第 9 章 初等数论基础

初等数论以整数的基本运算和性质为核心，内容包括整除理论、素数与合数体系，最大公因数、素因子分解、同余、不定方程等核心内容。相关内容是安全加密、隐私计算、离散优化与高效编码等领域的底层数学支撑。

9.1 整除理论与素数

整除理论与素数是整个数论体系的基石，素数的性质与分布规律是同余、不定方程、密码学的基础。

9.1.1 整除的定义与性质

1）整除的定义

定义 9.1：整数整除

设 a, b 为整数，且 $b\neq0$。若存在整数 c， 使得 $a=bc$，则

（1）称 a 被 b 整除，或 b 整除 a，记作 $b|a$；

（2）此时称 a 是 b 的倍数，b 和 c 都是 a 的约数（因子）；

（3）若不存在整数 c 满足上式，则称 b 不整除 a，记作 $b\nmid a$。

例如，对整数 6，有 8 个因子$\pm1, \pm2, \pm3$ 和±6，满足 $6=bc$。

定义 9.2：平凡因子与真因子

设 n 是大于 1 的正整数。若正整数 d 整除 n，则：

（1）$d=1$ 或 $d=n$ 时，称 d 为 n 的平凡因子；

（2）$1<d<n$ 时，称 d 为 n 的真因子。

例如，整数 6 的 8 个因子中，±1,和±6 是平凡因子； ±2 和 ±3 是真因子。

虽然整除体现的是整数之间一种确定、无剩余的倍数与因数关系，但在初等数论中，平凡因子、真因子、素数、合数、因数分解等概念，默认的讨论范围仅为正整数，不涉及负整数。其中平凡因子与真因子仅针对大于 1 的正整数定义，且仅考虑其正因子。负因子虽满足整除关系，但与对应正因子仅相差一个符号，并不改变整数的因子结构，为简化理论体系、避免重复讨论，一般不予考虑。

定理 9.1： 带余除法定理（除法算法）

设 a 为整数，d 为正整数，则存在唯一的一对整数 q（商）和 r（余数），使得 $a=dq+r$ 且满足 $0\leq r<d$。

定义 9.3：带余除法中的商与余数

设 a 为整数，d 为正整数，由带余除法定理，存在唯一整数 q 和 r 满足 $a=dq+r$，$0\leq r<d$。其中：

整数 q 称为商，可记为 $q = a \text{ div } d$；

整数 r 称为余数，记为 $r = a \bmod d$。

带余除法定理表明，对任意整数 a 与正整数 d，a 可唯一表示为 d 的整数倍与一个非负且小于 d 的余数之和，这一定理是整数结构分析、同余理论及数论推理的重要基础。商与余数的定义则给出了整数商 q 与余数 r 的标准符号表示，并通过记号 $a \bmod d$ 明确了数论中取余运算的唯一确定含义。

例如, 20 mod 6=2, −13 mod 4=3, 10 mod 2=0，$b|a$ 当且仅当 $a \bmod b = 0$（$q=-4$，$r=3$）。

2）整除的性质

定理 9.2：整除的性质

设 a, b, c, m 为整数，则下列结论成立：

（1）若 $a|b$ 且 $a|c$，则对任意整数 x, y，有 $a \mid (xb+yc)$；

（2）若 $a|b$ 且 $b|c$，则 $a|c$；

（3）若 $m\neq 0$，则 $a|b$ 当且仅当 $ma|mb$；

（4）若 $a|b$ 且 $b|a$，则 $a=b$ 或 $a=-b$；

（5）若 $a|b$ 且 $b\neq 0$，则 $|a|\leq|b|$。

整除的线性组合性质（1）用于将多个整除关系合并，是证明最大公因子、线性组合表示、互素性质的核心工具。传递性（2）用于链式推导整除关系，使整除成为一种偏序关系，是数论中进行递推、归纳、结构分析的基础。乘法等价性（3）建立了整除与整数乘法的一致性，可用于消去公因子、简化整除式、统一等价条件。反对称性（4）刻画了整除关系的 “单向性”，保证整数在整除意义下的唯一性，是素数、因子分解唯一性的基础。绝对值性质（5）给出了因子大小的上界，限制了因子的可能范围，是因子查找、素性检验、整数分解的重要依据。

9.1.2 素数的定义与性质

古希腊数学家基于整数乘法的因数分解特性（乘法可分解性），将大于 1 的正整数分为不能再分解的素数与可分解的合数，揭示了整数的乘法基本结构，为早期数论研究奠定了理论基础。

1）素数的定义

定义 9.4：素数与合数

大于 1 的整数 n，如果满足仅有正因子 1 和 n，则称 n 为素数（质数）。

大于 1 的整数 n，如果不是素数，则称 n 为合数。

注：素数、合数均只对大于 1 的正整数定义；1 既不是素数，也不是合数；素数没有真因子，合数必有真因子。例如, 2,3,5,7,11 是素数, 4,6,8,9 是合数。

2）素数与合数的基本性质（定义直接推论）

定理 9.3： 素数与合数的基本性质

(1) 整数 $a>1$ 是合数当且仅当存在整数 b, c，满足 $a=bc$，$1<b<a$， $1<c<a$；

(2) 任何大于 1 的合数必存在素因子；

(3) 素数的大于 1 的正因数只有其自身：若 p 为素数， $d>1$ 且 $d|p$，则 $d=p$。

性质（1）从可分解性说明合数至少存在一个非平凡因子（即既不是 1 也不是自身的因子）。性质（2）指出合数的因子最终可归结为素数，素数是构成合数的基本单元，体现了整数在乘法结构中的原子性。性质（3）刻画了素数的核心特征，即仅有 1 和自身两个正因子，强调素数在乘法意义下不可再分。

引理 9.1：欧几里得引理

设 p 为素数， 若 $p|ab$，则 $p|a$ 或 $p|b$。

推广：若素数 $p|a_1a_2\cdots a_k$，则存在某个 i 使得 $p|a_i$。

注：合数一般不具备该性质，即对合数 d，$d|ab$ 不能推出必有 $d|a$ 或 $d|b$。

欧几里得引理描述了素数的高阶性质，说明一个素数 p 去整除两个数相乘的结果 ab，它不会“一部分整除 a、一部分整除 b”，而是完整地整除其中某一个数，不会被拆分到两个乘数里。这是素数区别于合数的本质，也是整数唯一素因数分解的理论基础。例如，例如素数 $3|4\times6$，则只能整除 4 或 6 其中之一；合数 $4|2\times6$，但 4 既不整除 2、也不整除 6，它被“拆分”在两个乘数里。

3）素数的判定方法

定理 9.4：素数有限判别定理

设整数 $n>1$，若 n 不能被任一满足 $p \le \sqrt{n}$ 的素数 p 整除，则 n 为素数。

证明：采用反证法。

假设整数 $n>1$ 为合数，根据合数定义，必存在正整数 a,b，使得 $n=ab$，$1<a,b<n$。

不妨取 $a \le b$，则有 $a^2 \le ab=n$，即 $a \le \sqrt{n}$。

因为 $a>1$，故 a 存在素因子 p。由欧几里得引理可知，若素因子 $p|a$ 且 $a|n$，则必有 $p|n$。

同时由于 $p \le a \le \sqrt{n}$，可知存在不超过 $\sqrt{n}$ 的素数 p 整除 n，与定理前提条件矛盾，故 n 必为素数。

基于该定理可得到最为基础的试除法，用于单个小整数的素性检验，另外还存在几类其他素数判定方法：一是利用数论同余性质的定理判别法，通过威尔逊定理、费马小定理等条件间接判断；其次是适用于超大整数的快速素性测试方法，主要包括米勒 - 拉宾素性测试（概率性测试方法）和 AKS 素性测试（确定性测试方法）；三是批量筛法，如埃拉托斯特尼筛、线性欧拉筛法可批量筛选出指定范围内的全部素数。这些判定方法层层递进，分别适配基础计算、理论推导与大数高效运算等不同场景需求。

9.1.3 算术基本定理

算术基本定理证明了所有大于 1 的正整数，均可在不计素因子排列顺序的前提下，唯一分解为素数幂的乘积，确立素数是正整数的基本构造单元，揭示了素数与合数的内在本质联系，同时为公因数、公倍数、数论函数等数论内容提供核心理论支撑，搭建起完整自洽的正整数理论体系。

定理 9.5：算术基本定理

每个大于 1 的整数，都可以唯一表示为若干素数的乘积。若将所有素因子按照非递减次序排列，则任意大于 1 的整数 a 均可唯一分解为素数幂的乘积：$a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$，其中 $p_1,p_2,\dots,p_k$ 是不相同的素数，$r_1,r_2,\dots,r_k$ 是正整数。

例如，$30=2\times3\times5$，$117=3^2\times13$，$1024=2^{10}$，指数 1 可省略不写。

推论 9.1：正因数的素分解推论

设正整数 a 的标准素分解为 $a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$，其中 $p_1,p_2,\dots,p_k$ 为互异素数，$r_1,r_2,\dots,r_k$ 为正整数。正整数 d 是 a 的正因数，当且仅当 $d = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ 满足 $0 \le s_i \le r_i$，$i=1,2,\dots,k$。

该推论进一步揭示了正整数素分解后的 2 个特点，一是正整数分解后所有正因数只能由它本身所包含的素数构成，不会产生新的素因子；二是各素因子的幂次不会超过原整数对应素数的幂次，指数为 0 表示不含该素因子。该推论将整除关系与正因数判定问题转化为简洁直观的素因子指数大小比较。

例如，正整数 36 的标准素分解为 $36=2^2\cdot 3^2$。根据该推论，36 的所有正因数只能由素数 2,3 构造，不会出现 5,7,11 等新素因子；其中素数 2 的指数满足 $0\le s_1\le 2$，素数 3 的指数满足 $0\le s_2\le 2$。

