复杂同余方程求解的简单探究

何昊天

摘要：从同余的基础理论出发，分析几类同余方程的性质，并对其中具有代表性的离散对数问题和二次剩余问题的解的存在性与解法进行简单探究。浅谈离散对数问题在密码学中的运用与二次剩余在数论中的重要地位，展现同余方程重要的理论和应用价值。

关键词：同余方程；离散对数；大步小步算法；二次剩余；二次同余方程

同余是数论中一个重要的基本概念，利用同余及其相关定理来论证很多整除性问题将变得十分简便。在本学期的离散数学课上，老师已经给我们介绍了同余的基本概念与性质，并讲解了线性同余方程的求解方法，同时提及了二次同余方程求解的困难性。诚然，要将所有形式的同余方程统一起来，并给出一个通解，无疑是极为困难的。但我们仍可以从同余方程的茫茫海洋中汲取出几滴水来，对部分特殊情况进行研究，这亦会使我们受益匪浅。

本文将选取离散对数问题和二次剩余问题进行简单探究，其中离散对数已经在通信领域和军事领域有了广泛的运用，而与二次剩余相关的二次互反律在数论中有着极高的地位，甚至被高斯誉为算术理论中的“基石”。对它们进行探究，便是打开了同余方程的一扇窗，带来非凡的意义和乐趣。

1 同余方程概述

1.1 线性同余方程

线性同余方程指形如 $ax \equiv b(\mathrm{mod}\, m)$ 的一类方程，其中 $a \neq 0$，b，m 均为已知数，x 为未知数。在课堂上，我们已经学到了这类方程的解法：先将原方程转化为形如 $ax + my = b$ 的不定方程，根据 b 能否整除 $\gcd(a,m)$ 判断方程是否有解，若有解，则可以根据 Euclid 算法的流程找出其一组特解。

在得到一组特解后，我们不难利用整除和同余的性质找出方程的所有解，此处不再赘述。

1.2 线性同余方程组

线性同余方程组可以大致分为两类：一元线性同余方程组和多元线性同余方程组。

一元线性同余方程组指形如 $x \equiv b_1(\mathrm{mod}\, m_1)$，$x \equiv b_2(\mathrm{mod}\, m_2)$，…，$x \equiv b_n(\mathrm{mod}\, m_n)$ 的一组方程。若 m_1，m_2，…，m_n 两两互质，则根据中国剩余定理，可以找出方程组的所有解。若不互质，则可以对方程进行合并[1]，直到只剩一个同余方程，再对其进行求解。合并方程的方法不唯一，结合 Euclid 算法可以得到一个简便的合并方法，这里不再进一步讨论。

对于多元线性同余方程组，可以运用线性代数中的高斯消元法，在模意义下进行消元，

[1] 即将两个线性同余方程替换为一个新方程，且新方程的解集等于两个原方程的解集的交。

再借助解一元线性同余方程组的方法完成求解。

1.3 非线性同余方程

对只含一个未知数的同余方程进行推广，可以用 $f(x)\equiv 0(\mathrm{mod}\,m)$ 来描述一般情况。由 $f(x)$ 的不同形式可以导出不同类型的同余方程，在这里选取几种具有代表性的进行论述。

若 $f(x)$ 是一个次数大于等于 2 的多项式函数，则可以通过因式分解的方法来求解。考虑最基础的情形：$f(x)=ax^2+bx+c$，若 $ax^2+bx+c=a(x-x_1)(x-x_2)$，且 x_1，x_2 在模 m 剩余系下都有意义，则它们就是方程的两个解。类似地对更高次的多项式进行因式分解，就能得到它们的一些解。

不过这个解法具有很大的局限性，首先这种方法只能求出特解，难以推广到方程的一般解，其次不能用此法来判断解的存在性，例如 x^2+2x+3 无法进行因式分解，但同余方程 $x^2+2x+3\equiv 0(\mathrm{mod}\,6)$ 显然存在解 $x=1$。为了更深入的探究，我们可以做一些简化，即考虑 $b=0$ 的情况，此时问题便成了经典的二次剩余问题。对这个问题有十分可靠的解存在性判别方法和成套的求解方法，将在后文进一步讨论。

