因子；另一

方面,每一个非零整数皆可以整除 0.

若 $b\neq 0$ 为整数,则在不超过一个给予整数 a 和 b 之倍数中,正好有一个最大的倍数,记为 qb,所以 $a-qb=r$ 为一个小于 $|b|$ 的非负整数.这个由 a 与 b 惟一确定,并适合要求

$$a = qb + r, q \text{ 为整数}, 0 \leqslant r < |b|$$

的整数 r 称为 a 被 b 除的余数,或 a 的剩余模 b.因此,语句 $b|a$ 就等价于 $r=0$.

如果我们现在将注意力转到两个整数 a,b 的公因子 c,即满足 $c|a$ 与 $c|b$ 的整数,则首先要考虑的是一个惟一确定的最大公因子(简单记为 GCD);我们将它记为 $(a,b)=d$.按照这个定义我们总有 $d\geqslant 1$.为了寻求这个数 (a,b) 的性质,我们考虑到对于所有整数 x,y 总有 $d|ax+by$.若我们现在考虑所有数 $L(x,y)=ax+by$ 的集合,此处 x,y 过所有整数,则 d 显然亦是所有 $L(x,y)$ 的 GCD;事实上,由于它能整除所有的 $L(x,y)$,并且没有具有这一性质的更大的数,这是因为没有更大的数能同时整除 $a=L(1,0)$ 及 $b=L(0,1)$.在所有正整数 $L(x,y)$ 中,令 $d_0=L(x_0,y_0)$ 为最小者,所以由

$$L(x,y) > 0 \text{ 立即推出 } L(x,y) \geqslant d_0. \tag{1}$$

我们现在来证明每一个 $n=L(x,y)$ 皆为 d_0 的倍数及 $d=d_0$.命 $n \bmod d_0$ 的剩余 r 由

$$r = n - qd_0 = L(x - qx_0, y - qy_0)$$

决定.在此我们有 $0\leqslant r<d_0$;由(1)式可知由 $r>0$ 即得 $r\geqslant d_0$.所以我们只能有 $r=0$,即 $n=qd_0$.由于每一个倍数 $qd_0=L(qx_0,qy_0)$ 亦出现在 $L(x,y)$ 中,所以集合 $L(x,y)$ 与 d_0 的倍数集合是等同的.因此 d_0 亦为 $L(x,y)$ 的 GCD,即它与 d 恒等,特别由此推出:

定理 1 若 $(a,b)=d$,则方程

$$n = ax + by$$

有整数解当且仅当 $d|n$.

进而言之,由此推出 a 与 b 的每一个公因子都能整除 a,b 的 GCD.

为了确定 GCD,我们用到熟知的一直追溯到欧几里得的所谓欧几里得算法,这个算法的要点为将 (a,b) 的计算归结为两个较小数的 GCD 的计算.由 $a=qb+r$ 可知 a 与 b 的公因子恒同于 b 与 r 的公因子,从而有 $(a,b)=(b,r)$.为简单计,假定 $a>0,b>0$,因为对称性,我们置 $a=a_1,b=a_2$,然后命 $a_1 \bmod a_2$ 之剩余为 a_3.一般言之,命

$$a_{i+2} \text{ 为 } a_i \bmod a_{i+1} \text{ 的剩余}, \quad i=1,2,\cdots$$

直至剩余可以被决定,即 $a_{i+1}>0$,及事实上,命

$$a_i = q_i a_{i+1} + a_{i+2}, \quad 0 \leqslant a_{i+2} < a_{i+1}.$$

由于按照这一程序,当 $i \geqslant 2$ 时,a_i 形成一个单调递减序列,所以经有限步骤后,这一过程必须终止,即当剩余变为零时终止,假定 $a_{k+2}=0$,由于

$$(a_1,a_2)=(a_2,a_3)=\cdots=(a_i,a_{i+1})=(a_{i+1},a_{i+2})$$
$$=(a_{k+1},a_{k+2})=(a_{k+1},0)=a_{k+1},$$

则最后的非零剩余,即欲寻求的 GCD.

在定理 1 的证明中,我们仅用到数集合 $L(x,y)$ 的一个性质,即这一集合是一个模.在此我们定义:

定义 若一个整数系 S 至少包含一个异于 0 的数及当 m 与 n 属于 S 时,$m+n$ 与 $m-n$ 都属于 S,则 S 称为一个模.