定理 9.6：因子个数定理

设正整数 n 的标准素因子分解为：$n=p_1^{r_1}\,p_2^{r_2}\dots p_k^{r_k}$ 则 n 的正因子个数函数 $\tau(n)=(r_1+1)(r_2+1)\cdots(r_k+1)=\prod_{i=1}^{k}(r_i+1)$ 。

当 n 为素数时，$\tau(n)=2$。

9.1.4 素因子分解与判定方法

素数判定与素因子分解是数论的核心，针对不同规模的整数，可选用不同的求解方法。

1）素因子分解方法

（1）试除法：依据素数与整除的基本性质，对待分解整数从小到大依次用素数试除，不断析出素因子并化简商；只需检验不超过该数平方根的素数，即可完成素性判定与素因子分解，是基础的整数分解通用方法。

（2）埃拉托色尼筛法：基于 “素数的倍数均为合数” 这一性质，预先构造连续整数序列，从最小素数开始，逐次标记每个素数的所有倍数，最终未被标记的数即为区间内全部素数，多用于批量素数快速筛选。

（3）大整数分解算法：针对超大整数分解效率不足的问题，在基础分解方法之上，结合同余理论、二次剩余、椭圆曲线等高等数论工具构建的一类高效算法，典型包含费马分解法、椭圆曲线分解法、数域筛选法，主要应用于密码学与信息安全领域的大整数素因子分解。

例 9.1： 21560 有多少个正因子?

解：

（1）用试除法完成素因子标准分解

①从最小素数 2 开始试除，直到不能再被 2 整除：21560÷2=10780、10780÷2=5390、5390÷2=2695，连续除以 2 共 3 次，得素因子 2^3。

②用素数 5 试除共 1 次，得素因子 5^1，余 539。

③继续用素数 7 试除 2 次，得素因子 7^2，余 11。

④余数 11 为素数，得素因子 11^1。

综上，标准素因子分解：$21560=2^3\times5^1\times7^2\times11^1$

（2）根据正因子个数定理，$\tau(21560)=(3+1)(1+1)(2+1)(1+1)=4\times2\times3\times2=48$

结论：21560 共有 48 个正因子。

例 9.2：10!的二进制表示中从最低位数起有多少个连续的 0?

解：依据①一个二进制数中末尾连续的 0 表示了该数能被 2 的多少次幂整除；②十进制数的二进制表示中， 每个末尾的 0 代表该数可以被 2 整除一次。

$10!=1\times2\times3\times2^2\times5\times(2\times3)\times7\times2^3\times3^2\times(2\times5)$的质因子分解为：$10!=2^8\times3^4\times5^2\times7$ ，故 10!的二进制表示中从最低位数起有 8 个连续的 0。

2）素数的无限性

大于 1 的正整数集是无限集合，且合数无法穷尽所有整数，必然不断产生新的素数。欧几里得通过构造性反证法，严格证明了素数有无穷多个。

定理 9.7：素数的无限性定理

素数的个数有无穷多个，即不存在最大的素数，全体素数构成无限集合。

证：采用反证法。

假设素数仅有有限个，记全体素数为 $p_1,p_2,\ldots,p_n$。构造整数 $Q=p_1p_2\ldots p_n+1$，对任意 $1\le i\le n$，有 $p_i \mid p_1,p_2,\ldots,p_n$，故 $p_i \nmid Q$，余数恒为 1。

由算术基本定理，大于 1 的正整数必存在素因子：要么 Q 为素数，是集合 $\{p_1,p_2,\ldots,p_n\}$ 之外的新素数；要么 Q 为合数，其素因子必不包含在已知有限素数之中。两种情形均与素数有限的假设矛盾。因此假设不成立，故素数有无穷多个。

3）梅森数与梅森素数

为了解决任意大素数的判定效率低下的问题，人们借助代数构造形式，将无规律的随机大整数的素性检验问题转化为具备固定结构、有专属数论性质的定向判别。梅森数与梅森素数依托特殊指数表达式的内在规律，从代数构造维度简化了大素数的判定。

定义 9.5：梅森数与梅森素数

设 p 为素数，称形如 $M_p=2^p-1$ 的正整数为梅森数；若该梅森数自身也是素数，则称其为梅森素数。

梅森数与梅森素数的性质：

（1）形如 $M_n=2^n-1$ 的正整数称为梅森数（广义梅森数），梅森素数是自身为素数的梅森数，属于特殊类型的素数。

（2）若 $M_p=2^p-1$ 为梅森素数，则指数 p 必然是素数，该条件为梅森素数成立的必要条件。

（3）若指数 n 为合数，则对应的梅森数 M_n 一定是合数。例如，$M_6=2^6-1=63=7\times9$。

（4）素数指数仅为必要条件，而非充分条件；素数指数对应的梅森数仍可能是合数。例如：$M_{11}=2^{11}-1=2047=23\times89$。

（5）梅森素数数量稀少、分布稀疏，目前已知的超大素数大多数是梅森素数。截至目前，人类已陆续发现众多梅森素数，其中不乏位数极大的巨型素数。

互联网梅森素数大搜索项目（GIMPS）：

GIMPS 官网（www.mersenne.org）会发布最新发现的梅森素数及其发现过程。

2024 年 10 月 12 日发现的第 52 个梅森素数为 $2^{136279841}-1$，是当前最大的素数。

利用代数构造形式可以简化大素数的素性判定难题。除指数型构造（梅森素数 2^p-1、费马素数$2^{2^n}+1$）外，还有依托阶乘、素数乘积的运算组合构造，如 $n!\pm1$ 是借助整除性质定向筛选特殊素数；以回文、数位轮换为特征的数位形态构造形式，通过固定数字排布规律，精简筛选条件，降低素性判定的计算复杂度。

4）素数定理

定义 9.6：素数计数函数、素数分布

设 x 为正实数，素数计数函数 $\pi(x)$ 定义为不大于 x 的所有素数的个数；

依托函数 $\pi(x)$的增长性、疏密变化与取值规律，刻画素数在正整数集合中的整体排布与稀疏特征，统称为素数分布。

素数的分布研究关注素数在自然数中出现的规律性和分布模式，素数定理提供了一个关于素数分布频率的近似描述。例如， $\pi(0)=\pi(1)=0$, $\pi(2)=1$, $\pi(3)=\pi(4)=2$, $\pi(5)=\pi(6)=3$，$\pi(7)=\pi(8)=\pi(9)=\pi(10)=4$，即 (2、3、5、7)。

定理 9.8：素数定理

当 x 趋向于无穷大时，小于或等于 x 的素数的数量 $\pi(x)$ 与$\frac{x}{ln(x)}$的比率趋近于 1，数学上记作：$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{ln(x)}}=1$ ，该结论也可等价表述为：$\pi(x)$与$\frac{x}{ln(x)}$ 渐进等价，记作：$\pi(x)\sim\frac{x}{\ln(x)}(x\to\infty)$。

素数定理告诉我们在 1 到 x 之间大约有$\frac{x}{\ln(x)}$ 个素数。

定理 9.9：合数的因数属性

若 a 为合数，则 a 必有小于或等于$\sqrt{a}$ 的真因数。

证明：

（1）因 a 是合数，由合数定义，存在正整数 b，c，满足 $a=b\cdot c$,$1<b<a$,$1<c<a$ ；

（2）反证假设：设 a 没有小于等于 a 的真因数，则必有 $b>\sqrt{a}$,$c>\sqrt{a}$

两边相乘：$b\cdot c>\sqrt{a}\cdot\sqrt{a}=a$，推出：$b\cdot c>a$，与 $b\cdot c=a$ 矛盾。

故假设不成立，合数 a 至少有一个真因数 $\leq\sqrt{a}$。证毕。

推论 9.2：合数的素因子推论

若正整数 a 为合数，则 a 必存在小于或等于$\sqrt{a}$的素因子。

证明：

因为 a 是合数，由定理 9.9 可知，a 必有不大于 a 的真因数 d。

若 d 为素数，则 d 即为所求素因子；

若 d 为合数，则 d 自身含有素因子 p，满足 $p\leq d\leq\sqrt{a}$，因此 p 是 a 的素因子且 p≤a。

综上，合数 a 一定存在不大于 a 的素因子。

证毕。

定理 **9.9** 指出，任意合数必存在不超过其算术平方根的真因数，该真因数既可以是素数，也可以是合数，结论宽泛、证明简洁，侧重刻画合数因数的基础结构特征，是数论初等性质的基础铺垫。推论 9.2 作为该定理的强化结论，进一步限定合数必然存在不超过其算术平方根的素因子，剔除了合数因数的情形。推论收缩判定范围，为整数素性检验、试除法判定素数以及素数筛选算法提供严谨理论依据，兼具理论深化与实际应用价值。

例如。对于合数 a=36，依据合数的因数属性定理， 合数 $4\leq\sqrt{a}$是其真因数；依据推论，a 必存在不大于 6 的素因子，例如素数 2,3。推论限定该因数为素数，结论更强。

5）素数测试算法

素数测试算法可以分为确定性测试和概率性测试两大类。确定性测试算法能准确判定一个数是素数还是合数（如试除法），但对大数运算效率较低。概率性测试算法通过随机选取测试基进行运算，以极高的概率判定素性（非绝对准确）。概率性测试算法运算速度快，适用于大数素性初步筛查。两类方法共同构成素数测试的完整体系，且均以 “合数存在$\leq\sqrt{a}$ 的素因子” 为核心理论基础。

（1）试除法：对给定的数 a 除以所有小于或等于$\sqrt{a}$的正整数。如果 a 在这个范围内没有因子（不能整除），则它是素数；否则，它是合数。

（2）埃拉托斯特尼筛法：要筛选出小于或等于 n 的所有素数，只需从 2 开始，考虑那些小于或等于$\sqrt{a}$的数作为可能的素数候选，然后筛选掉这些数的倍数，剩下的数即为素数。