若 $f(x)=a^x+c$，则问题演变为了经典的离散对数问题。之所以称之为离散对数，是因为求解 x 相等于在剩余系下进行对数运算。对于这个问题已经有了完整的解法，且问题本身具有很高的实际意义，这些也将在后文中讨论。

若 $f(x)$ 是其它类型的基本初等函数甚至它们的有理运算与复合，也可以导出其它的求解同余方程的问题。但对于其中的大部分问题来说，目前还缺少有效的求解方法，且其中不乏孤问题[2]的存在，使得求解它们显得即困难又没有太大的意义。

2 离散对数问题

2.1 问题描述

离散对数问题指解形如 $a^x\equiv b(\mathrm{mod}\,m)$ 的一类方程，其中 $a\neq 0$，b，m 均为已知数，x 为未知数。这个问题到目前为止尚未完全解决[3]，不过对此问题已经有了一个优秀的算法：大步小步算法(Shank's Baby-Step-Giant-Step Algorithm)。利用此算法及其扩展，已经能够较快速地判断出解的存在性并找出该问题的所有解。

接下来将从特殊情况到一般情况，描述该算法的原理与流程。

2.2 m 为质数的情况

不妨假设 $a,b<m$，否则也只需要简单的转化即可满足该条件。

若 m 为质数，根据费马小定理，恒有 $a^{m-1}\equiv 1(\mathrm{mod}\,m)$，故原方程如果有解，则在

[2] 即难以归约、转化为其它问题的难题。
[3] 指还没有一个确定性的多项式算法。

$[0,m-1]$内一定有整数解。且若x_1是方程的解，那么$x_1+k(m-1),k\in Z$都是方程的解。同理不难证明方程所有的解都可以写作$x_1+k(m-1),k\in Z$的形式，其中$x_1\in[0,m-1]$。即我们只需要找出方程在$[0,m-1]$内的所有解，就可以找出方程的所有整数解。显然通过枚举的方法找到解是可行的，不过还可以继续探究效率更高的方法。

利用带余除法的性质，设原方程的解$x_1=q\lfloor\sqrt{m}\rfloor+r$，其中$\lfloor\sqrt{m}\rfloor$表示$\sqrt{m}$的整数部分，$q,r<\lfloor\sqrt{m}\rfloor$。由于$m$是质数，$a^r$在模$m$剩余系下一定存在乘法逆元，故解原方程等价为找一组$q$，$r$使其满足$a^{q\lfloor\sqrt{m}\rfloor}\equiv b\cdot a^{-r}(\mathrm{mod}\,m)$。由于$q$，$r$都不超过$\lfloor\sqrt{m}\rfloor$，故可以先计算出$a^0$，$a^1$，…，$a^{\lfloor\sqrt{m}\rfloor}$的值并从小到大排序得到一张表，然后枚举$q$的取值并计算$a^{q\lfloor\sqrt{m}\rfloor}$的值，再利用二分法在表中查找是否有相等的值，如果有，则这组q，r就可以导出原方程的一组解。如果枚举完成以后还没有找到满足条件的q，r，则原方程也是无解的。

由于枚举量不超过$\lfloor\sqrt{m}\rfloor$，二分法的步骤数是$\log_2\lfloor\sqrt{m}\rfloor$级别的，结合计算机科学中复杂度分析的方法，我们可以得出这个算法的时间复杂度是$O(\sqrt{m}\log m)$的。由于在实际应用中，m的值往往非常大，故这个算法的效率比起直接枚举已经相当优秀了。

至此，m为质数的情况已经得到了一个有效的解法。

2.3 a与m互质的情况

考虑这种情况的目的是为了理清上述算法中，哪些地方用到了m为质数这一性质。

第一个用到这条性质的地方是费马小定理。不过对于a与m互质的情况，我们可以运用其推广，即欧拉定理，使得由特解推出所有解的方法任然有效。若a与m互质，根据欧拉定理，有$a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$，其中$\varphi(m)$表示$m$的欧拉函数值。与上述算法同理，特解的范围被限定在了$[0,\varphi(m)]$中，且根据特解容易推出所有的解。

