C++数论知识核心大纲

一、数论基础（必备）

（一）整数基础概念

- 整数分类：正整数、负整数、零；奇数与偶数的性质及C++判断实现
- 整除与余数：整除定义、余数定理，模运算（%）基础及注意事项（负数取模）
- 质数与合数：定义、质数判定的朴素方法（适用于小范围数据）

（二）模运算核心规则

- 基本运算律：(a±b)%mod、(a×b)%mod 的计算及溢出规避（C++中long long适配）
- 模逆的前置认知：模运算中除法转化为乘法的前提
- 常用技巧：模运算与循环计数、范围限制的结合（如数组下标映射）

二、质数相关（高频考点）

（一）质数判定

- 优化算法：试除法优化（遍历到$\sqrt{n}$）及C++代码实现
- 高效筛法：埃氏筛（Eratosthenes）、线性筛（欧拉筛）原理与代码，适用于大范围质数筛选

（二）质数拓展

- 质因数分解：试除法分解、结合筛法的高效分解，适配大数场景
- 欧拉函数前置：质数与互质的关联，欧拉函数的基础定义

三、最大公约数（GCD）与最小公倍数（LCM）

（一）核心算法

- 欧几里得算法（辗转相除法）：原理、C++递归与迭代实现
- 扩展欧几里得算法：求解ax+by=gcd(a,b)，为模逆求解铺垫

（二）应用场景

- LCM计算：基于GCD的推导（LCM(a,b)=a×b/GCD(a,b)）及溢出处理

- 互质判定：GCD(a,b)=1的应用（分数化简、模逆存在性判断）
- C++标准库：algorithm头文件中__gcd函数的使用注意事项

四、模逆与同余方程（进阶必备）

（一）同余基础

- 同余定义：a≡b(mod m)的含义及基本性质
- 同余方程：一元线性同余方程ax≡b(mod m)的求解条件与步骤

（二）模逆求解

- 模逆定义：满足ax≡1(mod m)的x，即为a在模m下的逆元
- 求解方法：扩展欧几里得法、费马小定理（适用于m为质数的场景）
- 应用：模运算中除法的转化（a/b mod m = a×b⁻¹ mod m）

五、欧拉函数与欧拉定理（进阶）

（一）欧拉函数（φ函数）

- 定义：1~n中与n互质的整数个数，计算公式及推导
- 计算方法：基于质因数分解的公式计算、线性筛同步求欧拉函数

（二）欧拉定理与费马小定理

- 欧拉定理：若a与m互质，则a^φ(m)≡1(mod m)，应用于大数幂模简化
- 费马小定理：欧拉定理的特例（m为质数），a^(m-1)≡1(mod m)，简化模逆求解

六、大数幂模（快速幂）

- 核心原理：分治法简化幂运算（a^b mod m），降低时间复杂度至O(log b)
- C++实现：递归与迭代版本，适配大指数、大模数场景（结合long long/unsigned long long）
- 应用：结合欧拉定理/费马小定理，解决大数幂运算溢出问题

七、竞赛高频拓展（选学，适配蓝桥杯/CSP-J/S）

- 中国剩余定理（CRT）：求解多元线性同余方程组，适用于多模数场景
- 容斥原理：结合数论的计数问题（如1~n中不能被指定质数整除的数的个数）
- 斐波那契数列的数论性质：模周期、斐波那契质数相关题目适配

- 整除分块：快速计算含除法的数论求和问题（如Σ(n/i)，i从1到n）

八、C++实操注意事项

- 数据类型：大数场景优先使用long long，避免int溢出，必要时使用高精度模板
- 效率优化：大范围筛法、多次查询场景的预处理技巧（如预处理质数表、欧拉函数表）
- 易错点：负数模运算结果、模逆存在性判断、快速幂边界条件（b=0）

九、学习优先级建议

1. 基础层：模运算 → GCD/LCM → 质数判定与筛法 → 快速幂（必备，覆盖80%基础题目）；
2. 进阶层：欧拉函数与定理 → 模逆 → 线性同余方程（适配CSP-J/S中档题）；
3. 拓展层：中国剩余定理、容斥原理（针对蓝桥杯、CSP-S难题，按需学习）。

（注：文档部分内容可能由 AI 生成）