试除法和埃拉托斯特尼筛法是最为基础常用的确定性素数相关算法。确定性算法还有威尔逊判别法、确定性米勒 - 拉宾、卢卡斯 - 莱默检验、AKS 算法；主流的概率性算法有费马测试、（随机基底）米勒 - 拉宾、Solovay–Strassen、Baillie-PSW 算法等。

9.2 最大公因数与最小公倍数

整数之间的关联往往通过整除关系体现，最大公因数与最小公倍数是刻画两个正整数内在联系的核心概念。无论是整数化简、分数运算，还是同余问题和不定方程的求解，都离不开二者的支撑。

9.2.1 公因数与公倍数

数与数之间的整除关系衍生出的最大公因数与最小公倍数从收缩约简和扩张倍增两个相反维度揭示整数的内在关联性，是为数论推理、代数运算、工程周期设计与统筹规划问题的基础工具。

1）公因数（公因子）与公倍数

公因子与公倍数是刻画整数整除结构、反映整数内在关联的基础概念，深刻揭示了整数之间相容与制约的数量本质。能同时整除若干整数的数为公因数，体现整数间公共的约数特征；能同时为若干整数倍数的数为公倍数，反映整数共有的倍数规律。

定义 9.7：公因数与公倍数

设 a,b 为整数，且 a,b 不全为零。若整数 d 满足 $d \mid a$ 且 $d \mid b$，则称 d 是 a 与 b 的公因数；若整数 m 满足 $a \mid m$ 且 $b \mid m$，则称 m 是 a 与 b 的公倍数。

2）最大公因数与公倍数

定义 9.8： 最大公约数

设 a,b 为不全为 0 的整数，能同时满足 $d \mid a$ 和 $d \mid b$ 的最大正整数 d，称为最大公约数 $\gcd(a,b)$。

定义 9.9： 最小公倍数

设整数 a,b 均不为 0，满足 $a \mid m$ 和 $b \mid m$ 的最小正整数 m，称为 a 与 b 的最小公倍数，记作 $\mathrm{lcm}(a,b)$。

例如， $\gcd(12,18)=6$, $\gcd(-12,18)=2\times3=6$ ，$\mathrm{lcm}(12,18)=36$，$\mathrm{lcm}(-12,18)=2^2\times3^2=36$。

最大公因数与最小公倍数的特殊元性质：

对任意正整数 a 有：

（1）零元性质：$\gcd(0,a)=a$，即任意正整数 a 与 0 的最大公因数为该正整数本身；

（2）单位元互素性质：$\gcd(1,a)=1$，即 1 与任意正整数 a 互素；

（3）单位元倍数性质：$\mathrm{lcm}(1,a)=a$，即 1 与任意正整数 a 的最小公倍数为该正整数本身。

最大公因数与最小公倍数的对偶本质：

最大公因数表征整数的公共约数上限，最小公倍数表征整数的公共倍数下限，二者互为对偶。对任意正整数 a,b，满足恒等式 $ab=\gcd(a,b)\cdot\mathrm{lcm}(a,b)$，最大公因数与最小公倍数相互制约、反向变化，可相互推导换算。

定理 9.10：最大公因数的极大性与最小公倍数的极小性

（1）设 a,b 为正整数，若整数 m 满足 $a \mid m, b \mid m$，则 $\text{lcm}(a,b) \mid m$；

（2）设 a,b 为不全为 0 的整数，若整数 d 满足 $d \mid a, d \mid b$，则 $d \mid \gcd(a,b)$。

证明：

（1）因 $a|m$ 和 $b|m$，故 m 是 a,b 的公倍数。又 $\text{lcm}(a,b)$ 为 a,b 的最小公倍数，因此 $\text{lcm}(a,b) \mid m$。

（2）由 $d \mid a, d \mid b$，可知 d 是 a,b 的公因数。而 $\gcd(a,b)$ 是 a,b 的最大公因数，由最大公因数的定义，一切公因数都整除最大公因数，故 $d \mid \gcd(a,b)$。

9.2.2 gcd 与 lcm 求解方法与贝祖定理

求解最大公因数与最小公倍数有多种经典方法，素因数分解法与欧几里得辗转相除法是最常用的两类手段。在此基础上，贝祖定理进一步揭示了最大公因数的本质，建立起最大公因数与整数线性组合之间的内在联系。

1）素因数分解法求解 gcd 与 lcm

素因数分解法利用算术基本定理，将正整数唯一分解为素数幂乘积的形式，通过比对两数的素因子组成，公共素因子取最低次幂相乘求最大公因数，全体素因子取最高次幂相乘求最小公倍数。

算法 9.2： 素因子分解算法

（1）将正整数 a,b 分别进行素因子分解，统一选取相同的素数序列 $p_1,p_2,\ldots,p_n$，表示为：$a = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_n^{e_n}$， $b = p_1^{f_1} \cdot p_2^{f_2} \cdot \cdots \cdot p_n^{f_n}$，对缺失的素因子，指数记为 0。

（2）构造最大公因数：对每一个素因子的指数取最小值，依次作幂运算后相乘：$gcd(a,b) = p_1^{min(e_1,f_1)} \cdot p_2^{min(e_2,f_2)} \cdot \ldots \cdot p_n^{min(e_n,f_n)}$。

（3）构造最小公倍数：对每一个素因子的指数取最大值，依次作幂运算后相乘：$lcm(a,b) = p_1^{max(e_1,f_1)} \cdot p_2^{max(e_2,f_2)} \cdot \ldots \cdot p_n^{max(e_n,f_n)}$。

素因子分解算法依托整数唯一分解性，适合中小整数计算。劣势是大整数分解运算成本较高。

例 9.3：求 45，75，90 的最大公约数和最小公倍数。

解：

（1）素因子分解：$45=3^2\times5^1$，$75=3^1\times5^2$，$90=2^1\times3^2\times5^1$

（2）对每一个素因子的指数取最小值，依次作幂运算后相乘，得到最大公约数 $\gcd(45,75,90)=3^{\min(2,1,2)}\times5^{\min(1,2,1)}=3^1\times5^1=15$。

（3）对每一个素因子的指数取最大值，依次作幂运算后相乘，得到求最小公倍数 $\text{lcm}(45,75,90)=2^{\max(0,0,1)}\times3^{\max(2,1,2)}\times5^{\max(1,2,1)}=2^1\times3^2\times5^2=450$。

除了素因数分解法，还有枚举法、欧几里得辗转相除法，以及操作直观的短除法，各类方法各有适用场景，可结合数值大小灵活选用。

2）辗转相除法（欧几里得算法）

定理 9.11：辗转相除定理

对任意整数 $a,b(b\neq0)$，设 $a=qb+r$，则必有 $\gcd(a,b)=\gcd(b,r)$，即 a,b 的最大公因数等于除数 b 与余数 r 的最大公因数。

证明：

设 $d \mid b$，$d \mid r$，

由整除的线性运算性质：若一个整数能分别整除两个整数，则必整除二者的整数线性组合，根据 $a=qb+r$，因此 $d \mid a$。

反之，设 $d \mid a$，$d \mid b$，同理依据整除的线性运算封闭性，由 $r=a-qb$，可得 $d \mid r$。

综上，能同时整除 a,b 的整数与能同时整除 b,r 的整数完全一致，即 a,b 与 b,r 具有完全相同的全体公因数，因而二者的最大公因数必然相等，即 $\gcd(a,b)=\gcd(b,r)$。证毕。