大步小步算法中用到m为质数性质的地方是a^r的乘法逆元的存在性，而我们知道当a与m互质时，a在模m剩余系一定有乘法逆元，故a^r的乘法逆元任然存在。

接下来只需模仿 2.2 中的算法，就可以解决a与m互质的情况了。

2.4 一般情况

在一般情况中，我们并不能限定解的范围，也不能保证乘法逆元的存在性。不过我们对特殊情况已经有了解法，故可以考虑将一般情况做同解变形转化为特殊情况。

将原方程写为$a^x+my=b$的形式，类比线性同余方程，设$d=\gcd(a,m)$，如果$b\nmid d$，则可以推出方程无解的结论。否则在方程两边同时除以d，得$\frac{a}{d}a^{x-1}+\frac{m}{d}y=\frac{b}{d}$。重新构造同余方程$\frac{a}{d}a^{x-1}\equiv\frac{b}{d}(\mathrm{mod}\,\frac{m}{d})$，由于此时一定有$\gcd(\frac{a}{d},\frac{m}{d})=1$，故$\frac{a}{d}$一定存在乘法逆元。不妨设$x'=x-1$，$b'=\frac{b}{d}\left(\frac{a}{d}\right)^{-1}$，$m'=\frac{m}{d}$，则得到了一个新的离散对数问题：$a^{x'}\equiv b'(\mathrm{mod}\,m')$。如果此时$a$与$m'$互质，则直接套用 2.3 的解法即可，否则的话就继续做上述变形，直到a与m'互质为止。

注意到上述变形中，模数的值是严格单调递减的，故算法一定会终止。同时易证在变形

的过程中解的数量没有改变，且变形后的方程的每个解唯一对应原方程的一个解。由于 m 的因数个数是 $\sqrt{m}$ 级别的，故整个流程的效率瓶颈任然在大步小步算法上。

至此，离散对数问题的一般情况已经得到了一个有效的解法。

2.5 离散对数与密码学

在密码学中，伪随机数的产生是设计密码时必不可少的一环。在构造序列密码时，有一种方法称为复杂性理论方法，即使密码系统的破解难度基于或等同于一些已知的难题，而离散对数问题则是其中非常具有代表性的一个问题。

著名的 Blum-Micali 发生器正是利用计算离散对数的难度来保证它的安全性：

设 g 是质数，P 是奇质数，x_0 是密钥，令 $x_{i+1}=g^{x_i} \bmod P$。若 $x_i<\frac{p-1}{2}$，则发生器在该位输出是 1；否则，输出是 0。

如果 P 足够大，使用大步小步算法计算离散对数的代价是相当大的，在密码学中，如果破解的代价大于破解后获得的利益，那么可以认为这个密码系统就是安全的。在这一点上，离散对数问题的价值得到了体现：基于其求解的困难设计密码体现了它的理论价值；如果真的找出了多项式解法，很多密码破译问题便迎刃而解，这在军事和政治上意义重大。

离散对数的应用远不限于此，但碍于篇幅，这里不再额外举例。

3 二次剩余问题

3.1 问题描述

二次剩余问题指解形如 $x^2 \equiv a(\bmod m)$ 的一类二次同余方程，其中 a，m 均为已知数，x 为未知数。如果存在满足条件的 x，则称 a 是模 m 的一个二次剩余；否则，称 a 是模 m 的一个非二次剩余。故为了求解原方程，判断一个数是否为模 m 的二次剩余（即判断解的存在性）显得尤为重要。

