网络空间安全学院

School of Cyberspace Security, BUPT

信息安全数学基础

—— 导　论

信数课题组

北京邮电大学网络空间安全学院

2024 年 9 月 8 日

目录

1. 课程概述
   - 背景
   - 目标
2. 教学计划
   - 学时安排
   - 教学方法
   - 课程资源
3. 课程考核

目录

1 课程概述
- 背景
- 目标

2 教学计划
- 学时安排
- 教学方法
- 课程资源

3 课程考核

国家战略前瞻

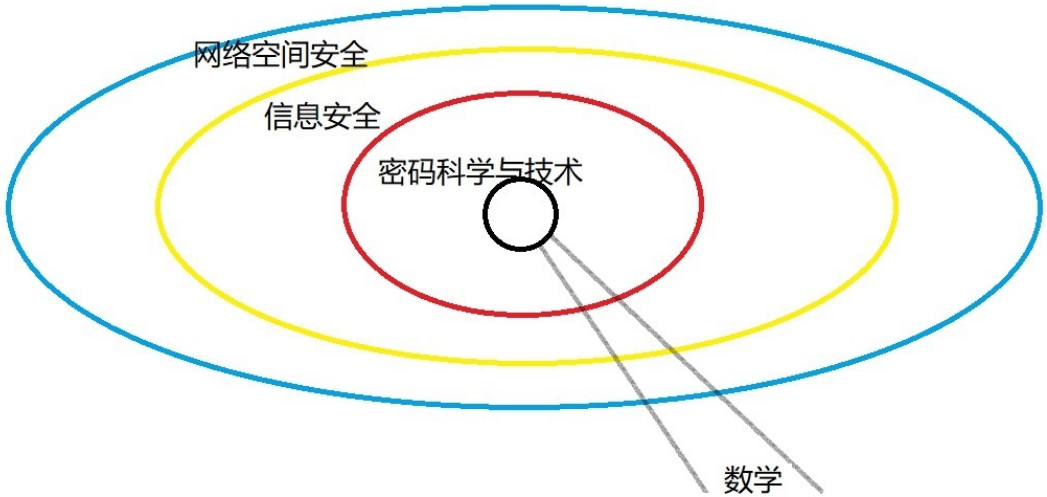
要全面贯彻网络强国战略，把数字技术广泛应用于政府管理服务，推动政府数字化、智能化运行，为推进国家治理体系和治理能力现代化提供有力支撑。

—— 习近平 2022 年 4 月 19 日在中央全面深化改革委员会第二十五次会议上的讲话

没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；……

—— 习近平 2014 年 2 月 27 日在中央网络安全和信息化领导小组第一次会议上的讲话

网络空间安全大类三大专业



专业关系示意图

注：通过密码技术（ **基于数学理论的变换** ）实现 **基本安全属性**。

基本安全属性

1. 机密性:

   保证信息被授权者使用而不泄露给未授权者；即让未授权者看不到信息或者看不懂信息。

基本安全属性

1. 机密性:

   保证信息被授权者使用而不泄露给未授权者；即让未授权者看不到信息或者看不懂信息。

2. 认　证：
   - 消息认证：包括消息源认证和消息完整性，前者保证消息来源未被冒充，后者保证消息未被篡改;
   - 身份认证：保证通信实体的真实性。

基本安全属性

1. 机密性:

   保证信息被授权者使用而不泄露给未授权者；即让未授权者看不到信息或者看不懂信息。

2. 认　证：
   - 消息认证：包括消息源认证和消息完整性，前者保证消息来源未被冒充，后者保证消息未被篡改;
   - 身份认证：保证通信实体的真实性。

3. 完整性：
   - 数据完整性：数据未被未授权篡改或损坏；
   - 系统完整性：系统未被非授权操控，即按既定的程序运行。

基本安全属性

1. 机密性:

   保证信息被授权者使用而不泄露给未授权者；即让未授权者看不到信息或者看不懂信息。

2. 认　证：
   - 消息认证：包括消息源认证和消息完整性，前者保证消息来源未被冒充，后者保证消息未被篡改;
   - 身份认证：保证通信实体的真实性。

3. 完整性：
   - 数据完整性：数据未被未授权篡改或损坏；
   - 系统完整性：系统未被非授权操控，即按既定的程序运行。

4. 不可否认性：

   无论发送方还是接收方都不能抵赖所进行的传输等行为。

数学理论基础

类别	涵盖内容	开课学期
先修课程	高等数学、线性代数、离散数学	第一、二学期
本门课程	数论、近世（抽象）代数、有限域	第三学期
其他课程	概率论与数理统计、数学建模、组合数学、复变函数、……	第三、四学期

注：详见各专业培养方案。

目录

1 课程概述
- 背景
- 目标

2 教学计划
- 学时安排
- 教学方法
- 课程资源

3 课程考核

课程目标

1. 掌握信息安全领域的编码与密码的数学基础知识，能够将信息安全数学基础中的基本概念、基本理论和基本方法应用到信息安全等相关系统中。
2. 能够根据信息安全领域中复杂工程问题的需求描述，运用信息安全数学基础的基本原理、方法进行综合分析，建立解决问题的抽象模型。

目录

1 课程概述
- 背景
- 目标

2 教学计划
- 学时安排
- 教学方法
- 课程资源

3 课程考核

计划表——数论 (1)

知识模块	教学内容	学时
整数的可除性（1）	整除的概念，素数及其平凡判别，Eratosthenes 筛法、欧几里德除法、整数 b 进制表示	3
整数的可除性（2）	最大公因数，广义欧几里德除法，贝祖等式，最小公倍数，整数分解	3
同余（1）	同余的概念及基本性质，剩余，剩余类及完全剩余系	3
同余（2）	简化剩余系，欧拉函数，欧拉定理，费马小定理，Wilson 定理，模重复平方计算法	3
同余方程（1）	同余方程的基本概念，一次同余方程，中国剩余定理，同余方程组	3

计划表——数论 (2)

知识模块	教学内容	学时
同余方程（2）	二次同余方程，平方剩余，勒让德符号，二次互反定律，雅可比符号，二次同余方程求解	3
同余方程（3）	高次同余方程的解数，素数模的高次同余方程，素数幂模的高次同余方程——幂指数提升	3
阶与原根	阶及其基本性质，原根的定义，原根存在的充要条件，指标与 n 次同余方程	3
素性检测	Fermat 素性检测、S-S 素性检测、M-R 素性检测、A-K-S 素性检测	3