算法 9.3：欧几里得算法

算法功能：求解两个正整数的最大公因数

（1）输入两个非负整数 a 和 b，若 $a<b$ 则交换两数，保证 $a>b$ 且 $b\neq 0$；

（2）依据带余除法，求得整数 q,r，使得 $a=bq+r$ ，满足 $0\leq r<b$；

（3）令 $a\leftarrow b$, $b\leftarrow r$ ；

（4）循环步骤（2）和步骤（3）,直到余数 $r=0$；

（5）当余数 $r=0$ 时, 当前非零数 b 即为 gcd(a,b)。

例 9.4：求 414 与 662 的最大公约数。

解：由辗转相除定理和欧几里得算法求 gcd(662,414)。

（1）$662=414\times 1+248 \Rightarrow \gcd(662,414)=\gcd(414,248)$；

（2）$414=248\times 1+166 \Rightarrow \gcd(414,248)=\gcd(248,166)$；

（3）$248=166\times 1+82 \Rightarrow \gcd(248,166)=\gcd(166,82)$；

（4）$166=82\times 2+2 \Rightarrow \gcd(166,82)=\gcd(82,2)$

（5）$82=2\times 41+0$

余数为 0，停止运算，最后的非零除数为 2， $\gcd(662,414)=2$。

3）贝祖定理与 gcd 的线性表示

定理 9.12：贝祖定理

设 a 和 b 不全为 0, 则存在整数 x 和 y 使得 $\gcd(a,b)=xa+yb$。

证明：用辗转回代法构造贝祖系数

记 $r_0=a$, $r_1=b$，对两数连续做带余除法（欧几里得辗转相除）：

$r_0=q_1r_1+r_2$, $0<r_2<r_1$

$r_1=q_2r_2+r_3$, $0<r_3<r_2$

⋮

$r_i=q_{i+1}r_{i+1}+r_{i+2}$

⋮

$r_k=q_{k-1}r_{k-1}+r_k$

$r_{k-1}=q_kr_k+0$

由辗转相除定理：$\gcd(a,b)=\gcd(r_0,r_1)=\gcd(r_1,r_2)=\cdots=r_k$

即 $\gcd(a,b)=r_k$。

将各式变形，把余数表示为前两项的线性组合：$r_{i+2}=r_i-q_{i+1}r_{i+1}$

从最后一个非零余数开始，由后向前逐次回代：r_k 可表为 rk−2,r_{k-1} 的整数线性组合；

不断用上层式子替换中间余数，依次消去 $r_{k-1},r_{k-2},\ldots,r_2$；

最终仅保留 $r_0=a$,r_1=b，整理得：$r_k=xa+yb$ 其中 x,y 为整数。

因此 gcd(a,b)=xa+yb

证毕。

贝祖定理（贝祖等式）不仅证明了任何两个整数的最大公约数总是存在的，而且还提供了一种计算最大公约数的具体方法。

例 9.5：计算 gcd(119,544)，并通过逆向替代过程找到满足方程 119x+544y=gcd(119,544) 的 x 和 y 的值。

解：

（1）辗转相除法求得 gcd(119,544)=17

544=4×119+68 （a）

119=1×68+51 （b）

68=1×51+17 （c）

51=3×17+0

求得 gcd(119,544)=17

（2）采用逆向回代（贝祖等式）

由式（c）有 17=68−1×51，由式（b）有 51=119−1×68，代入：

17=68−1(119−1×68) = −1×119+2×68

由式 （a）有 68=544−4×119，代入：

17 = −1×119+2(544 − 4×119) = −1×119+2×544 − 8×119= −9×119+2×544

（3）结果：119×(−9) + 544 ×2= 17gcd(119,544) = 17, x = −9， y=2 。

9.2.3 互素的定义、等价条件与整除性质

两个整数互素，本质是彼此除了最大公因数为 1 外，再没有公共素因子约束，是整数之间相互独立、约束最弱的整除关系。互素的等价特征与整除性质是同余方程求解、严谨数论推导的核心基础工具。

1）互素与两两互素的定义

定义 9.10：两整数互素（互质）

设 a,b 为不全为 0 的整数，若 gcd(a,b)=1 则称整数 a 与 b 互素。

2）互素的充要条件

定理 9.13：互素充要条件定理（贝祖定理推论）

整数 a,b 互素的充分必要条件是：存在整数 x,y，使得 ax+by=1。

证明：

（1）必要性证明

若整数 a,b 互素，则 gcd(a,b)=1。

由贝祖定理：对任意整数 a,b，存在整数 x,y 满足 ax+by=gcd(a,b)，代入 gcd(a,b)=1，即得 ax+by=1。

（2）充分性证明

假设存在整数 x,y，使得 ax+by=1。设 d 为 a,b 的任一正公约数，则 d | a, d | b。

因此 d 整除 a,b 的任意整数线性组合（线性组合整除性质），即：d | (ax+by)，代入已知等式 ax+by=1 ，得到 d | 1；

正整数中唯一整除 1 的数只有 d=1，故 gcd(a,b)=1，由互素定义，a,b 互素。

3）互素整除性定理（互素消去律）

定理 9.14：互素因子整除定理

设 a,b,c 为整数，若 $a \mid c$，$b \mid c$，且 gcd(a,b)=1，即整数 a 与 b 互素，则必有 $ab \mid c$。

证明：

（1）根据互素的充要条件（贝祖定理互素形式），存在整数 x,y，使得 $xa+yb=1$

（2）等式两边同乘整数 c，得：$acx+bcy=c$，由 $b \mid c$，结合 $a \mid a$，可得 $ab \mid acx$。

（3）由 $a \mid c$，结合 $b \mid b$，可得 $ab \mid bcy$。依据线性组合整除引理：若一个整数同时整除两个整数，则必整除二者之和。因此 $ab \mid (acx+bcy)$，即 $ab \mid c$。证毕。

互素的定义以是否存在最大公因子基础，定义什么是互素； 互素的充要条件从线性组合、素因子结构、同余模运算三个不同维度，给出互素的等价判定标准，回答如何判定互素；互素整除性定理从运算规则出发，依托互素前提推导整除结论，回答互素有什么用、能推出什么结论。

gcd(a,b)=1 仅说明整数 a 与 b 互素，即二者不存在大于 1 的公因数，并不要求 a,b 自身为素数；其等价于存在整数 x，使得 $ax \equiv 1 \pmod{b}$，即乘积 ax 除以模数 b 的余数为 1，$ax-1$ 能够被 b 整除；反之，若 gcd(a,b)≠1，则不存在整数 x 满足 $ax \equiv 1 \pmod{b}$。

9.3 同余

同余从整数除以同一正整数所得余数的角度，对全体无限整数进行等价类划分，以有限剩余类简化对无限整数的研究。借助模运算体系，可在剩余类中完成超大整数的运算，是现代公钥密码、对称加密、哈希函数、数字签名等密码技术的底层数学基础。

9.3.1 模 m 同余的定义

在整数带余除法的基础上，以固定正整数 m 为划分依据，围绕整数除法的余数特征，引入模 m 的同余概念。同余是整除关系的推广与形式化表达，通过简洁的符号刻画余数相同的整数间的等价关联。

定义 9.11：模 m 同余

设 m 为正整数，a,b 为整数。

若 $m \mid (a-b)$，则称 a 与 b 模 m 同余，记作 $a \equiv b \pmod{m}$；

若 $m \nmid (a-b)$，则称 a 与 b 模 m 不同余，记作 $a \not\equiv b \pmod{m}$。

当 $m \mid (a-b)$命题为真时，$a \equiv b \pmod{m}$也为真；当 $m \nmid (a-b)$命题为真时，$a \not\equiv b \pmod{m}$也为真。

定理 9.15：同余等价刻画定理

设 m 为正整数，a,b 为整数，则以下两个条件互相等价，且都与 $a \equiv b \pmod{m}$ 等价：

（1）$a \bmod m = b \bmod m$；

（2）a 与 b 模 m 同余的条件是 $a-b$ 是 m 的倍数，即 $a=b+km$, k 是整数。

同余等价刻画定理从两个不同视角给出整数 a,b 模 m 同余的充要条件。（1）说明 a,b 模 m 同余就是两个数除以 m 所得最小非负余数相等；（2）说明 a,b 模 m 同余，等价于 a,b 之间相差模数 m 的某个整数倍。

例 9.6：设模数 m=19，整数 a=327，b=137，通过同余定义、余数等价、线性表示三等价充要条件验证 a 与 b 模 19 是否同余。

解：

（1）用同余原始定义验证

327−137=190，19｜190 满足同余定义，故 327≡137(mod 19)。

（2）用余数相等充要条件验证

327 mod 19=4，137 mod 19=4，两数模 19 的最小非负余数相等，因此 a,b 模 19 同余。

（3）用线性表示充要条件验证

若存在整数 k=19/190=10，使的 327=137+19×10，故 a,b 模 19 同余。

9.3.2 同余关系的基本性质

同余的等价关系、运算封闭、约数缩放和推理规则 4 类性质，将模 m 同余类比成普通等式，建立一套完整、可运算、可推理、可化简的规则体系，既能像等式一样做加减、乘、数乘、乘方运算，又能实现换位、传递、分类、缩模、扩模、消去、同余与整除互化，实现简化大数计算、求解同余方程、划分同余等价类和数论推导与证明。

1）等价关系类性质：自反、对称、传递

设 m 为正整数，则整数集上模 m 的同余关系是等价关系，满足自反性、对称性、传递性三条基本性质：

（1）自反性：对任意整数 a，有 $a\equiv a(\mathrm{mod}\ m)$

（2）对称性：对任意整数 a,b，若 $a\equiv b(\mathrm{mod}\ m)$，则必有 $b\equiv a(\mathrm{mod}\ m)$

（3）传递性：对任意整数 a,b,c，若 $a\equiv b(\mathrm{mod}\ m)$, $b\equiv c(\mathrm{mod}\ m)$，则可推出 $a\equiv c(\mathrm{mod}\ m)$。若多个整数两两模 m 同余，可记作：$a_1\equiv a_2\equiv\cdots\equiv a_k(\mathrm{mod}\ m)$ 。

2）运算封闭性质

加减、乘法、幂运算性质：

设 m 为正整数，若 $a\equiv b(\mathrm{mod}\ m)$, $c\equiv d(\mathrm{mod}\ m)$则满足：

（1）加减保持性：$a\pm c\equiv b\pm d(\mathrm{mod}\ m)$

（2）乘法保持性：$ac\equiv bd(\mathrm{mod}\ m)$

（3）乘方保持性：$a^k\equiv b^k(\mathrm{mod}\ m)$，其中 k 为非负整数。

同余数乘性质（常数倍性质）：

设 m 为正整数，a,b 为整数，若 $a\equiv b(\mathrm{mod}\ m)$, 对任意整数 k，**有** $ka\equiv kb(\mathrm{mod}\ m)$ 。

反向性质：若 $a\equiv b(\mathrm{mod}\ m)$，则 $-a\equiv -b(\mathrm{mod}\ m)$。

3）约数缩放性质：模数分解、模数缩放

（1）同余的整除分解性质（模数分解）

设 m 为正整数，a,b 为整数。若 $a\equiv b(\mathrm{mod}\ m)$，且正整数 d 满足 d｜m，则必有 a≡b(mod d)。

（2） 同余的模数缩放性质

若 $a\equiv b(\mathrm{mod}\ m)$，对任意正整数 k，有：$ka\equiv kb(\mathrm{mod}\ km)$。

4）推理规则：互素消去律、同余与整除互推

（1）同余的约分性质（互素消去律）

若 $ac\equiv bc(\bmod m)$，且 $\gcd(c,m)=1$（c 与模数 m 互素），则可消去 c：$a\equiv b(\bmod m)$。