这一部分将简单解决二次剩余判别问题的基础。为了解决这一问题，需要引入一些符号，并用到著名的二次互反律。

3.2 勒让德符号

若 p 为奇质数，a 为整数，则记 $L(a,p)$ 为 a 关于 p 的勒让德符号[4](Legendre symbol)，其值规定为：

$L(a,p)=1$，如果 $p \nmid a$ 且 a 是模 p 的二次剩余

$L(a,p)=-1$，如果 $p \nmid a$ 且 a 是模 p 的二次剩余

$L(a,p)=0$，如果 $p \mid a$

勒让德符号具有很多优秀的性质，这里仅不加证明地列举一条与其计算有关的性质，即

[4] 常用 $\left(\frac{a}{p}\right)$ 表示勒让德符号，文中的表示方法是为了与雅克比符号做出区分。

欧拉判别准则：$a^{\frac{p-1}{2}} \equiv L(a,p)(\mathrm{mod}\ p)$。

这条准则已经可以用于二次剩余的判别，但仅限 p 为奇质数的情况。

3.3 雅克比符号

雅克比符号是勒让德符号的推广。若 m 为大于 1 的奇数，a 为整数，则记 $J(a,m)$ 为 a 关于 m 的雅克比符号(Jacobi symbol)，其值规定为：

$J(a,m)=\prod L(a,p_i)$

其中 p_i 是质数且 $\prod p_i = m$，允许 p_i 中有相同的值出现。

注意雅克比符号的值不能类比勒让德符号用于二次剩余的判别(两者的定义是不同的)，例如：$J(7,143)=L(7,11)\cdot L(7,13)=(-1)\cdot(-1)=1$，但事实上 7 不是模 143 的平方剩余。但倘若 $J(a,m)=-1$，可以断言 a 是模 m 的非二次剩余。

3.4 二次互反律

不加证明地给出二次互反律：$L(p,q)\cdot L(q,p)=(-1)^{\frac{(p-1)(q-1)}{4}}$，其中 p，q 为奇质数。

利用二次互反律，可以把 $x^2 \equiv p(\mathrm{mod}\,q)$ 和 $x^2 \equiv q(\mathrm{mod}\ p)$ 的解联系起来。简单来说，设 $q'=(-1)^{\frac{q-1}{2}}q$，则根据二次互反律，$x^2 \equiv p(\mathrm{mod}\,q)$ 有解当且仅当 $x^2 \equiv q'(\mathrm{mod}\ p)$ 有解。

利用二次互反律，可以得到勒让德符号的快速计算方法，使得当模数为奇质数时二次剩余的判别变得简单可行。使用强数学归纳法，可以得出雅克比符号也满足二次互反律，也就可以用类似方法导出一个针对模数为奇数的二次剩余判别方法。

接下来就来考虑如何求解二次同余方程 $x^2 \equiv a(\mathrm{mod}\,m)$。

4 二次同余方程的解

4.1 $m=p$ 为奇质数的情况

根据欧拉准则，若 a 是模 p 的二次剩余，则有 $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$。

不妨设 $p-1=2^t\cdot s(2\nmid s)$，令 $x_{t-1}=a^{\frac{s+1}{2}}$，可以推出 $(a^{-1}\cdot x_{t-1}^2)^{2^{t-1}} \equiv 1(\mathrm{mod}\ p)$。观察发现原方程可以变形为 $(a^{-1}\cdot x^2)^{2^0} \equiv 1(\mathrm{mod}\ p)$，故我们可以考虑设法从 x_k 递推到 x_{k-1}，而 x_0 就是原方程的解。为了求解方便，记 $\xi_k = a^{-1}\cdot x_k^2$ 为模 p 的 2^k 次单位根，则有 $\xi_k^{2^k} \equiv 1(\mathrm{mod}\ p)$，接下来考虑从 2^{k-1} 次单位根和 2^k 次单位根之间的关系入手完成递推。

由 $\xi_k^{2^k} \equiv 1(\mathrm{mod}\ p)$ 知 $\xi_k^{2^{k-1}} = \pm 1(\mathrm{mod}\ p)$。