计划表——近世（抽象）代数及有限域

知识模块	教学内容	学时
群（1）	群的定义与性质，子群	3
群（2）	正规子群，商群，群同态与同构，群同态基本定理	3
群（3）	循环群，置换群	3
环（1）	环的定义，子环，理想和商环，环同态与同构，环同态基本定理	3
环（2）	多项式整环，多项式整除与不可约多项式，多项式欧几里德除法，多项式同余	3
域（1）	域与子域，分式域，素域，有限扩域，代数扩域，单扩域，分裂域	3
域（2）	Galois 基本定理，有限域	3

目录

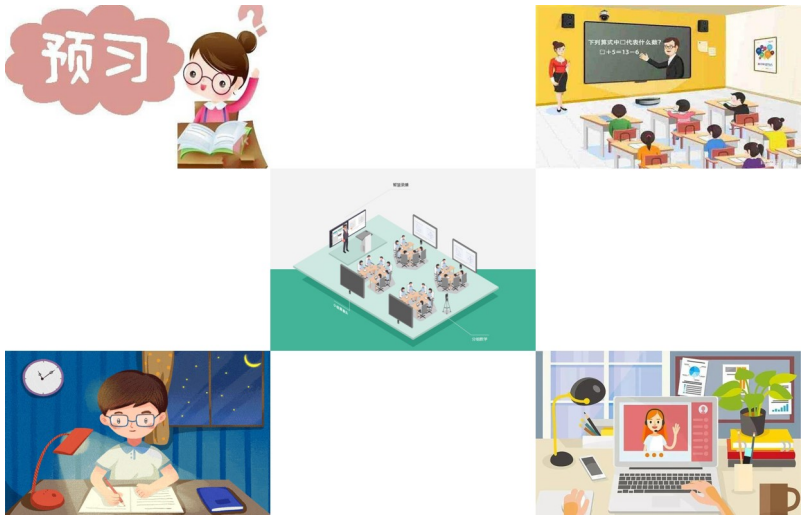
1 课程概述
- 背景
- 目标

2 教学计划
- 学时安排
- 教学方法
- 课程资源

3 课程考核

学习要求

1. 课前预习，充分准备。
2. 课堂教学，认真听讲。
3. 研讨教学，积极探索。
4. 课后复习，消化巩固。
5. 线上自学，融汇贯通。



注：课程性质决定需要这样的学习方法 (成熟、会学习的表现)。

目录

1 课程概述
- 背景
- 目标

2 教学计划
- 学时安排
- 教学方法
- 课程资源

3 课程考核

教学资料

1. 课程教材

《信息安全数学基础》(第 2 版), 陈恭亮, 清华大学出版社, 2014 年 10 月.

2. 参考书目

《信息安全数学基础》, 罗守山、徐国胜, 北京邮电大学出版社, 2018 年 8 月.

《公钥密码学的数学基础》, 王小云、王明强等, 科学出版社, 2013 年 1 月.

《初等数论》（第三版）, 潘承洞、潘承彪, 北京大学出版社, 2019 年 5 月.

《算法数论》, 裴定一、祝跃飞, 科学出版社, 2015 年 9 月.

《近世代数基础》, 张禾瑞, 高等教育出版社, 2010 年 11 月.

《数论与密码》, 杨思熳, 华东师范大学出版社, 2010 年 9 月.

《数论与有限域》, 董丽华等, 机械工业出版社, 2010 年 10 月.

《代数学基础与有限域》, 林东岱, 高等教育出版社, 2006 年 7 月.

线上课程

1. 课程名：Number Theory

   开课学校：University of York

   课程链接：

   https://www.york.ac.uk/maths/research/number-theory/

2. 课程名：Modern Algebra

   开课学校：Massachusetts Institute of Technology

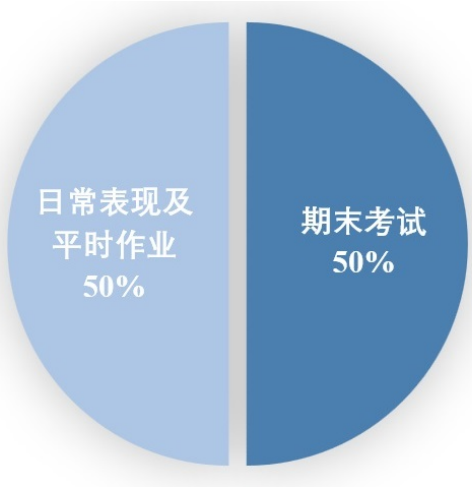
   课程链接：https://ocw.mit.edu/courses/mathematics/18-703-modern-algebra-spring-2013/

考核环节

考核环节主要包括日常表现、平时作业和期末考试。

课堂小作业、课堂讨论

1. 日常表现及平时作业
   包括出勤、课堂表现等，作业一般为每周一次，涵盖课程所有内容，根据是否按时提交、完成情况等进行综合评定。
2. 期末考试
   闭卷考试，题目涉及课程全部教学内容，按照卷面成绩进行评定。



交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn

网络空间安全学院

School of Cyberspace Security, BUPT

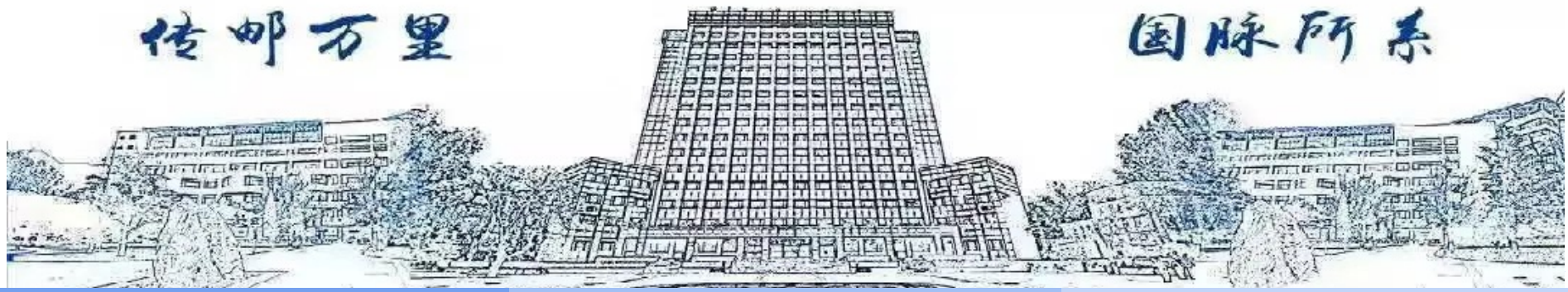
信息安全数学基础

—— 整数的可除性 (1)