因此,若 m 属于 S,则 $m+m=2m, m+2m=3m,\cdots$ 属于 S;进而言之,$m-m=0, m-2m=-m, m-3m=-2m,\cdots$ 属于 S.所以一般说来,当 m 属于 S 时,对于每一个整数 x,mx 亦属于 S.从而当 m,n 属于 S 时,对于所有整数 x,y,$mx+ny$ 亦属于 S.

借助于定理 1 的证明,我们可以证明下面关于模非常一般的定理.

定理 2 一个模 S 中的数恒同于某个数 d 的倍数,除一个因

子 ± 1 之外，d 由 S 决定.

在证明定理时，我们可以考虑 S 仅包含正整数.命 d 为 S 中的最小正整数，若 n 属于 S，则如前可知，对于每一整数 q，$n - qd$ 都属于 S，特别 $n \bmod q$ 之剩余属于 S，它 $< d$ 但 $\geqslant 0$. 因此必须等于零.从而 S 中的每一个数 n 都是 d 的倍数，又由于 d 属于 S，所以全体 d 的倍数亦属于 S，命 d' 为具有这一性质的第二个数. S 中的数恒同于 d' 的倍数——则 d 必为 d' 的倍数，且其逆亦真. 所以 $d' = \pm d$.

如果在一个以整数为系数的任意线性型 $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ 中，命 $x_1, \cdots, x_n$ 过所有整数，则按这个途径定义的值域显然是一个模.特别我们得到

定理 3 任意 n 个变数的非全为零的整系数线性型的值域恒同于某一个变数的线性型 $d \cdot x$ 的值域.在此 d 为原来线性型的系数的 GCD.

欲方程(所谓丢番图方程)

$$k = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

有整数解 $x_1, \cdots, x_n$，其充要条件为 $a_1, \cdots, a_n$ 的 GCD 整除 k.

若 $(a, b) = 1$，我们称 a 与 b 互素.由定理 1 可知欲 $(a, b) = 1$，其充要条件为方程

$$ax + by = 1$$

有整数解 x, y.

关于记号 (a, b)，最重要的计算规则如下：

定理 4 对于任何三个整数 a, b, c，其中 $c > 0$，我们有

$$(a, b)c = (ac, bc). \tag{2}$$

事实上，若 $(a, b) = d$，则由 $ax + by = d$ 的可解性及定理 1 可知，方程 $acx + bcy = cd$ 可解；从而再由定理 1 可知，cd 为 (ac, bc) 的倍数.另一方面，cd 亦为 ac, bc 的一个公因子，所以它必须等于 (ac, bc).

除此以外，我们注意到两个数 a 与 b 的最小公倍这一概念.这是同时可以被 a 与 b 整除的最小正数 v，对于这个数，我们有

$$v = \frac{|a \cdot b|}{d}, \quad \text{此处}(a,b) = d. \tag{3}$$

因为由(2)式可知

$$\left(\frac{a}{d},\frac{b}{d}\right) = 1, \quad v = \left(\frac{a}{d}v,\frac{b}{d}v\right).$$

由于$\frac{ab}{d}$为$\left(\frac{a}{d}\right)v$与$\left(\frac{b}{d}\right)v$的一个公因子，所以它整除$v$，即$v \geqslant \frac{|ab|}{d}$；另一方面，$\frac{ab}{d}$为一个可以同时被$a$与$b$整除的数，所以它的绝对值$\geqslant v$. 因此$\frac{ab}{d}$只可能等于$\pm v$.

由于可以同时被a与b整除的数构成一个模，及v为其中的最小正数，所以每一个同时被a与b整除的数也必须是v的倍数.

现在我们来讨论一个数a的乘法分解. 若除了寻常整数分解，即其中一个因子为± 1，另一个$\pm a$外，再没有其他分解了，我们就称a为一个素数. 这种数是存在的，例如$\pm 2, \pm 3, \pm 5, \cdots$. 我们不把$\pm 1$算作素数. 为了简单起见，如果我们限于把正数$a$分解为正因子，首先我们见到每一个$a > 1$至少被一个正素数整除，这是由于$a$的$>1$的最小正因子显然只能是一个素数. 现在我们从$a$的分解$a = p_1 a_1$中分离出一个素数$p_1$，若$a_1 > 1$，则从分解$a_1 = p_2 a_2$中还可以分离出另一个素数$p_2$，如此等等. 因为$a_1, a_2, \cdots$构成一个正整数的递减序列，所以经过有限步骤必须终止，即某a_k必须$= 1$. 至此a已被表示为素数的一个乘积$p_1 \cdot p_2 \cdots p_k$. 因此素数是建筑用的砖，每一个整数都可以由乘法被建筑起来. 我们现在有

定理 5(算术基本定理) 除因子的次序外，每一个整数> 1都可以惟一地表示成素数的一个乘积.