若 $\xi_k^{2^{k-1}} \equiv 1(\mathrm{mod}\ p)$，则令 $x_{k-1}=x_k$ 即可。

若 $\xi_k^{2^{k-1}} \equiv -1(\mathrm{mod}\ p)$，我们假设存在 λ 使得 $(a^{-1}\cdot(\lambda\cdot x_k)^2)^{2^{k-1}} \equiv 1(\mathrm{mod}\ p)$，如果存在，则令 $x_{k-1}=\lambda\cdot x_k$ 即可。显然 λ 只需满足 $\lambda^{2^k} \equiv -1(\mathrm{mod}\ p)$，根据欧拉准则，若一个数 b 是模 p 的非二次剩余，则有 $b^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\ p)$，故我们可以找出模 p 的一个非二次剩余 b，再令 $\lambda = b^{2^{t-k-1}\cdot s}$ 即完成了递推。

易知模 p 的非二次剩余恰有 $\frac{p-1}{2}$ 个，故可以在 $[1,p-1]$ 之间随机取值并进行验证，期望意义下选取两次就可以找出一个满足条件的 b。显然对于模 p 的一个二次剩余，在其剩余系下恰有两个互为加法逆元的解，故递推出一个 x_0 后易求另一个解。

至此，$m=p$ 为奇质数的情况已完全解决。

4.2 $m=p^q$ 为奇质数的幂的情况

不失一般性，$a=0$ 时的解是平凡的。

设 $a=p^k\cdot a'(p\nmid a')$，由于 x^2 中含有因数 p 的次数显然为偶数，故当且仅当 $2\mid k$ 时 a 是模 p^q 的二次剩余。此时由于 p^k 是完全平方数，故它是任意模数的二次剩余。根据雅可比符号的相关性质，易推出如下结论：对于同一个模数，两个二次剩余或非二次剩余的乘积仍是二次剩余，一个二次剩余和一个非二次剩余的乘积是非二次剩余。再由 p^k 一定是模 p^q 的二次剩余，故 a 是模 p^q 的二次剩余当且仅当 a' 是模 p^q 的二次剩余。不妨设 $x=p^{\frac{k}{2}}\cdot x'$，则方程 $x'^2\equiv a'(\mathrm{mod}\ p^{q-k})$ 的解与原方程的解一一对应。

现在问题已经被规约为了求解方程 $x^2\equiv a(\mathrm{mod}\ p^q)(p\nmid a)$，接下来只考虑这个新问题。

设 g 是模 p^q 的一个原根[5]，当 $2\mid k$ 时 g^k 显然是模 p^q 的二次剩余。当 $2\nmid k$ 时，根据原根的性质易知 $\gcd(g^k,p^q)=1$，故可推出时 g^k 一定是模 p^q 的非二次剩余。

取出一个模 p^q 的二次剩余 g^{2k}，结合欧拉定理有 $(g^{2k})^{\frac{\varphi(p^q)}{2}}\equiv(g^k)^{\varphi(p^q)}\equiv 1(\mathrm{mod}\ p^q)$。

取出一个模 p^q 的非二次剩余 g^{2k+1}，有 $(g^{2k+1})^{\frac{\varphi(p^q)}{2}}\equiv(g^k)^{\varphi(p^q)}\cdot g^{\frac{\varphi(p^q)}{2}}\equiv g^{\frac{\varphi(p^q)}{2}}(\mathrm{mod}\ p^q)$。因为 g 是模 p^q 的一个原根，故 $g^{\varphi(p^q)}\not\equiv g^{\frac{\varphi(p^q)}{2}}(\mathrm{mod}\ p^q)$，故 $g^{\frac{\varphi(p^q)}{2}}\equiv -1(\mathrm{mod}\ p^q)$，则有 $(g^{2k+1})^{\frac{\varphi(p^q)}{2}}\equiv -1(\mathrm{mod}\ p^q)$。

综上所述，可以得到一个欧拉准则的推广：$a^{\frac{\varphi(p)}{2}}\equiv L(a,p)(\mathrm{mod}\ p),\gcd(a,p)=1$。运用此结论，再套用 4.1 中的算法，就可以得到原问题的解。