信数课题组

北京邮电大学网络空间安全学院

2024 年 9 月 8 日



目录

1. 整除　欧几里德除法　整数表示
   - 整除的概念
   - 素数及其平凡判别
   - Eratoshenes 筛法
   - 欧几里德除法
   - 整数 b 进制表示

目录

1 整除　欧几里德除法　整数表示
- 整除的概念
- 素数及其平凡判别
- Eratoshenes 筛法
- 欧几里德除法
- 整数 b 进制表示

定义 1.1.1

设 a, b 是任意两个整数, 其中 $b \neq 0$. 若存在一个整数 q 使得等式

$$a = q \cdot b \tag{1.1.1}$$

成立, 就称 b **整除** a, 或者 a 被 b 整除, 记作 $b \mid a$, 把 b 叫做 a 的**因数**, 把 a 叫做 b 的**倍数**.

否则, 就称 b 不能整除 a, 或者 a 不能被 b 整除, 记作 $b \nmid a$.

此外, 由于整数的乘法运算具有可以交换的性质, 因此, q 也叫 a 的因数, 我们常常将 q 写成 a/b 或 $\frac{a}{b}$.

定义 1.1.1

设 a, b 是任意两个整数, 其中 $b \neq 0$. 若存在一个整数 q 使得等式

$$a = q \cdot b \tag{1.1.1}$$

成立, 就称 b **整除** a, 或者 a 被 b 整除, 记作 $b \mid a$, 把 b 叫做 a 的**因数**, 把 a 叫做 b 的**倍数**.

否则, 就称 b 不能整除 a, 或者 a 不能被 b 整除, 记作 $b \nmid a$.

此外, 由于整数的乘法运算具有可以交换的性质, 因此, q 也叫 a 的因数, 我们常常将 q 写成 a/b 或 $\frac{a}{b}$.

注 1:

0 是任何非零整数的倍数.

1 是任何整数的因数.

任何非零整数 a 是其自身的倍数, 也是其自身的因数.

定义 1.1.1

设 a, b 是任意两个整数, 其中 $b \neq 0$. 若存在一个整数 q 使得等式

$$a = q \cdot b \tag{1.1.1}$$

成立, 就称 b **整除** a, 或者 a 被 b 整除, 记作 $b \mid a$, 把 b 叫做 a 的**因数**, 把 a 叫做 b 的**倍数**.

否则, 就称 b 不能整除 a, 或者 a 不能被 b 整除, 记作 $b \nmid a$.

此外, 由于整数的乘法运算具有可以交换的性质, 因此, q 也叫 a 的因数, 我们常常将 q 写成 a/b 或 $\frac{a}{b}$.

注 1:

0 是任何非零整数的倍数.

1 是任何整数的因数.

任何非零整数 a 是其自身的倍数, 也是其自身的因数.

例 1.1.1　$3 \mid 21$, $-3 \mid 21$, $3 \nmid 22$, $5 \mid 0$, $7 \mid 7$.

注 2：设 b_1,b_2, $\cdots$, b_k 是 a 的所有因数, 那么 $-b_1$,$-b_2$, $\cdots$, $-b_k$ 也是它的所有因数, 同时 $\frac{a}{b_1}$, $\frac{a}{b_2}$, $\cdots$, $\frac{a}{b_k}$ 也是它的所有因数.

注 2：设 b_1,b_2, $\cdots$, b_k 是 a 的所有因数, 那么 $-b_1$,$-b_2$, $\cdots$, $-b_k$ 也是它的所有因数, 同时 $\frac{a}{b_1}$, $\frac{a}{b_2}$, $\cdots$, $\frac{a}{b_k}$ 也是它的所有因数.

也就是说,

(1) 当 b 遍历整数 a 的所有因数时, $-b$ 也遍历 a 的所有因数.

(2) 当 b 遍历整数 a 的所有因数时, $\frac{a}{b}$ 也遍历 a 的所有因数.

注 2：设 $b_1, b_2, \cdots, b_k$ 是 a 的所有因数，那么 $-b_1, -b_2, \cdots, -b_k$ 也是它的所有因数，同时 $\frac{a}{b_1}, \frac{a}{b_2}, \cdots, \frac{a}{b_k}$ 也是它的所有因数.

也就是说，

(1) 当 b 遍历整数 a 的所有因数时，$-b$ 也遍历 a 的所有因数.

(2) 当 b 遍历整数 a 的所有因数时，$\frac{a}{b}$ 也遍历 a 的所有因数.

例 1.1.2　$105 = 3 \cdot 35 = 5 \cdot 21 = 7 \cdot 15$.

注 2：设 $b_1, b_2, \cdots, b_k$ 是 a 的所有因数，那么 $-b_1, -b_2, \cdots, -b_k$ 也是它的所有因数，同时 $\frac{a}{b_1}, \frac{a}{b_2}, \cdots, \frac{a}{b_k}$ 也是它的所有因数.

也就是说，

(1) 当 b 遍历整数 a 的所有因数时，$-b$ 也遍历 a 的所有因数.

(2) 当 b 遍历整数 a 的所有因数时，$\frac{a}{b}$ 也遍历 a 的所有因数.

例 1.1.2　$105 = 3 \cdot 35 = 5 \cdot 21 = 7 \cdot 15$.

3, 5, 7 分别整除 105，或者 105 被 3, 5, 7 分别整除，

记作 $3 \mid 105, 5 \mid 105, 7 \mid 105$.

3, 5, 7 都是 105 的因数，105 是 3, 5, 7 的倍数.

注 2：设 $b_1, b_2, \cdots, b_k$ 是 a 的所有因数，那么 $-b_1, -b_2, \cdots, -b_k$ 也是它的所有因数，同时 $\frac{a}{b_1}, \frac{a}{b_2}, \cdots, \frac{a}{b_k}$ 也是它的所有因数.

也就是说，

(1) 当 b 遍历整数 a 的所有因数时，$-b$ 也遍历 a 的所有因数.

(2) 当 b 遍历整数 a 的所有因数时，$\frac{a}{b}$ 也遍历 a 的所有因数.