为此只要证明若p可以整除两个数的乘积ab，则仅当它可以整除至少一个因子. 这是定理 4 的推论：若素数不能整除a，则作为一个素数，它与a不能存在任何公因子，从而$(a,p) = 1$. 因此，对于每一个正整数b由定理 4 可知

$$(ab, pb) = b.$$

现在若 $p \mid ab$，则我们必须有 $p \mid b$；即素数 p 可整除乘积 ab 的另一个因子 b. 这一定理可以立即推广至多个因子的情况.

为了证明定理 5，我们考虑一个正数 a 的不同正素数 p_i, q_i 幂乘积的表示法

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}.$$

如同刚才所证明的，每一个素数 q 至少除得尽左端一个素因子，从而它与某 p_k 恒同. 因此，除可能的次序外，$q_1, \cdots, q_k$ 恒同于 $p_1, \cdots, p_r$；所以 $k = r$. 我们选取次序使 $p_i = q_i$. 若对应的指数不等，例如 $a_1 > b_1$，则把方程除以 $q_1^{b_1}$ 之后，则左端仍有因子 $p_1 = q_1$，而右端已没有这一因子. 因此 $a_1 = b_1$ 及一般地有 $a_i = b_i$.

在有了每一整数惟一素因子分解定理后，我们有一个处理上述问题本质不同的方法，例如，一个整数 b 是否整除另一个整数 a，如何寻求 (a, b) 或 a 与 b 的最小公倍等等. 特别若我们设想 a 与 b 被分解为它们的素因子 $p_1, \cdots, p_r$ 乘积

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$
$$b = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r},$$

此处 0 被允许作为指数 a_i, b_i，则 $b \mid a$ 成立显然当且仅当 $a_i \geqslant b_i$，进而言之，我们有

$$(a, b) = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}, d_i = \min(a_i, b_i), \quad i = 1, 2, \cdots, r,$$

$$v = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}, c_i = \max(a_i, b_i), \quad i = 1, 2, \cdots, r.$$

无穷多个素数的存在性立即从下面的事实中得到：

$$z = p_1 \cdot p_2 \cdots p_n + 1$$

为一个数，它不能被任何素数 $p_1, \cdots, p_n$ 整除，因此至少被一个异于 $p_1, \cdots, p_n$ 的素数整除. 从而若有 n 个素数，则有 $n+1$ 个素数.

§2. 同余式与剩余类

由前一节可知，由一个整数 $n \neq 0$ 立即决定了按剩余 $\bmod n$，

所有整数的分布.我们把两个 mod$n$ 有同样剩余的整数a 与b 归于同样的剩余类 mod$n$,或更简单些,同样的类 mod$n$,并记为

$$a \equiv b(\mathrm{mod}n)(a \text{ 同余于} b \text{ 模} n).$$

它等价于 $n \mid a-b$.若 a 不同余于 b 模 n,则记为 $a \not\equiv b(\mathrm{mod}n)$,$a \equiv 0(\mathrm{mod}n)$表示 a 可以被 n 整除,每一个数都称为它所在类的代表.因为 mod$n$ 的不同剩余为 $0,1,\cdots,|n|-1$,所以 mod$n$ 的不同剩余类个数为$|n|$.下面是一些易于验证的同余式的运算规律:若 a,b,c,d 为整数,$n \neq 0$,则我们有

(i) $a \equiv a(\mathrm{mod}n)$.

(ii) 若 $a \equiv b(\mathrm{mod}n)$,则 $b \equiv a(\mathrm{mod}n)$.

(iii) 若 $a \equiv b(\mathrm{mod}n)$及 $b \equiv c(\mathrm{mod}n)$,则 $a \equiv c(\mathrm{mod}n)$.

(iv) 若 $a \equiv b(\mathrm{mod}n)$及 $c \equiv d(\mathrm{mod}n)$,则 $a \pm c \equiv b \pm d(\mathrm{mod}n)$.

(v) 若 $a \equiv b(\mathrm{mod}n)$,则 $ac \equiv bc(\mathrm{mod}n)$.