至此，$m=p^q$ 为奇质数的幂的情况已完全解决。

4.3 $m=2^q$ 为 2 的幂的情况

与 4.2 同理，该问题可以被规约为求解方程 $x^2\equiv a(\mathrm{mod}\ 2^q)(2\nmid a)$，故接下来也只考虑规约后的问题。

由于 a 是奇数，方程的解 x 也是奇数。设 $x=2k+1$，有 $x^2=(2k+1)^2=4k(k+1)+1$，因为 $4k(k+1)+1\equiv 1(\mathrm{mod}\ 2^3)$，所以 $a\equiv 1(\mathrm{mod}\ 2^3)$，结合模数为 2^1，2^2 的两种特殊情况，不难得出结论：若 a 是模 2^q 的二次剩余，则 $a=8t+1,t\in Z$。实际上，这个结论也是 a 为二次剩余的充分条件，将在下文中继续说明。

在开始求解之前，先说明解的个数问题。假设 $x^2\equiv a(\mathrm{mod}\ 2^q)$ 有一个解 x_1，那么显然 $-x_1$ 也是方程的解。考虑 x_1+2^{q-1}，有 $(x_1+2^{q-1})^2=x_1^2+2^q\cdot x_1+2^{2(q-1)}\equiv x_1^2(\mathrm{mod}\ 2^q)$，故 $\pm(x_1+2^{q-1})$ 均为方程的解。假设 $a=8t+1,t\in Z$ 是 a 为模 2^q 的二次剩余的充分条件，而对

[5] 称 g 是模 p 的一个原根，当且仅当 $g^1,g^2,\cdots,g^{\varphi(p)}$ 的值两两不同，原根一般很小，可以枚举求得。

于不同的 a，解显然是不同的，那么易知方程恰有 4 个解[6]。

现在假设我们已经得到了方程 $x^2 \equiv a(\mathrm{mod}\, 2^q)$ 的 4 个解 $\pm x_1$，$\pm(x_1 + 2^{q-1})$，考虑如何从它们递推出方程 $x^2 \equiv a(\mathrm{mod}\, 2^{q+1})$ 的解。模 2^q 意义下的解放到模 2^{q+1} 意义下，只有两种可能：是方程 $x^2 \equiv a(\mathrm{mod}\, 2^{q+1})$ 的解，或者是方程 $x^2 \equiv a + 2^q(\mathrm{mod}\, 2^{q+1})$ 的解。将原来的 4 个解各加上 2^q，得到 4 个新解，故只用考虑如何在 8 个解中找出 $x^2 \equiv a(\mathrm{mod}\, 2^{q+1})$ 的 4 个解即可完成递推。

更进一步，$\pm x_1$ 从模 2^q 意义下放到模 2^{q+1} 意义下，平方值仍然相等，$\pm(x_1 + 2^{q-1})$ 也同理，故只需从 8 个解中任取 1 个进行试验，就可以得出结论。

考虑 $x^2 \equiv a(\mathrm{mod}\, 2^3)$，可以验证当且仅当 $a = 1$ 时方程有 4 个解 ± 1，± 5，再结合上面的递推关系，可以证明 $a = 8t + 1, t \in Z$ 是 a 为模 2^q 的二次剩余的充分条件，同时也可以求出所有满足条件的 a 对应的解。

至此，$m = 2^q$ 为 2 的幂的情况已完全解决。

4.4 一般情况

现在来完成一般情况的解。根据算术基本定理，不妨设 $m = p_1^{q_1} p_2^{q_2} \ldots p_n^{q_n}$，其中 p_1，p_2，…，p_n 均为质数且互不相同。我们考虑如下方程组：

$x^2 \equiv a(\mathrm{mod}\, p_1^{q_1})$，$x^2 \equiv a(\mathrm{mod}\, p_2^{q_2})$，…，$x^2 \equiv a(\mathrm{mod}\, p_n^{q_n})$

这些方程的解法都已经完成了讨论，故可令它们的一组解依次为 x_1，x_2，…，x_n。再来解如下同余方程组：

$x \equiv x_1(\mathrm{mod}\, p_1^{q_1})$，$x \equiv x_2(\mathrm{mod}\, p_2^{q_2})$，…，$x \equiv x_n(\mathrm{mod}\, p_n^{q_n})$