例 1.1.2　$105 = 3 \cdot 35 = 5 \cdot 21 = 7 \cdot 15$.

3, 5, 7 分别整除 105，或者 105 被 3, 5, 7 分别整除，

记作 $3 \mid 105, 5 \mid 105, 7 \mid 105$.

3, 5, 7 都是 105 的因数，105 是 3, 5, 7 的倍数.

105 的所有因数是 $\{\pm 1, \pm 3, \pm 5, \pm 7, \pm 15, \pm 21, \pm 35, \pm 105\}$.

或是，$\{\mp 1, \mp 3, \mp 5, \mp 7, \mp 15, \mp 21, \mp 35, \mp 105\}$.

注 2：设 $b_1, b_2, \cdots, b_k$ 是 a 的所有因数，那么 $-b_1, -b_2, \cdots, -b_k$ 也是它的所有因数，同时 $\frac{a}{b_1}, \frac{a}{b_2}, \cdots, \frac{a}{b_k}$ 也是它的所有因数.

也就是说，

(1) 当 b 遍历整数 a 的所有因数时，$-b$ 也遍历 a 的所有因数.

(2) 当 b 遍历整数 a 的所有因数时，$\frac{a}{b}$ 也遍历 a 的所有因数.

例 1.1.2　$105 = 3 \cdot 35 = 5 \cdot 21 = 7 \cdot 15$.

3, 5, 7 分别整除 105，或者 105 被 3, 5, 7 分别整除，

记作 $3 \mid 105, 5 \mid 105, 7 \mid 105$.

3, 5, 7 都是 105 的因数，105 是 3, 5, 7 的倍数.

105 的所有因数是 $\{\pm 1, \pm 3, \pm 5, \pm 7, \pm 15, \pm 21, \pm 35, \pm 105\}$.

或是，$\{\mp 1, \mp 3, \mp 5, \mp 7, \mp 15, \mp 21, \mp 35, \mp 105\}$.

或是，$\{\pm 105 = \frac{105}{\pm 1}, \pm 35 = \frac{105}{\pm 3}, \pm 21 = \frac{105}{\pm 5}, \pm 15 = \frac{105}{\pm 7}, \pm 7 = \frac{105}{\pm 15}, \pm 5 = \frac{105}{\pm 21}, \pm 3 = \frac{105}{\pm 35}, \pm 1 = \frac{105}{\pm 105}\}$.

定理 1.1.1

设 $a, b \neq 0, c \neq 0$ 是三个整数. 若 $c \mid b, b \mid a$, 则 $c \mid a$.

定理 1.1.1

设 $a, b \neq 0, c \neq 0$ 是三个整数. 若 $c \mid b, b \mid a$, 则 $c \mid a$.

证：设 $c \mid b, b \mid a$, 根据整除的定义, 分别存在整数 q_1, q_2 使得 $b = q_1 \cdot c, a = q_2 \cdot b$. 因此, 有 $a = q_2 \cdot b = q_2 \cdot (q_1 \cdot c) \triangleq q \cdot c$.

因为 $q = q_2 \cdot q_1$ 是整数, 所以根据整除的定义知 $c \mid a$.

定理 1.1.1

设 $a, b \neq 0, c \neq 0$ 是三个整数. 若 $c \mid b, b \mid a$, 则 $c \mid a$.

证：设 $c \mid b, b \mid a$, 根据整除的定义, 分别存在整数 q_1, q_2 使得 $b = q_1 \cdot c, a = q_2 \cdot b$. 因此, 有 $a = q_2 \cdot b = q_2 \cdot (q_1 \cdot c) \triangleq q \cdot c$.

因为 $q = q_2 \cdot q_1$ 是整数, 所以根据整除的定义知 $c \mid a$.

例 1.1.3　因为 $3 \mid 12, 12 \mid 36$, 所以 $3 \mid 36$.

定理 1.1.1

设 $a, b \neq 0, c \neq 0$ 是三个整数. 若 $c \mid b, b \mid a$, 则 $c \mid a$.

证：设 $c \mid b, b \mid a$, 根据整除的定义, 分别存在整数 q_1, q_2 使得 $b = q_1 \cdot c, a = q_2 \cdot b$. 因此, 有 $a = q_2 \cdot b = q_2 \cdot (q_1 \cdot c) \triangleq q \cdot c$.

因为 $q = q_2 \cdot q_1$ 是整数, 所以根据整除的定义知 $c \mid a$.

例 1.1.3　因为 $3 \mid 12, 12 \mid 36$, 所以 $3 \mid 36$.

定理 1.1.2

设 $a, b, c \neq 0$ 是三个整数. 若 $c \mid a, c \mid b$, 则 $c \mid a \pm b$.

定理 1.1.1

设 $a, b \neq 0, c \neq 0$ 是三个整数. 若 $c \mid b, b \mid a$, 则 $c \mid a$.

证：设 $c \mid b, b \mid a$, 根据整除的定义, 分别存在整数 q_1, q_2 使得 $b = q_1 \cdot c, a = q_2 \cdot b$. 因此, 有 $a = q_2 \cdot b = q_2 \cdot (q_1 \cdot c) \triangleq q \cdot c$.

因为 $q = q_2 \cdot q_1$ 是整数, 所以根据整除的定义知 $c \mid a$.

例 1.1.3　因为 $3 \mid 12, 12 \mid 36$, 所以 $3 \mid 36$.

定理 1.1.2

设 $a, b, c \neq 0$ 是三个整数. 若 $c \mid a, c \mid b$, 则 $c \mid a \pm b$.

证：设 $c \mid a, c \mid b$, 则存在两个整数 q_1, q_2 分别使得 $a = q_1 \cdot c, b = q_2 \cdot c$. 因此, 有 $a \pm b = q_1 \cdot c \pm q_2 \cdot c = (q_1 \pm q_2) \cdot c$.

因为 $q_1 \pm q_2$ 是整数, 所以 $c \mid a \pm b$.

定理 1.1.1

设 $a, b \neq 0, c \neq 0$ 是三个整数. 若 $c \mid b, b \mid a$, 则 $c \mid a$.

证：设 $c \mid b, b \mid a$, 根据整除的定义, 分别存在整数 q_1, q_2 使得 $b = q_1 \cdot c, a = q_2 \cdot b$. 因此, 有 $a = q_2 \cdot b = q_2 \cdot (q_1 \cdot c) \triangleq q \cdot c$.

因为 $q = q_2 \cdot q_1$ 是整数, 所以根据整除的定义知 $c \mid a$.

