

# 《初等数论基础》课程知识点汇总

## 第一章

- 本原勾股数组（三元组）的概念
- 本原勾股三元组的定理及其证明

## 第二章

- 整除、公因数、最大公因数的概念
- 欧几里得辗转相除算法
- 线性方程的概念
- 掌握线性方程定理
- 掌握求解线性方程  $ax+by=gcd(a,b)$  的方法

## 第三章

- 素数、合数的概念
- 素数整除性质及其证明
- 算术基本定理
- 掌握素数分解的几种方法及其各自的优缺点

## 第四章

- 同余式的概念，及其性质
- 求解带未知数的同余式的通用方法
- 掌握线性同余式定理，以及求解形如  $ax \equiv c(mod m)$  同余式的方法
- 掌握费马小定理，及其证明基本思想和应用

## 第五章

- 欧拉  $\Phi$  函数的定义
- 欧拉公式及其证明
- 欧拉  $\Phi$  函数公式及其计算
- 中国剩余定理

## 第六章

- 无穷多素数定理，及其欧几里得证明基本思想
- 算术级数的素数狄利克雷定理
- 素数计数函数  $\pi(x)$  的定义
- 函数  $x/\ln(x)$  逼近  $\pi(x)$  的素数定理

## 第七章

- 梅森素数、完全数、 $\sigma$  函数的定义
- $\sigma$  函数公式定理及其证明和应用
- 欧拉  $\phi$  函数求和公式及其证明

## 第八章

- $a$  模  $p$  的次数的定义，以及求次数的方法
- 次数整除性质及其应用
- 原根概念、指标的概念和法则
- 掌握求解一个素数所有原根的方法
- 二次剩余(QR)和二次非剩余(NR)的定义
- 二次乘法法则定理 (2 种版本)
- 掌握判断一个整数是素数  $p$  的 QR 还是 NR 的方法

## 第九章

- 佩尔方程的定义
- 佩尔方程定理
- 狄利克雷丢番图逼近定理 (2 种版本)

## 第十章

- 高斯整数的概念
- 高斯整数基本运算的封闭性
- 高斯整数的整除性定义及性质
- 单位和相伴的定义
- 高斯素数的定义, 及其判断的基本方法
- 高斯整数的唯一分解定理, 以及高斯整数的整除性质

## 第十一章

- 连分数的基本概念