根据中国剩余定理知，它们的解等价于方程 $x \equiv x_0(\mathrm{mod}\, m)$ 的解，其中 x_0 恰好是原方程 $x^2 \equiv a(\mathrm{mod}\, m)$ 的解。

至此，二次同余方程的一般情况已经得到了一个有效的解法。

4.5 二次剩余的意义

求解二次同余方程在密码学和大数分解等应用领域同离散对数问题一样有着重要的意义，在此对这些不再进一步讨论，而是简单展示一下二次剩余的理论价值。

二次剩余问题具有悠久的历史，最初是费马把一系列质数表示为平方和的形式并给出了一些命题，开启了二次剩余问题的前期探索，为了证明费马的这些问题，而间接导致了二次互反律的发现。欧拉首先给出了定理的叙述，并给出了几个相关的猜想。后来由勒让德证明了有关猜想，又给出了二次互反律的完整表述。而直到高斯给出了二次互反律的第一个证明，这个问题才算是初步解决。

高斯一生一共给出了二次互反律的 8 个证明，而至今该定理的证明足足有 200 余种之多，如此多的证明方式足以表示，这个定理十分基础而典雅，难怪高斯称之为“基石”，将其誉

[6] 可能包含重根。

为“黄金定理”。

对二次互反律最初的一个应用是，由该定理可以导出狄利克雷定理[7]，两者的等价性在勒让德时代就已经得到证明。我们知道数论中有关质数的证明，尤其是其中一些简洁而优美的定理，往往有着“皇冠上的宝石”般的美誉，如家喻户晓的哥德巴赫猜想便是一例。而二次互反律直接摘下了其中一枚宝石，足以展示其理论价值之高。

到了今天，二次互反律在数论的发展中仍然处于中心地位，在高斯给出证明地 100 年后，以此为基础逐渐发展出了类域论，并奠定了解析数论，而对于高次互反律的研究，也一直有人在孜孜不倦地进行着。如此，足见二次剩余在数论中的深刻性。

5 结束语

同余作为数论的奠基石，与其各个方向的发展都密切相关。此外，同余和模算术在数学的其它分支、计算机科学、化学甚至法律、音乐等领域都有着广泛的应用，而同余方程在其中都占据了重要的地位，展现出了同余理论的重要意义。即使抛开这些不谈，对纯粹数学的研究本就能带来无穷的乐趣，相信同余理论的发展，将会继续给世人带来震撼。

参考文献

[1]Rosen, K.H.著. 离散数学及其应用（原书第 7 版） [M]. 徐六通, 杨娟, 吴斌, 译. 北京: 机械工业出版社, 2014.

[2]Cormen, T.H.等著. 算法导论（原书第 3 版） [M]. 殷建平, 徐云, 王刚, 刘晓光, 苏明, 邹恒明, 王志宏, 译. 北京: 机械工业出版社, 2013.

[3]Ronald, L.G.等著. 具体数学：计算机科学基础（第 2 版） [M]. 张明尧, 张凡, 译. 北京: 人民邮电出版社, 2013.

[4]Schneier, B.著. 应用密码学：协议、算法与 C 源程序（原书第 2 版） [M]. 吴世忠, 祝世雄, 张文政, 等译. 北京: 机械工业出版社, 2014.

[5]顾森著. 思考的乐趣：Matrix67 数学笔记[M]. 北京: 人民邮电出版社, 2012.

[6]Wikipedia. 二次剩余 [Z/OL]. https://en.wikipedia.org/wiki/Quadratic_residue

[7]Wikipedia. 二次互反律 [Z/OL]. https://en.wikipedia.org/wiki/Quadratic_reciprocity

[8]miskcoo. Miskcoo's Space [Z/OL]. http://blog.miskcoo.com/

[7] 对于任意互质的正整数 a,d，有无限多个形如 $a+kd,k\in Z$ 的质数。