（2）同余与整除等价性质

$a\equiv b(\bmod m)\Leftrightarrow m\mid(a-b)$是同余原始定义，也是所有性质推导的根基。

（3）同余的乘法逆元性质：

设 m 为正整数，若整数 c 与 m 互质，则 $a\equiv b(\bmod m)\Leftrightarrow ca\equiv cb(\bmod m)$，即：互素系数 c 作用于同余式两边时，同余关系双向等价，既可同乘也可消去。

9.3.3 模 m 剩余类与商集

同余作为整数集上的等价关系，天然具备分类功能。依据余数差异可将全体整数划分为有限个同余剩余类，以此构建模 m 商集，从集合结构层面完成整数的模块化划分，是研究剩余系、同余方程及进阶数论内容的理论支撑。

1）模 m 剩余类$[a]_m$及其商集 $\mathbb{Z}_m$

模 m 剩余类、同余剩余类、模 m 等价类是指同一个对象：都是按模 m 同余关系归为同一类的整数子集。模 m 剩余类、同余剩余类侧重于数论角度，依据整数除以 m 的余数相同进行分类；模 m 等价类从等价关系的角度，强调它是由模 m 同余等价关系划分出来的类。

模 m 等价类的集合、模 m 商集、整数集 $\mathbb{Z}$ 按模 m 同余关系的划分，都是指由全部互不相同的模 m 等价类组成的集合；其中 “模 m 等价类的集合” 是通俗表述，“模 m 商集” 是代数与集合论的标准名称，“整数集 $\mathbb{Z}$ 模 m 同余关系划分” 则是从集合划分角度的专业表述。

定义 9.12：模 m 剩余类与模 m 商集

设 m 为正整数，在整数集 $\mathbb{Z}$ 上定义模 m 同余关系：

所有与整数 a 模 m 同余的整数构成的子集 $[a]_m=\{x\in\mathbb{Z}\mid x\equiv a(\bmod m)$，则称 $[a]_m$ 为模 m 剩余类；

由全体互不相同的模 m 剩余类所构成的集合 $\mathbb{Z}_m=\{[0]_m,[1]_m,[2]_m,\dots,[m-1]_m\}$，称为模 m 商集，它也是整数集 $\mathbb{Z}$ 被模 m 同余关系诱导的集合划分。

例 9.7：求整数集 $\mathbb{Z}$ 上模 5 同余关系导出的所有等价类及整数集 $\mathbb{Z}$ 的划分。

解：

模 5 同余是 $\mathbb{Z}$ 上的等价关系，即有$\forall x,y\in\mathbb{Z}, x\equiv y(\bmod 5)\Leftrightarrow 5\mid(x-y)$成立。

按等价类将 $\mathbb{Z}$ 划分为 5 个两两不交的等价类：模 m 等价类的集合

$[0]_5=\{x\in\mathbb{Z}\mid x\equiv 0\ (\bmod 5)\}$,

$[1]_5=\{x\in\mathbb{Z}\mid x\equiv 1\ (\bmod 5)\}$,

$[2]_5=\{x\in\mathbb{Z}\mid x\equiv 2\ (\bmod 5)\}$,

$[3]_5=\{x\in\mathbb{Z}\mid x\equiv 3\ (\bmod 5)\}$,

$[4]_5=\{x\in\mathbb{Z}\mid x\equiv 4\ (\bmod 5)$。

将 5 个两两不交的等价类并为模 5 等价类的集合：$\mathbb{Z}_5=\{[0]_5,[2]_5,[2]_5,[3]_5,[4]_5\}$。$\mathbb{Z}_5$ 就是整数集 $\mathbb{Z}$ 由模 5 同余关系所确定的划分，既实现了整数的规范化分类，又将整数运算简化为有限剩余类的运算。

模 m 等价类集合 $\mathbb{Z}_m$ 可将整数集上运算的无限性（定义域无限、元素无穷多）简化为 m 个元素构成的有限集合 $\mathbb{Z}_m$ 上，把无穷整数集上的运算与性质研究，转化为模 m 剩余类有限集合上的运算与规律分析，并可广泛用于同余求解、周期推算、计算机模运算、密码学、离散代数系统等场景。

2）模 m 商集上的代数运算

模 m 商集 $\mathbb{Z}_m=\{[0]_m, [1]_m, [2]_m, \dots, [m-1]_m\}$上定义四种基本代数运算：

（1）剩余类加法：$[a]_m+[b]_m=[a+b]_m$

（2）剩余类减法：$[a]_m - [b]_m=[a-b]_m$

（3）剩余类乘法：$[a]_m \cdot [b]_m=[a \cdot b]_m$

（4）剩余类幂运算：$[a]_m^k = [a^k]_m$，$k\in\mathbb{N}^+$

例 9.8：举例说明 $\mathbb{Z}_5$ 上的加、减、乘、幂运算。

解：$\mathbb{Z}_5=\{[0]_5, [2]_5 ,[2]_5 ,[3]_5 ,[4]_5 \}$

加法：$[2]_5 + [3]_5 =[2+3]_5=[5]_5=[0]_5$

减法：$[1]_5-[4]_5=[1-4]_5=[-3]_5=[2]_5$

乘法：$[3]_5 \cdot [4]_5=[12]_5=[2]_5$

幂运算：$[2]_5^3 = [2^3]_5 = [8]_5 = [3]_5$

四种运算统一规则：先对代表元做整数运算，结果再对模 5 取余，运算结果仍在 $\mathbb{Z}_5$ 中，满足封闭性。

定理 9.16：模 m 商集剩余类幂周期定理

设 $\mathbb{Z}_m$ 为整数模 m 商集，$[a]_m\in\mathbb{Z}_m$ 为任意一个剩余类，则剩余类的幂序列$[a]_m^1$, $[a]_m^2$, $[a]_m^3$, … 必呈现周期性重复；且存在最小的正整数 T，使得对任意正整数 k，都有$[a]_m^{k+T} = [a]_m^k$ ，称该最小正整数 T 为剩余类$[a]_m$的幂周期。

例如，对于模 10 商集 $\mathbb{Z}_{10}$，取剩余类 $[3]_{10}$，依次计算各次幂：

$[3]_{10}^1 = [3]_{10}$，$[3]_{10}^2 = [9]_{10}$，$[3]_{10}^3 = [7]_{10}$，$[3]_{10}^4 = [1]_{10}$，$[3]_{10}^5 = [3]_{10}$

第 5 次幂回到初始剩余类 $[3]_{10}$，所以剩余类 $[3]_{10}$ 的最小幂周期 T=4。

例 9.9：以 3^{455} 为例，利用模 m 商集的剩余类幂运算，求解该整数高次幂在 k（k=10,8,2）进制下的末位数字。

解：k 进制末位数字等价于对模数 m=k 取余；模 m 商集剩余类幂运算规则：$[a]_m^n = [a^n]_m$ 。

（1）当 k=10（十进制），取模数 m=10，有剩余类幂运算规则： $[3]_{10}^{455} = [3^{455}]_{10}$。

由于直接计算 3^{455} 数值过大、运算困难，可利用模 10 下底数 3 的剩余类幂周期，对大指数进行周期化简，再求十进制个位（模 10 余数）。

依次计算底数 3 在模 10 下的各次剩余类：

由 $3^1\equiv3 \pmod{10}$，$3^2\equiv9 \pmod{10}$，$3^3\equiv7 \pmod{10}$，$3^4\equiv1 \pmod{10}$，$3^5\equiv3 \pmod{10}$。可见底数为 3 时，模 10 的剩余类幂周期 T=4。

根据幂周期 T=4，将指数 455 对周期 4 取余： $455 \bmod 4=3$。

在模 10 意义下：$[3^{455}]_{10} = [3^3]_{10}$

只需计算 3^3 模 10 的余数，即可得到 3^{455} 的十进制个位。

$3^3 \bmod 4 =7$，因此 3^{455} 的十进制个位数是 7。

（2）当 k=8（八进制），取模数 m=8，$[3]_8^{455} = [3^{455}]_8$

计算模 8 幂序列：$3^1 \equiv 3 \pmod 8$, $3^2 \equiv 1 \pmod 8$，$3^3 \equiv 3 \pmod 8$，得幂周期 T=2。

455 mod 2=1，于是 $[3^{455}]_8=[3^1]_8$，$3^1 \bmod 8=3$。故 3^{455} 的八进制末位为 3。

（3）当 k=2（二进制），取模数 m=2，$[3]_2^{455} = [3^{455}]_2$

计算模 2 幂序列：$3^1 \equiv 1 \pmod 2$, $3^2 \equiv 1 \pmod 2$, $3^3 \equiv 1 \pmod 2$，得幂周期 T=1。

直接得 $3^{455} \equiv 1 \pmod 2$。故 3^{455} 的二进制末位为 1。

3）中国古典模 *m* 商集运算实例

中国古代自发运用模 m 商集思想，将无限数值推演转化为有限集合上的代数运算，比西方建立系统同余与商集理论早千年以上。

古典实例	核心代数运算	对应现代结构
孙子算经・物不知数	剩余类加法、同余归约	$\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{105}$
秦九韶大衍求一术	剩余类加、乘法、求逆元	模 m 商集 $\mathbb{Z}_m$ 的加、乘、逆元
干支六十甲子纪历	周期循环加法、取模	$\mathbb{Z}_{10}$, $\mathbb{Z}_{12}$, $\mathbb{Z}_{60}$ 循环群
周易揲蓍起卦	模 4 取余、剩余类归类	$\mathbb{Z}_4$ 模商集取余

这些古籍与历法实践，把无穷的数值、年份、天数推算，化归为有限模商集上的代数运算，暗含 “化无限为有限” 的现代代数核心思想，是中国古典数学领先世界的重要成就。

9.4 线性同余方程与中国剩余定理

9.4.1 线性同余方程及有解条件

1）线性同余方程

线性同余方程 $ax \equiv b \pmod m$突破普通整数方程的局限，用模同余关系刻画整数间余数约束规律，可解决整数余数求解、大数化简、周期推算、密码学模运算等实际问题。