例 1.1.3　因为 $3 \mid 12, 12 \mid 36$, 所以 $3 \mid 36$.

定理 1.1.2

设 $a, b, c \neq 0$ 是三个整数. 若 $c \mid a, c \mid b$, 则 $c \mid a \pm b$.

证：设 $c \mid a, c \mid b$, 则存在两个整数 q_1, q_2 分别使得 $a = q_1 \cdot c, b = q_2 \cdot c$. 因此, 有 $a \pm b = q_1 \cdot c \pm q_2 \cdot c = (q_1 \pm q_2) \cdot c$.

因为 $q_1 \pm q_2$ 是整数, 所以 $c \mid a \pm b$.

例 1.1.4　$5 \mid 25, 5 \mid 45$, 故 $5 \mid (25 + 45) = 70, 5 \mid (25 - 45) = -20$.

定理 1.1.3

设 $a, b, c \neq 0$ 是三个整数. 若 $c \mid a, c \mid b$, 则对任意整数 s 和 t, 有 $c \mid (s \cdot a + t \cdot b)$.

定理 1.1.3

设 $a, b, c \neq 0$ 是三个整数. 若 $c \mid a, c \mid b$, 则对任意整数 s 和 t, 有 $c \mid (s \cdot a + t \cdot b)$.

证：设 $c \mid a, c \mid b$, 则存在两个整数 q_1, q_2 分别使得 $a = q_1 \cdot c, b = q_2 \cdot c$. 因此, 有 $s \cdot a + t \cdot b = s \cdot (q_1 \cdot c) + t \cdot (q_2 \cdot c) = (s \cdot q_1 + t \cdot q_2) \cdot c$.

因为 $s \cdot q_1 + t \cdot q_2$ 是整数, 所以 $c \mid (s \cdot a + t \cdot b)$.

定理 1.1.3

设 $a, b, c \neq 0$ 是三个整数. 若 $c \mid a, c \mid b$, 则对任意整数 s 和 t, 有 $c \mid (s \cdot a + t \cdot b)$.

证：设 $c \mid a, c \mid b$, 则存在两个整数 q_1, q_2 分别使得 $a = q_1 \cdot c, b = q_2 \cdot c$. 因此, 有 $s \cdot a + t \cdot b = s \cdot (q_1 \cdot c) + t \cdot (q_2 \cdot c) = (s \cdot q_1 + t \cdot q_2) \cdot c$.

因为 $s \cdot q_1 + t \cdot q_2$ 是整数, 所以 $c \mid (s \cdot a + t \cdot b)$.

例 1.1.5　$3 \mid 6, 3 \mid 15$, 故 $3 \mid (2 \cdot 6 + 5 \cdot 15) = 87, 3 \mid (2 \cdot 6 - 5 \cdot 15) = -63$.

定理 1.1.3

设 $a, b, c \neq 0$ 是三个整数. 若 $c \mid a, c \mid b$, 则对任意整数 s 和 t, 有 $c \mid (s \cdot a + t \cdot b)$.

证：设 $c \mid a, c \mid b$, 则存在两个整数 q_1, q_2 分别使得 $a = q_1 \cdot c, b = q_2 \cdot c$. 因此, 有 $s \cdot a + t \cdot b = s \cdot (q_1 \cdot c) + t \cdot (q_2 \cdot c) = (s \cdot q_1 + t \cdot q_2) \cdot c$.

因为 $s \cdot q_1 + t \cdot q_2$ 是整数, 所以 $c \mid (s \cdot a + t \cdot b)$.

例 1.1.5　$3 \mid 6, 3 \mid 15$, 故 $3 \mid (2 \cdot 6 + 5 \cdot 15) = 87, 3 \mid (2 \cdot 6 - 5 \cdot 15) = -63$.

推论 1.1.1

设 $a, b, c \neq 0$ 是三个整数, $c \mid a, c \mid b$. 如果存在整数 s 和 t, 使得 $s \cdot a + t \cdot b = 1$, 则 $c = \pm 1$.

定理 1.1.3

设 $a, b, c \neq 0$ 是三个整数. 若 $c \mid a, c \mid b$, 则对任意整数 s 和 t, 有 $c \mid (s \cdot a + t \cdot b)$.

证：设 $c \mid a, c \mid b$, 则存在两个整数 q_1, q_2 分别使得 $a = q_1 \cdot c, b = q_2 \cdot c$. 因此, 有 $s \cdot a + t \cdot b = s \cdot (q_1 \cdot c) + t \cdot (q_2 \cdot c) = (s \cdot q_1 + t \cdot q_2) \cdot c$.

因为 $s \cdot q_1 + t \cdot q_2$ 是整数, 所以 $c \mid (s \cdot a + t \cdot b)$.

例 1.1.5　$3 \mid 6, 3 \mid 15$, 故 $3 \mid (2 \cdot 6 + 5 \cdot 15) = 87, 3 \mid (2 \cdot 6 - 5 \cdot 15) = -63$.

推论 1.1.1

设 $a, b, c \neq 0$ 是三个整数, $c \mid a, c \mid b$. 如果存在整数 s 和 t, 使得 $s \cdot a + t \cdot b = 1$, 则 $c = \pm 1$.

证：设 $c \mid a, c \mid b$, 因为存在整数 s 和 t 使得 $s \cdot a + t \cdot b = 1$, 根据定理 1.1.3, 有 $c \mid (s \cdot a + t \cdot b)$, 即 $c \mid 1$. 因此, $c = \pm 1$.

定理 1.1.3 可推广为多个整数的线性组合：

推论 1.1.2

设整数 c. 若整数 $a_1, \cdots, a_n$ 都是整数 $c \neq 0$ 的倍数, 则对任意 n 个整数 $s_1, \cdots, s_n$, 整数 $s_1a_1 + \cdots + s_na_n$ 是 c 的倍数.

定理 1.1.3 可推广为多个整数的线性组合：

推论 1.1.2

设整数 c. 若整数 $a_1, \cdots, a_n$ 都是整数 $c \neq 0$ 的倍数, 则对任意 n 个整数 $s_1, \cdots, s_n$, 整数 $s_1a_1 + \cdots + s_na_n$ 是 c 的倍数.

例 1.1.6　$3 \mid 6$, $3 \mid 15$, $3 \mid 21$, 故 $3 \mid (2 \cdot 6 + 5 \cdot 15 - 2 \cdot 21) = 45$.