一般说来,由 $a \equiv b(\mathrm{mod}n)$与 $c \equiv d(\mathrm{mod}n)$可得 $ac \equiv bd(\mathrm{mod}n)$.特别若 $a \equiv b(\mathrm{mod}n)$,则对每一个正整数 k 皆有 $a^k \equiv b^k(\mathrm{mod}n)$,不断运用(iv)与(v),我们得:若 $a \equiv b(\mathrm{mod}n)$,则 $f(a) \equiv f(b)(\mathrm{mod}n)$,此处 $f(x)$为一个有整系数的 x 的整有理函数(x 的多项式).

总之,对于整有理运算而言,我们可以计算同样模的同余式就如同通常的方程运算一样.但除法就不一样.若 $ca \equiv cb(\mathrm{mod}n)$,则不能由此得出 $a \equiv b(\mathrm{mod}n)$.这是由于假设的意思是 $n \mid c(a-b)$.现在若$(n,c)=d$,则我们进而有

$$\left(\frac{n}{d},\frac{c}{d}\right)=1, \quad \frac{n}{d} \Big| \frac{c}{d}(a-b).$$

所以由定理 4 可知

$$\frac{n}{d} \Big| a-b, \text{即 } a \equiv b\left(\mathrm{mod}\frac{n}{d}\right).$$

例如:由 $5 \cdot 4 \equiv 5 \cdot 1(\mathrm{mod}15)$不能导出 $4 \equiv 1(\mathrm{mod}15)$,仅能得出它们同余 $\mathrm{mod}\left(\frac{15}{5}\right)=3$,因此我们能得到

定理 6 若 $ca \equiv cb(\mathrm{mod}n)$,则

$$a \equiv b\left(\mathrm{mod}\frac{n}{d}\right),$$

其中$(c,n)=d$.

据此可得出下面的结论:两个整数的乘积可能同余于 0 mod$n$,尽管每一个因子都没有这个性质.

例如 $2\cdot 3 \equiv 0(\mathrm{mod}\ 6)$,尽管 2 与 3 都$\not\equiv 0(\mathrm{mod}\ 6)$,对于不同模的同余式之间的关系,我们由定义直接得知:若一个同余式对 mod$n$ 成立,则它对于模 n 的每一个因子都成立.特别对于模 $-n$ 成立.进而言之,若

$$a \equiv b(\mathrm{mod}n_1) \text{ 与 } a \equiv b(\mathrm{mod}n_2),$$

则

$$a \equiv b(\mathrm{mod}v).$$

其中 v 为 n_1 与 n_2 的最小公倍.

由于剩余类 mod$n$ 与剩余类 mod $-n$ 是一致的,所以仅研究模一个正整数 n 的剩余类即可.

一个 n 个整数的数系,它正好包含 mod$n$ 的每一个剩余类的代表,则称为一个完全剩余系 mod$n$.

由于一个完全剩余系 mod$n$ 包含 $|n|$ 个不同的数,$|n|$ 个互不同余的数 mod$n$ 总是一个完全剩余系 mod$n$,例如,诸数 0,1,$\cdots$,$|n|-1$.更一般地有

定理 7 若 $x_1,\cdots,x_n$ 为一个完全剩余系 mod$n$($n>0$),则 $ax_1+b,\cdots,ax_n+b$ 亦是一个完全剩余系.其中 a,b 为整数及 $(a,n)=1$.

事实上,由定理 6 可知,n 个数ax_i+b ($i=1,2,\cdots,n$)同样是互不同余 mod$n$ 的.

下面给出的关于复合数模的剩余系的表示常常是很有用的.

定理 8 若 $a_1,\cdots,a_n$ 为两两互素的整数,则一个完全剩余系 mod A,由形如

$$L(x_1,\cdots,x_n)=\frac{A}{a_1}c_1x_1+\frac{A}{a_2}c_2x_2+\cdots+\frac{A}{a_n}c_nx_n$$

的数给出，此处 $A = a_1 a_2 \cdots a_n$ 及 x_i 独立地过一个完全剩余系 $\bmod a_i$，其中 c_i 为任意与 a_i 互素的整数.