定义 9.13：线性同余方程及其解

设 a,b,m 为整数且 $m>0$，形如 $ax \equiv b \pmod m$的同余式称为线性同余方程（一次同余方程）；

若整数 x_0 满足 $ax_0 \equiv b \pmod m$，则称 x_0 为该线性同余方程的一个解。在模 m 下，彼此同余的整数视为同一个解。

线性同余方程 $ax \equiv b \pmod m$ 含单个一次未知整数 x，具备线性结构特征。它依托模 m 同余关系建立等量约束，不在孤立整数中求解，而是在模 m 剩余类范畴内讨论等价解，方程有解的核心判定依据是系数 a 与模数 m 的最大公因子能够整除常数项 b，即 gcd(a,m)｜b。

例如， $3x \equiv 4 \pmod 7$的解为 $x \equiv 6 \pmod 7$，如 6,13,20,−1 等； $2x \equiv 1 \pmod 4$无解。

2）线性同余方程有解充要条件及解的数量

定理 9.17：线性同余方程有解充要条件定理（含解的数量）

设 a,b 为整数，m 为正整数，线性同余方程 $ax \equiv b \pmod m$ 有解的充分必要条件是：$\gcd(a,m) \mid b$（即 a 与 m 的最大公约数能整除 b）。

若方程有解，则模 m 意义下共有 $\gcd(a,m)$ 个不同的解（解的数量等于 a 与 m 的最大公约数）；若上述条件不满足，则方程无解。

证明：

（1）必要性：由同余定义，若方程 $ax\equiv b(\mathrm{mod}\ m)$有解，则 $m\mid(ax-b)$，即存在整数 k 使得 $ax-km=b$；设 $d=\gcd(a,m)$，$d\mid a, d\mid m$，故 d 整除 a,m 整系数线性组合 $ax-km$，即 $d\mid b$，所以有 $\gcd(a,m)\mid b$ 成立。

（2）充分性：若 $\gcd(a,m)\mid b$，设 $b=d\cdot t$（t 为整数）。由贝祖定理，存在整数 u,v 满足：$au+mv=d$，两边同乘 t 得 $a(ut)+m(vt)=dt=b$；取 $x=ut$，则 $ax-b=-m(vt)$，是 m 的整数倍，故 $ax\equiv b(\mathrm{mod}\ m)$ 有解。

证毕。

例 9.10：求解线性同余方程：$6x\equiv 15(\mathrm{mod}\ 21)$。

（1）判断是否有解：设 $a=6, b=15, m=21$，$d=\gcd(6,21)=3$；有 $3\mid 15$ 成立，故方程有 3 个不同解。

（2）方程约分化简：两边同除以 d=3，$2x\equiv 5(\mathrm{mod}\ 7)$，将原方程模 21 约简为 7。

（3）枚举试根求特解：$\gcd(2,7)=1$，将模 7 的余数 0,1,2,3,4,5,6 逐一代入 $2x\equiv 5(\mathrm{mod}\ 7)$，$x=6$ 时，$2\times 6=12\equiv 5(\mathrm{mod}\ 7)$，求得最简同余特解：$x\equiv 6(\mathrm{mod}\ 7)$。

（4）写出全部模 21 解：以 $x_0=6$ 为特解、步长$\frac{m}{d}=7$，在模 21 意义下，取满足方程的 3 个互不相同的余数（即 3 个不同的解对应的剩余类）：$x\equiv 6, 13, 20(\mathrm{mod}\ 21)$。

最终结果：方程 $6x\equiv 15(\mathrm{mod}\ 21)$有解，模 21 下共 3 个解：$x\equiv 6, 13, 20(\mathrm{mod}\ 21)$。

3）模 *m* 乘法逆元及存在唯一性定理

定义 9.14：模 m 乘法逆元

设 a,m 为整数，且 $m>1$。若存在整数 b，使得 $ab\equiv 1(\mathrm{mod}\ m)$，则称 b 是 a 的模 m 乘法逆元，简称模 m 逆元，记作 $a^{-1}(\mathrm{mod}\ m)$ 或简写为 a^{-1}。

等价表述：$a^{-1}(\mathrm{mod}\ m)$ 就是线性同余方程 $ax\equiv 1(\mathrm{mod}\ m)$的解。

定理 9.18：模 m 乘法逆元的存在唯一性定理

设整数 $m>1$，a 为整数：

(1) 存在性：a 的模 m 乘法逆元存在的充分必要条件是 $\gcd(a,m)=1$（即 a 与 m 互素）；

(2) 唯一性：若 $m>1$ 且 a 与 m 互素，则 a 在模 m 的意义下乘法逆元唯一。

证明：

（1）证明逆元存在的充要条件

充分性：由 gcd(a,m)=1 证明逆元存在

①若 a 与 m 互素，由贝祖定理，存在整数 x,y 使得 $ax+my=1$；

② 变形得 $ax-1=-my$，即 $m\mid(ax-1)$，由同余定义有 $ax\equiv 1(\mathrm{mod}\ m)$，故整数 x 就是 a 的一个模 m 乘法逆元，逆元存在。

必要性：由逆元存在证明 $\gcd(a,m)=1$

①若存在整数 b 为 a 的模 m 逆元，则 $ab\equiv 1(\mathrm{mod}\ m)$，由同余定义，存在整数 k 满足 $ab-1=km$，整理得 $ab-km=1$；

② 设 $d=\gcd(a,m)$，则 $d\mid a, d\mid m$，从而 d 整除整系数线性组合 $ab-km$，即 $d\mid 1$。故只能 $d=1$，即 $\gcd(a,m)=1$。

（2）证明模 m 逆元的唯一性

设 a 与 m 互素，假设 b_1,b_2 都是 a 的模 m 逆元，则 $ab_1\equiv 1(\mathrm{mod}\ m), ab_2\equiv 1(\mathrm{mod}\ m)$

①由同余定义，存在整数 k,l，使得 $ab_1=1+km, ab_2=1+lm$，两式相减得：$a(b_1-b_2)=(k-l)m$；

②上式表明 $m \mid a(b_1-b_2)$，即 $a(b_1-b_2)\equiv 0 \pmod m$；

③ 已知 $\gcd(a,m)=1$，若 $m \mid a(b_1-b_2)$且 a,m 互素，则必有 $m \mid (b_1-b_2)$；

④ 由整除定义得 $b_1 \equiv b_2 \pmod m$。

这说明：同一个数 a 在模 m 下的任意两个逆元，模 m 必相等，即模 m 逆元唯一。

证毕。

4）常见的模 m 乘法逆元求解方法

（1）试错枚举法：依据模 m 乘法逆元的定义，满足同余方程 $ax\equiv 1 \pmod m$的解 x 即为 a 的模 m 逆元。

主要求解步骤：① 先判定逆元存在性：计算 $\gcd(a,m)$，只有满足 $\gcd(a,m)=1$ 时，逆元才存在；② 建立同余方程 $ax\equiv 1 \pmod m$；③ 在模 m 的最小非负剩余范围内，依次取 $x=1,2,\ldots,m-1$，逐一计算 $ax \bmod m$；④ 若存在某个 x 使得 $ax \bmod m=1$，则该 x 就是 a 在模 m 下的乘法逆元 $a^{-1} \pmod m$。

（2）扩展欧几里得法（辗转相除法）：由贝祖定理，对任意整数 a,m，存在整数 x,y 使得 $ax+my=\gcd(a,m)$，当 $\gcd(a,m)=1$ 时，$ax+my=1$，变形即得 $ax\equiv 1 \pmod m$，此时 x 为模逆元。

主要求解步骤：① 用扩展欧几里得算法，求出不定方程 $ax+my=\gcd(a,m)$的一组整数解 x,y；② 若 $\gcd(a,m)=1$，则求得的整数 x 是 a 的一个模 m 乘法逆元；③ 若所得 x 为负数，不断加上整数倍 m，将其归化到模 m 的标准剩余区间 $1\le x\le m-1$，得到规范逆元。

例如，用试错枚举法求 5 在模 11 下的逆元，首先判定 $\gcd(5,11)=1$ 成立，逆元存在；然后枚举验证 x（x 取 1～10），当 x=9 时，$5\times 9=45\equiv 1 \pmod 1$ 1），即 5 在模 11 下的逆元为 9。

乘法逆元是公钥体系中 “私钥与公钥对应关系” 的核心支撑。 在指定模 m 下，公钥和私钥互为对方的乘法逆元，模 m 越复杂、数值越大，加密程度越高，越难被破解。

9.4.2 中国剩余定理

中国剩余定理源自公元 5 世纪的《孙子算经》中的“物不知数”千古名题，在公元 1247 年由秦九韶创 “大衍总数术”完善定理体系。定理以线性同余方程的求解原理为底层支撑，凝练了中国古代数学经典智慧，是求解多元同余方程组的重要理论成果。

1）孙子算经

“物不知数”问题：今有物，不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？

设物品总数为 x，依题意可列出线性同余方程组：

$$x\equiv 2 \pmod 3$$
$$x\equiv 3 \pmod 5$$
$$x\equiv 2 \pmod 7$$

“物不知数”同时给出模 3、模 5、模 7 三组余数约束，提出了在不同模数下同时满足多个同余条件的求解诉求。该特例经过抽象提炼，把两两互质模数下的求解规律一般化，再逐步推广到模数不互质的普遍情形，依托线性同余方程有解判定、模逆元构造等基础理论，系统归纳出同余方程组的通用求解法则，逐步构思并完善出中国剩余定理，也构建了初等数论中求解联立同余方程的核心理论框架。