定理 1.1.3 可推广为多个整数的线性组合：

推论 1.1.2

设整数 c. 若整数 $a_1, \cdots, a_n$ 都是整数 $c \neq 0$ 的倍数, 则对任意 n 个整数 $s_1, \cdots, s_n$, 整数 $s_1a_1 + \cdots + s_na_n$ 是 c 的倍数.

例 1.1.6　$3 \mid 6$, $3 \mid 15$, $3 \mid 21$, 故 $3 \mid (2 \cdot 6 + 5 \cdot 15 - 2 \cdot 21) = 45$.

定理 1.1.4

设 a, b 都是非零整数. 若 $a \mid b, b \mid a$, 则 $a = \pm b$.

定理 1.1.3 可推广为多个整数的线性组合：

推论 1.1.2

设整数 c. 若整数 $a_1, \cdots, a_n$ 都是整数 $c \neq 0$ 的倍数, 则对任意 n 个整数 $s_1, \cdots, s_n$, 整数 $s_1a_1 + \cdots + s_na_n$ 是 c 的倍数.

例 1.1.6　$3 \mid 6$, $3 \mid 15$, $3 \mid 21$, 故 $3 \mid (2 \cdot 6 + 5 \cdot 15 - 2 \cdot 21) = 45$.

定理 1.1.4

设 a, b 都是非零整数. 若 $a \mid b, b \mid a$, 则 $a = \pm b$.

证：设 $a \mid b, b \mid a$, 则存在两个整数 q_1, q_2 分别使得 $a = q_1 \cdot b, b = q_2 \cdot a$. 从而, $a = q_1 \cdot b = q_1 \cdot (q_2 \cdot a) = (q_1 \cdot q_2) \cdot a$. 进而, $(q_1 \cdot q_2 - 1) \cdot a = 0$.

因为 $a \neq 0$, 根据整数乘法的性质, 有 $q_1 \cdot q_2 = 1$.

而 q_1, q_2 都是整数, 所以 $q_1 = q_2 = \pm 1$. 进而, $a = \pm b$.

目录

1 整除　欧几里德除法　整数表示
- 整除的概念
- 素数及其平凡判别
- Eratoshenes 筛法
- 欧几里德除法
- 整数 b 进制表示

定义 1.1.2

设 $n \neq 0, \pm 1$. 如果除了显然的因数 ± 1 和 $\pm n$ 外, n 没有其他因数, 那么 n 叫做 **素数** (或**质数**, 或**不可约数**). 否则, n 叫做**合数**.

定义 1.1.2

设 $n \neq 0, \pm 1$. 如果除了显然的因数 ± 1 和 $\pm n$ 外, n 没有其他因数, 那么 n 叫做 **素数** (或**质数**, 或**不可约数**). 否则, n 叫做**合数**.

注：当 $n \neq 0, \pm 1$ 时, n 和 $-n$ 同为素数或合数. 因此, 若没有特别声明, 素数总是指正整数, 通常写成 p.

定义 1.1.2

设 $n \neq 0, \pm 1$. 如果除了显然的因数 ± 1 和 $\pm n$ 外, n 没有其他因数, 那么 n 叫做 **素数** (或**质数**, 或**不可约数**). 否则, n 叫做**合数**.

注：当 $n \neq 0, \pm 1$ 时, n 和 $-n$ 同为素数或合数. 因此, 若没有特别声明, 素数总是指正整数, 通常写成 p.

例 1.1.7　整数 $2, 3, 5, 7, 11$ 都是素数; 而整数 $4, 6, 8, 9, 10, 12$ 都是合数.

定义 1.1.2

设 $n \neq 0, \pm 1$. 如果除了显然的因数 ± 1 和 $\pm n$ 外, n 没有其他因数, 那么 n 叫做 **素数** (或**质数**, 或**不可约数**). 否则, n 叫做**合数**.

注：当 $n \neq 0, \pm 1$ 时, n 和 $-n$ 同为素数或合数. 因此, 若没有特别声明, 素数总是指正整数, 通常写成 p.

例 1.1.7　整数 $2, 3, 5, 7, 11$ 都是素数; 而整数 $4, 6, 8, 9, 10, 12$ 都是合数.

定理 1.1.6

设 n 是一个正合数, p 是 n 的一个大于 1 的最小正因数, 则 p 一定是素数, 且 $p \leqslant \sqrt{n}$.

定义 1.1.2

设 $n \neq 0, \pm 1$. 如果除了显然的因数 ± 1 和 $\pm n$ 外, n 没有其他因数, 那么 n 叫做 **素数** (或**质数**, 或**不可约数**). 否则, n 叫做**合数**.

注：当 $n \neq 0, \pm 1$ 时, n 和 $-n$ 同为素数或合数. 因此, 若没有特别声明, 素数总是指正整数, 通常写成 p.

例 1.1.7　整数 $2, 3, 5, 7, 11$ 都是素数; 而整数 $4, 6, 8, 9, 10, 12$ 都是合数.

定理 1.1.6

设 n 是一个正合数, p 是 n 的一个大于 1 的最小正因数, 则 p 一定是素数, 且 $p \leqslant \sqrt{n}$.

证：若 p 不是素数, 则存在整数 $q, 1 < q < p$, 使得 $q \mid p$. 但 $p \mid n$, 根据定理 1.1.1, 有 $q \mid n$. 这与 p 是 n 的最小正因数矛盾. 所以, p 是素数.

因为 n 是合数, 所以存在整数 n_1 使得 $n = n_1 \cdot p, 1 < p \leqslant n_1 < n$.

因此, $p^2 \leqslant n$. 故 $p \leqslant \sqrt{n}$.

定理 1.1.6

素数有无穷多个.

定理 1.1.6

素数有无穷多个.

证：反证法. 假设只有有限个素数 $p_1, p_2, \cdots, p_k$. 考虑整数

$$n = p_1 \cdot p_2 \cdots p_k + 1.$$

因为 $n > p_i, i = 1, \cdots, k$, 所以 n 一定是合数 (因为素数有限, n 又不是有限个素数中的一个). 根据定理 1.1.5, n 的大于 1 的最小正因数 p 是素数. 因此, p 是 $p_1, p_2, \cdots, p_k$ 中的某一个, 即存在 $j, 1 \leqslant j \leqslant k$, 使得 $p = p_j$. 根据定理 1.1.2, 有

$$p \mid n - (p_1 \cdots p_{j-1} \cdot p_{j+1} \cdots p_k) \cdot p_j, \text{ 即 } p \mid 1.$$

这是不可能的. 故存在无穷多个素数.