这种 L 的个数为 $|A|$，而且它们互不同余 $\bmod A$. 事实上，由同余式 $\bmod A$

$$L(x_1, \cdots, x_n) \equiv L(x'_1, \cdots, x'_n) (\bmod A)$$

可知，这一同余式模每一个 a_i 仍成立. 由于

$$\frac{A}{a_k} \equiv 0 (\bmod a_i)，\text{其中 } k \neq i,$$

所以当 $i = 1, \cdots, n$ 时

$$c_i \frac{A}{a_i} x_i \equiv c_i \frac{A}{a_i} x'_i (\bmod a_i).$$

进而言之，由于 $(c_i, a_i) = 1$ 及 $\left(\frac{A}{a_i}, a_i\right) = 1$，所以由定理 6 可知 $x_i \equiv x'_i (\bmod a_i)$. 因此定理 8 中所示的数 L 总是互不同余 $\bmod A$ 的.

用同法可以证明如果让 $x + by$ 中的 x 通过一个完全剩余系 $\bmod b$，而让 y 独立地通过一个完全剩余系 $\bmod a$，则 $x + by$ 通过一个完全剩余系 $\bmod a \cdot b$.

每一个剩余类 $\bmod n$ 的特征为这一类中任意数与 n 的最大公因子都相等. 因为若 $a \equiv b (\bmod n)$，则 $a = b + qn$，其中 q 为整数，所以 a 与 n 的每一个公因子都是 b 与 n 的一个公因子，且其逆亦真. 因此可以称一个剩余类 $\bmod n$ 与 n 的 GCD.

特别，我们要寻求与 n 互素的剩余类 $\bmod n$ 的个数. 这个数是欧拉函数 $\varphi(n)$. 首先 $\varphi(n)$ 对于一个素数 p 的幂的情况 $n = p^k$ 是容易确定的，这时 $\varphi(p^k)$ 为 $1, \cdots, p^k$ 中不被 p 整除的整数个数. 在这些数中能被 p 整除的数为 1 与 p^k 之间 p 的倍数，共有 p^{k-1} 个，所以

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

为了确定复合数 n 的 $\varphi(n)$ 值，我们现在来证明

引理 当 $(a, b) = 1$ 时，$\varphi(ab) = \varphi(a)\varphi(b)$.

由定理 8 可知，我们有形如 $ax + by$ 的完全剩余系 $\bmod ab$. 其

中 x 通过一个完全剩余系 mod$b$，及 y 通过一个完全剩余系 mod$a$，欲这样一个数与 ab 互素，即同时与 a 及 b 互素，其充要条件是$(ax,b)=1$ 及$(by,a)=1$. 由于$(a,b)=1$，所以这一条件为$(x,b)=1$ 及$(y,a)=1$. 因此当我们命 x 通过与 b 互素的剩余类 mod$b$ 及 y 通过与 a 互素的剩余类 mod$a$ 时，$ax+by$ 就通过与 ab 互素的剩余类 modab，引理证完. 不断应用引理，若 n 分解为正素因子积 $n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$，则得

$$\varphi(n)=\varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_r^{a_r})=n\prod_{p\mid n}\left(1-\frac{1}{p}\right). \tag{4}$$

此处在乘积中，p 通过 n 的所有正素因子.

一个与 n 互素的完全剩余类 mod$n$ 称为一个既约剩余类 mod$n$，它包含 $\varphi(n)$个剩余类，在每一个这种类中取一个代表构成的数系称为一个完全既约剩余系 mod$n$.

如同定理 7，我们可以证明：

若 $x_1,\cdots,x_h$ 为一个完全既约剩余系 mod$n$，则当$(a,n)=1$ 时，$ax_1,\cdots,ax_n$ 亦是一个完全既约剩余系 mod$n$.

由此我们得到关于每一个与 n 互素的整数 a 的非常重要的性质. 由于 $ax_1,\cdots,ax_h$ 中每一个数都同余于 $x_1,\cdots,x_h$ 中的一个数，所以 $ax_1,\cdots,ax_h$ 的乘积同余于乘积 $x_1\cdots x_h$，即

$$a^hx_1x_2\cdots x_h\equiv x_1x_2\cdots x_h(\mathrm{mod}n).$$

由于每一个 x 都与 n 互素，所以

$$a^h\equiv 1(\mathrm{mod}n).$$

由于 $h=\varphi(n)$，所以得

定理 9(费马定理) 对于每一个与 n 互素的数 a，我们有

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

特别当 n 为一个素数 $p(>0)$时，则 $\varphi(p)=p-1$，乘以 a 之后可知对于每一个整数 a，皆有同余式

$$a^p\equiv a(\mathrm{mod}p). \tag{5}$$

当我们在第二章中将群的一般概念引入这个研究中时，这个定理的重要性及其证明的核心就真正变成了可以理解的了. 这一定理