2）中国剩余定理

（1）秦九韶《数书九章》大衍总数术原文

大衍总数术曰：置诸问数，一曰元数，二曰收数，三曰通数，四曰复数。元数者，先以两两连环求等，约奇弗约偶、复约归一；遍约毕，乃变元数皆曰定母。各立天元一为子，以诸定母互乘左行之子，各得名曰衍数。次以各定母满去衍数，各余名曰奇数。以奇数与定母，用大衍求一术求一，得乘率。以乘率乘衍数，得用数。以余数乘用数，得各总。并各总，得总数，满衍母去之，余即为所求物数。

（2）白话文解释：大衍总数术求解一次同余方程组的完整步骤：

①先整理题目给出的所有模数，分为四类：整数模数、带小数模数、分数模数、整十倍数模数；

②对普通整数模数，两两求取最大公约数，按约奇数不约偶数的规则逐步约化，把原本不互质的模数，化约为一组两两互质的定母；

③把所有定母相乘得到衍母，每个定母与其余定母分别相乘，得到各自的衍数；

④用定母去除衍数，所得余数称为奇数；

⑤用大衍求一术，对奇数和定母辗转推算，求出满足同余条件的乘率（即今模逆元）；

⑥乘率乘以衍数得到用数，再用题目给出的余数乘用数，得到每一项的各总；

⑦将所有各总相加得到总数，不断减去衍母，余下的最小正整数，就是同余方程组的最小正解。

（2）现代数论规范表述

设一次同余方程组：$x\equiv a_1 \pmod{m_1}$，$x\equiv a_2 \pmod{m_2}$，…，$x\equiv a_n \pmod{m_n}$

①记原模数 $m_1,m_2,\ldots,m_n$ 为元数，通过两两求最大公约数等价化约，化为两两互质的定母 $d_1,d_2,\ldots,d_n$；

②记衍母 $M=\prod_{i=1}^{n} d_i$，衍数 $M_i=\frac{M}{d_i}$；

③求乘率 k_i，满足 $M_ik_i\equiv 1 \pmod{d_i}$；

④用数：$N_i=M_ik_i$；

⑤各总：$S_i=a_iN_i$；

⑥方程组解为：$x=\sum_{i=1}^{n} a_iM_ik_i \pmod{M}$

在模 M 下解唯一，全体整数解为 $x=\sum_{i=1}^{n} a_iM_ik_i+tM$，$t\in\mathbb{Z}$。

（4）中国剩余定理

定理 9.19：中国剩余定理经典形式（模数两两互质）

设正整数 $m_1, m_2,\ldots,m_k$ 两两互素, 则一次同余方程组

$$x\equiv a_i \pmod{m_i},\ i=1,2,\ldots,k$$

有整数解, 并且在模 $m=m_1m_2\ldots m_k$ 下解是惟一的, 即任意两个解都是模 m 同余的。

证明：

解的存在性证明：

令 $M_i=\frac{m}{m_i}$，因 $m_1, m_2,\ldots,m_k$ 两两互素，故从 m 中去掉 m_i 得到的 M_i 与 m_i 也互素，即 $\gcd(M_i,m_i)=1$。

由贝祖定理，M_i 与 m_i 互素互素必存在模 m_i 逆元 t_i，使得 $M_it_i\equiv 1 \pmod{m_i}$；

构造解$x_0 = \sum_{i=1}^{k} a_i M_i k_i$，使能满足同余方程组的每一个 m_j 下余数都等于 a_j 的同余条件，即 $x_0 \equiv a_j (\mathrm{mod}\ m_j)$，因为当 $i \neq j$ 时，$m_j \mid M_i$，即 $M_i \equiv 0 (\mathrm{mod}\ m_j)$，$i=j$ 时，$x_0 \equiv a_j M_j t_j \equiv a_j \cdot 1 \equiv a_j (\mathrm{mod}\ m_j)$；

所以 x_0 是方程组的一个整数解，解存在。

解的唯一性证明：

设 x_1, x_2 都是方程组的解，对于所有 i，都能模 m_j 余 a_i，由同余的等价定义，则有 $m_i \mid (x_1 - x_2)$；

因 $m = m_1 m_2 \ldots m_k$ 两两互素，由互素因子整除定理，且每个 $m_i \mid (x_1 - x_2)$，则 m_i 的乘积 m 也满足 $m \mid (x_1 - x_2)$，即存在整数 k：$x_1 - x_2 = km$，由同余定义得 $x_1 \equiv x_2 (\mathrm{mod}\ m)$；

即所有解在模 m 下彼此同余，解模 m 唯一。

例 9.11：求解《孙子算经》“物不知数” 问题。

解：“物不知数”同时给出模 3、模 5、模 7 三组余数约束，提出了在不同模数下同时满足多个同余条件的求解诉求。

（1）建立同余方程组：设所求物数为整数 x，翻译成同余方程组：

$$\begin{cases} x \equiv 2 (\mathrm{mod} 3) \\ x \equiv 3 (\mathrm{mod} 5) \\ x \equiv 2 (\mathrm{mod} 7) \end{cases}$$

（2）取模数：$m_1=3, m_2=5, m_3=7$，三者两两互素，满足中国剩余定理适用条件。总模数 $m = m_1 m_2 m_3 = 3 \times 5 \times 7 = 105$。

（3）计算$M_i = \frac{m}{m_i}$，$M_1=35$，$M_2=21$，$M_3=15$，

（4）求各M_i模 m_i 的逆元t_i，即满足 $M_i t_i \equiv 1 (\mathrm{mod}\ m_i)$

将 $35t_1 \equiv 1 (\mathrm{mod}\ 3)$中的 35 模 3 约简成 2，再找到满足 $2t_1 \equiv 1 (\mathrm{mod}\ 3)$ 的整数 t_1，得逆元 $t_1=2$。

同理将 $21t_2 \equiv 1 (\mathrm{mod}\ 5)$化简成 $t_2 \equiv 1 (\mathrm{mod}\ 3)$，得逆元 $t_2=1$。

将 $15t3 \equiv 1 (\mathrm{mod}\ 7)$，化简得 $t_3 \equiv 1 (\mathrm{mod}\ 7)$，得逆元 $t_3=1$

（5）构造特解 $x_0 = a_1 M_1 t_1 + a_2 M_2 t_2 + a_3 M_3 t_3$

将 $a_1=2$，$a_2=3$，$a_2=2$ 和各 $M_i\ t_i$ 带入

$x_0 = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233$

（6）求通解与最小正整数解

同余方程组通解为 $x = 233\ (\mathrm{mod}\ 105)$

最小正整数解为 $x=23$。

标准中国剩余定理针对模数两两互素的线性同余方程组，判定必有解，且解在模数乘积下唯一，可通过固定公式直接构造通解。广义中国剩余定理放宽限制，允许模数不两两互素，以任意两个同余方程余数对对应模数的最大公约数同余作为有解充要条件，有解时解在全体模数的最小公倍数下唯一，无解则方程组无整数解。

9.4.3 大整数的模表示算术运算

普通大整数运算存储开销大、计算复杂度高。基于中国剩余定理的大整数模表示算术运算，可将一个超大整数分解为若干两两互素模数下的余数，把整体的超大数算术运算，拆解为

多个小模数下的小规模模算术运算，无需存储和处理原始超长整数，大幅降低存储和计算成本。

1）整数的模表示

定义 9.15：整数的模表示

设整数 $m_1,m_2,\ldots,m_k$ 大于 1，且两两互素，记 $m=m_1m_2\ldots m_k$。对任意整数 x 满足 $0\le x<m$，令 $x_i=x \bmod m_i$, $i=1,\ldots,k$，称有序数组$(x_1,x_2,\ldots,x_k)$ 为整数 x 关于模 $m_1,\ldots,m_k$ 的模表示，简称 x 的模表示，记作 $x=(x_1,x_2,\ldots,x_k)$。

整数的模表示是依附于一组两两互素的模数定义的，总模 m 决定了这组模数能承载多大的大整数。例如，取一组两两互素的模数 $m_1=7$, $m_2=11$, $m_3=13$, $m_4=17$\)，总模数 m=7×11×13×17=17017；设大整数 $x=15869243$，分别计算：

$x_1=x \bmod 7=5$, $x_2=x \bmod 11=5$, $x_3=x \bmod 13=0$, $x_4=x \bmod 17=15$，则大整数可用该组模数的模表示为 $x=(5,5,0,15)$。

2）模表示的算术运算（同余运算）

定理 9.20：模表示的算术运算

设整数 x,y 的模表示分别为 $x=(x_1,x_2,\ldots,x_k)$, $y=(y_1,y_2,\ldots,y_k)$,则有

$x+y=((x_1+y_1)\bmod m_1, (x_2+y_2)\bmod m_2, \ldots, (x_k+y_k)\bmod m_k)$,

$x-y=((x_1-y_1)\bmod m_1, (x_2-y_2)\bmod m_2, \ldots, (x_k-y_k)\bmod m_k)$,

$xy=(x_1y_1\bmod m_1, x_2y_2\bmod m_2, \ldots, x_ky_k\bmod m_k)$。

例如，给定模数 $m_1=3$, $m_2=5$, $m_3=7$,大整数 x 的模表示为 $x=(2,4,6)$， $y=(1,2,3)$；

$x+y=$ (2+1) mod 3, (4+2) mod 5, (6+3) mod 7 =(0,1,2)

$x-y=$ (2-1) mod 3, (4-2) mod 5, (6-3) mod 7 =(1,2,3)\)

x×y= (2×1) mod 3, (4×2) mod 5, 6×3) mod 7 =(2,3,4)\)

3）整数模余数表示的优势

（1）拆解与重构大整数运算

可将大整数整体运算，拆解为各模数下独立的小规模模算术运算，运算结束后通过中国剩余定理还原成原整数。该方案可大幅提升运算效率、适配分布式并行处理，同时提升大整数算法的设计灵活性。