设 $\pi(x)$ 表示不超过 x 的素数个数, 即

$$\pi(x) = \sum_{p \leqslant x} 1$$

是素数集的函数.

根据定理 1.1.6, 存在无穷个素数, 这就是说, $\pi(x)$ 随 x 趋于无穷. 但人们希望知道 $\pi(x)$ 的具体公式. 为此, 先给出一个基础性结论.

设 $\pi(x)$ 表示不超过 x 的素数个数, 即

$$\pi(x)=\sum_{p\leqslant x}1$$

是素数集的函数.

根据定理 1.1.6, 存在无穷个素数, 这就是说, $\pi(x)$ 随 x 趋于无穷. 但人们希望知道 $\pi(x)$ 的具体公式. 为此, 先给出一个基础性结论.

定理 1.1.7 (契比谢夫不等式)

设 $x\geqslant 2$, 则有 $\frac{\ln 2}{3}\frac{x}{\ln x}<\pi(x)<6\ln 2\frac{x}{\ln x}$ 和

$$\frac{1}{6\ln 2}n\ln n<p_n<\frac{8}{\ln 2}n\ln n, n\geq 2.$$

其中 p_n 是第 n 个素数.

设 $\pi(x)$ 表示不超过 x 的素数个数, 即

$$\pi(x)=\sum_{p\leqslant x}1$$

是素数集的函数.

根据定理 1.1.6, 存在无穷个素数, 这就是说, $\pi(x)$ 随 x 趋于无穷. 但人们希望知道 $\pi(x)$ 的具体公式. 为此, 先给出一个基础性结论.

定理 1.1.7 (契比谢夫不等式)

设 $x\geqslant 2$, 则有 $\frac{\ln 2}{3}\frac{x}{\ln x}<\pi(x)<6\ln 2\frac{x}{\ln x}$ 和

$$\frac{1}{6\ln 2}n\ln n<p_n<\frac{8}{\ln 2}n\ln n, n\geq 2.$$

其中 p_n 是第 n 个素数.

定理 1.1.8 (素数定理)

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\ln x}}=1.$$

在了解素数个数的相关结论之后, 根据定理 1.1.5, 我们还可以得到一个整数为素数的平凡判别法则.

定理 1.1.9 (素数的平凡判别)

设 n 是正整数, 如果对于所有的素数 $p \leqslant \sqrt{n}$, 都有 $p \nmid n$, 则 n 一定是素数.

在了解素数个数的相关结论之后, 根据定理 1.1.5, 我们还可以得到一个整数为素数的平凡判别法则.

定理 1.1.9 (素数的平凡判别)

设 n 是正整数, 如果对于所有的素数 $p \leqslant \sqrt{n}$, 都有 $p \nmid n$, 则 n 一定是素数.

例 1.1.8　证明 $N = 89$ 是素数.

在了解素数个数的相关结论之后, 根据定理 1.1.5, 我们还可以得到一个整数为素数的平凡判别法则.

定理 1.1.9 (素数的平凡判别)

设 n 是正整数, 如果对于所有的素数 $p \leqslant \sqrt{n}$, 都有 $p \nmid n$, 则 n 一定是素数.

例 1.1.8　证明 $N = 89$ 是素数.

证：先求出所有的 p, 使得 $p \leq \sqrt{89}$，并检验 $p \nmid 89$.

1）所有小于 $\sqrt{89}$ 的素数 p 为 $2, 3, 5, 7$.

2）$p \nmid 89$, 因为 $p = 2, 3, 5, 7$ 的倍数都不是 89.

所以, 89 是素数.

目录

1 整除　欧几里德除法　整数表示
- 整除的概念
- 素数及其平凡判别
- Eratoshenes 筛法
- 欧几里德除法
- 整数 b 进制表示

为了更好地描述数学概念和问题，我们引入数学符号 $[x]$:

设 x 是一个实数, $[x]$ 表示实数 x 的整数部分是小于或等于 x 的最大整数. 这时，我们有 $[x] \leq x < [x] + 1$.

为了更好地描述数学概念和问题，我们引入数学符号 $[x]$:

设 x 是一个实数, $[x]$ 表示实数 x 的整数部分是小于或等于 x 的最大整数. 这时，我们有 $[x] \leq x < [x] + 1$.

例 1.1.9　[9.15]=9, [-9.15]=-10, [9]=9, [-9]=-9.

为了更好地描述数学概念和问题，我们引入数学符号 $[x]$:

设 x 是一个实数, $[x]$ 表示实数 x 的整数部分是小于或等于 x 的最大整数. 这时，我们有 $[x] \leq x < [x] + 1$.

例 1.1.9　[9.15]=9, [-9.15]=-10, [9]=9, [-9]=-9.

根据定理 1.1.9, 我们有一个寻找素数的确定性方法, 通常叫做**厄拉托塞师** (Eratoshenes)**筛法** (简称 E-筛法).

定理 1.1.10 (E-筛法)

输入：任意给定的正整数 N.　输出：所有不超过 N 的素数.

1. 列出 N 整数 $1, \cdots, N$;
2. 从中删除不大于 $\sqrt{N}$ 的所有素数 $p_1, p_2, \cdots, p_k$ 的倍数 (除素数 $p_1, p_2, \cdots, p_k$ 外);
3. 余下的整数 (不包括 1) 就是所要求的不超过 N 的素数.

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

1. 删除 2 的倍数;

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

1. 删除 2 的倍数;

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

1. 删除 2 的倍数;

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3		5		7		~~9~~	
11		13		~~15~~		17		19	
~~21~~		23		25		~~27~~		29	
31		~~33~~		35		37		~~39~~	
41		43		~~45~~		47		49	
~~51~~		53		55		~~57~~		59	
61		~~63~~		65		67		~~69~~	
71		73		~~75~~		77		79	
~~81~~		83		85		~~87~~		89	
91		~~93~~		95		97		~~99~~	

1. 删除 2 的倍数;
2. 删除 3 的倍数;

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

1. 删除 2 的倍数;
2. 删除 3 的倍数;

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3		5		7			
11		13				17		19	
		23		~~25~~				29	
31				~~35~~		37			
41		43				47		49	
		53		~~55~~				59	
61				~~65~~		67			
71		73				77		79	
		83		~~85~~				89	
91				~~95~~		97			

1. 删除 2 的倍数;
2. 删除 3 的倍数;
3. 删除 5 的倍数;

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

1. 删除 2 的倍数;
2. 删除 3 的倍数;
3. 删除 5 的倍数;

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		~~49~~	
		53						59	
61						67			
71		73				~~77~~		79	
		83						89	
~~91~~						97			

1. 删除 2 的倍数;
2. 删除 3 的倍数;
3. 删除 5 的倍数;
4. 删除 7 的倍数.