（2）降低计算复杂度

传统大整数直接进行加、乘、幂等运算，位数冗余高、耗时量大。采用模表示可分解为多组小模数简易运算，有效压低整体计算复杂度。

（3）节约内存开销

无需完整存储超长位大整数，以各模数对应的余数向量代替原数表征可显著缩减存储空间占用，提升内存利用率。

（4）天然适配并行计算

模表示中各模数的余数分量彼此独立，可在多计算单元上同步并行求解，和很好适配分布式与并行处理架构。

（5）赋能密码学高效安全应用

大整数模运算是公钥密码体制的核心基础，模表示可加速大数模幂、模乘等核心运算，为密码学场景兼顾运算效率与安全强度提供支撑。

9.5 欧拉定理和费马小定理

本章前面各小节介绍了整数的整除、素性、同余规则、解同余方程组、大整数拆分与基础模运算，本节通过欧拉函数和费马小定理对互素个数定量统计、高次幂模化简、快捷求模逆元等核心问题进行求解。

9.5.1 费马小定理

前面介绍的模加减、模乘、线性同余、大数拆分模运算，只能解决普通数值与线性同余问题，超高次幂的模运算计算量极大、效率极低。费马小定理利用素数的同余性质对超大指数进行降幂化简，将高次幂压缩为低次幂，快速完成模幂运算。

1）费马小定理

定理 9.21：费马小定理

设 p 为素数，若整数 a 与 p 互素，则 $a^{p-1}\equiv 1(\mathrm{mod}\ p)$，对任意整数 a，恒有 $a^p\equiv a(\mathrm{mod}\ p)$。

等价表述：若 p 为素数且 a 与 p 互素，则 a^{p-1}-1 能被 p 整除。

由 $a^{p-1}\equiv 1(\mathrm{mod}\ p)$的变形 $a.a^{p-2}\equiv 1(\mathrm{mod}\ p)$ 可得 因此 $a^{p-2}\ \mathrm{mod}\ p$ 即为 a 在模 p 下的乘法逆元。

2）费马小定理的应用

（1）求解同余方程 $ax\equiv b(\mathrm{mod}\ p)$：当 p 为素数时，费马小定理可简化模 p 下的幂运算求解；

（2）素性检测：虽然并非绝对可靠，但在多数情况下，可用费马小定理检验一个数是否为素数。

（3）直接判定部分整数为合数：对整数 (p>1)，若存在整数 a 满足 (1<a<p) 且 (gcd(a,p)=1)，使得 $a^{p-1}\mathrm{mod}\ p\neq 1$，则可断定 p 为合数。例如， $2^{9-1}=4\ \mathrm{mod}\ 9$ ，由此可判定 9 是合数。

9.5.2 欧拉函数及其计算方法

欧拉函数量化统计与 n 互素的整数个数，回答“模 n 里面，到底有多少个数和 n 互素？”。

1）欧拉函数的定义

定义 9.16：欧拉 φ 函数（欧拉函数）

设 n 为正整数，欧拉函数 $\varphi(n)$定义为小于等于 n、且与 n 互素的正整数的个数。

数学表示为：$\varphi(n)=\{k\in\mathbb{Z}^+ \mid 1\le k\le n, \gcd(k,n)=1\}$

2）欧拉函数的性质与计算

设 n 为正整数，$\varphi(n)$为欧拉函数。

（1）初值性质：$\varphi(1)=1$，1 与自身互素，是定义直接约定。

（2）素数的欧拉函数：若 p 为素数，则 $\varphi(p)=p-1$。即 1,2, … , p-1 都与素数 p 互素。

（3）素数幂的欧拉函数

设 p 为素数， k≥1 为正整数, $\varphi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)$。即 1 到 p^k 去掉所有 p 的倍数，剩余即为与 p^k 互素的数。

（4）积性性质：若 gcd(m,n)=1，则：$\varphi(mn)=\varphi(m)\,\varphi(n)$。即互素的两个正整数，欧拉函数可分离乘积。

（5）欧拉函数的素因子分解乘积计算公式

对任意正整数素因数分解：$n=p_1^{k1}\cdot p_2^{k2}\cdots\cdot p_1^{kr}$，其中 $p_1,p_2,\ldots,p_r$ 是不同的素数，则

$\varphi(n)=n\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\cdots\cdot\left(1-\frac{1}{p_r}\right)$。

例如，$\varphi(4)=2$，只有 1 与 3 与 4 互素。12 的素数分解为 $2^2\times3$,有 $p_1=2$ 和 $p_2=3$，有: $\varphi(12)=12\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)=4$。

除上述核心定义、基本性质与计算公式外，欧拉函数还具备整除大小估值、因数求和恒等式以及与简化剩余系相关的衍生性质。

9.5.3 欧拉定理

费马小定理主要用于素数模数下对高次幂同余进行降幂化简，可用于快速求解大指数模运算、判定素数与合数以及求解线性同余方程；欧拉函数用来统计一个正整数范围内与其互素的整数个数。欧拉定理把费马小定理从素数模数推广到任意正整数模数，实现任意模数下快速模幂运算。

定理 9.22：欧拉定理

设 a 与 n 互素（gcd(a,n)=1）, 则有 $a^{\varphi(n)}\equiv1\pmod n$。

欧拉定理中的互素条件只是要求 a 与 n 没有 1 以外的公因数，并不要求 a 和 n 自身必须是素数，二者可以同为合数、一素一合或同为素数，只要满足互素即可。而费马小定理是欧拉定理的特例，不但要求整数 ***a* 与 *n*** 互素，而且要求 n 为素数，因而欧拉定理是费马小定理的推广。

当 n 为素数时，$\varphi(n)=n-1$，欧拉定理退化为费马小定理 $a^{n-1}\equiv1\pmod n$。

当 n 是合数时，欧拉定理提供了寻找模 n 下逆元的方法，因为 $a^{\phi(n)-1}$ 就是 a 的模 n 逆元。

例 9.12：用欧拉定理求解同余方程 $5x\equiv8\pmod{101}$

解：

（1）确定参数：在给定方程中，a=5, n=101, b=8。a 与 n 互素 gcd(5,101)=1，满足欧拉定理条件，n =101 为素数，有 $\varphi(101)=101-1=100$；

（2）应用欧拉定理

由 $a^{\varphi(n)}\equiv1\pmod n$，有 $5^{100}\equiv1\pmod{101}$，变形得 $5.5^{99}\equiv1\pmod{101}$，根据乘法逆元的定义，$5^{99}$ 就是 5 在模 101 下的乘法逆元，即 $5^{-1}\equiv5^{99}\pmod{101}$。

（3）求 5 在模 101 下的乘法逆元

根据正整数的二进制表示原理，有 $99=2^6+2^5+2^1+2^0=64+32+2+1$;

5^{99} 直接计算困难，根据乘法模运算乘法性质有 $5^{99}=5^{64}\cdot5^{32}\cdot5^2\cdot5^1$

$5^{99}\pmod{101}\equiv5^{64}\cdot5^{32}\cdot5^2\cdot5^1\pmod{101}$

$\equiv81\pmod{101}$

即乘法逆元 $5^{-1}\equiv81\pmod{101}$

（4）解同余方程 $5x\equiv8\pmod{101}$

方程两边同时乘逆元 81：

$81.5x\equiv81.8$

$x \equiv 42 \pmod{101}$

（5）验证：$5\times42=210$，$210 \equiv 8 \pmod{101}$成立。

最终解：$x \equiv 42 \pmod{101}$。

知识扩展提示词

1. 借助 AI 工具证明算术基本定理。
2. 为什么将模 m 等价类的集合称为整数模 m 商集？
3. 乘法逆元如何影响公钥/私钥加密体系的破解难度？
4. 广义中国剩余定理与标准中国剩余定理的主要区别？
5. 费马小定理的证明过程？
6. 欧拉定理和费马小定理有什么区别和联系？

第 9 章 主要符号表

序号	符号	含义	示例
1	$\mid$	整除关系符号	命题：b 整除 a，记作 $b\|a$，如 $6\mid2$ 结果为假，$2\mid6$ 结果为真
2	$\nmid$	不能整除关系符号	$6\nmid2$，6 不能整除 2，命题为真； $2\nmid6$，2 能整除 6，命题为假。
3	div	整除运算、商运算	6 div 2=3，2 div 6=0
4	mod	模运算符号	7 mod 3=1，3 mod 7=3
5	$\pi(x)$	不大于 x 的所有素数的个数	$\pi(7)=\pi(8)=\pi(9)=\pi(10)=4$，即 (2、3、5、7)
6	$\gcd(a,b)$	a 和 b 的最大公约数	$\gcd(-12,18)=2\times3=6$
7	$\mathrm{lcm}(a,b)$	a 和 b 的最小公倍数	$\mathrm{lcm}(-12,18)=2^2\times3^2=36$
8	$a\equiv b \pmod m$	同余关系式，表示整数 a 与 b 模 m 同余	$327\equiv137 \pmod{19}$ 是真命题
9	$a\not\equiv b \pmod m$	a 与 b 模 m 不同余	$327\not\equiv137 \pmod{19}$ 是假命题，说明“327 与 137 模 19 不同余”这句话是错的，二者实际同余。
10	$ax\equiv b \pmod m$	线性同余方程	$3x\equiv4 \pmod 7$的解为 $x\equiv6 \pmod 7$，如 6,13,20,−1 等。
11	$a^{-1} \pmod m$ 或 a^{-1}	模 m 逆元	$a^{-1} \pmod m$ 是满足 $ax\equiv1 \pmod m$ 的整数解 x
12	$\varphi(n)$	欧拉函数	$\varphi(n)=\{k\in\mathbb{Z}^+ \mid 1\le k\le n, \gcd(k,n)=1\}$