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

1	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

1. 删除 2 的倍数;
2. 删除 3 的倍数;
3. 删除 5 的倍数;
4. 删除 7 的倍数.

例 1.1.10　求出所有不超过 $N = 100$ 的素数.

解：因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 那么依次删除 2, 3, 5, 7 的倍数, 余下的整数 (不包括 1) 即为所求.

~~1~~	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

1. 删除 2 的倍数;
2. 删除 3 的倍数;
3. 删除 5 的倍数;
4. 删除 7 的倍数.

余下的整数 (不包括 1) 就是所要求的不超过 100 的素数, 即 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

目录

1 整除　欧几里德除法　整数表示
- 整除的概念
- 素数及其平凡判别
- Eratoshenes 筛法
- 欧几里德除法
- 整数 b 进制表示

定理 1.1.11 (欧几里德除法 – 最小非负余数)

设 a, b 是两个整数, 其中 $b > 0$, 则存在唯一的整数 q, r 使得

$$a = q \cdot b + r,\ 0 \leqslant r < b. \tag{1.1.2}$$

定理 1.1.11 (欧几里德除法 – 最小非负余数)

设 a, b 是两个整数, 其中 $b > 0$, 则存在唯一的整数 q, r 使得

$$a = q \cdot b + r,\ 0 \leqslant r < b. \tag{1.1.2}$$

证：(存在性) 考虑一个整数序列

$$\cdots, -3 \cdot b, -2 \cdot b, -b, 0, b, 2 \cdot b, 3 \cdot b, \cdots,$$

它们将实数轴分成长度为 b 的区间, 而 a 必定落在其中的一个区间中. 因此存在一个整数 q 使得 $q \cdot b \leqslant a < (q+1) \cdot b$. 令 $r = a - q \cdot b$, 则有 $a = q \cdot b + r,\ 0 \leqslant r < b$.

定理 1.1.11 (欧几里德除法 – 最小非负余数)

设 a, b 是两个整数, 其中 $b > 0$, 则存在唯一的整数 q, r 使得

$$a = q \cdot b + r,\ 0 \leqslant r < b. \tag{1.1.2}$$

证：(存在性) 考虑一个整数序列

$$\cdots, -3 \cdot b, -2 \cdot b, -b, 0, b, 2 \cdot b, 3 \cdot b, \cdots,$$

它们将实数轴分成长度为 b 的区间, 而 a 必定落在其中的一个区间中. 因此存在一个整数 q 使得 $q \cdot b \leqslant a < (q+1) \cdot b$. 令 $r = a - q \cdot b$, 则有 $a = q \cdot b + r,\ 0 \leqslant r < b$.

(唯一性) 如果分别有整数 q, r 和 q_1, r_1 满足式 (1.1.2), 则

$$a = q \cdot b + r,\ 0 \leqslant r < b.$$

$$a = q_1 \cdot b + r_1,\ 0 \leqslant r_1 < b.$$

两式相减得 $(q - q_1) \cdot b = -(r - r_1)$. 当 $q \neq q_1$ 时, 左边的绝对值 $\geqslant b$, 而右边的绝对值 $< b$, 这是不可能的, 故 $q = q_1, r = r_1$.

定义 1.1.3

在 $a = q \cdot b + r,\ 0 \leqslant r < b$ 式中，q 叫做 a 被 b 除所得的**不完全商**，r 叫做 a 被 b 除所得的**余数**.

定义 1.1.3

在 $a = q \cdot b + r,\ 0 \leqslant r < b$ 式中，q 叫做 a 被 b 除所得的**不完全商**，r 叫做 a 被 b 除所得的**余数**.

例 1.1.11　证明 $N = 2027$ 为素数.

证: 小于等于 $\sqrt{2027} < 46$ 的所有素数为 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 故依次用这些素数去试除:

$$2027 = 1013 \cdot 2 + 1, \quad 2027 = 675 \cdot 3 + 2, \quad 2027 = 405 \cdot 5 + 2,$$

$$2027 = 289 \cdot 7 + 4, \quad 2027 = 184 \cdot 11 + 3, \quad 2027 = 155 \cdot 13 + 12,$$

$$2027 = 119 \cdot 17 + 4, \quad 2027 = 106 \cdot 19 + 13, \quad 2027 = 88 \cdot 23 + 3,$$

$$2027 = 69 \cdot 29 + 26, \quad 2027 = 65 \cdot 31 + 12, \quad 2027 = 54 \cdot 37 + 29,$$

$$2027 = 49 \cdot 41 + 18, \quad 2027 = 47 \cdot 43 + 6.$$

所以, 小于等于 $\sqrt{2027}$ 的所有素数都不能整除 2027, 根据定理 1.1.9, $N = 2027$ 为素数.

定理 1.1.12 (欧几里德除法 – 一般余数)

设 a, b 是两个整数, 其中 $b > 0$, 则对任意的整数 c, 存在唯一的整数 q, r 使得

$$a = q \cdot b + r,\ c \leqslant r < b + c. \tag{1.1.3}$$

定理 1.1.12 (欧几里德除法 – 一般余数)

设 a, b 是两个整数, 其中 $b > 0$, 则对任意的整数 c, 存在唯一的整数 q, r 使得

$$a = q \cdot b + r,\ c \leqslant r < b + c. \tag{1.1.3}$$

证：(存在性) 考虑一个整数序列

$$\cdots, -3 \cdot b + c, -2 \cdot b + c, -b + c, c, b + c, 2 \cdot b + c, 3 \cdot b + c, \cdots,$$

它们将实数轴分成长度为 b 的区间, 而 a 必定落在其中的一个区间中. 因此存在一个整数 q 使得 $q \cdot b + c \leqslant a < (q + 1) \cdot b + c$. 令 $r = a - q \cdot b$, 则有 $a = q \cdot b + r,\ c \leqslant r < b + c$.

定理 1.1.12 (欧几里德除法 – 一般余数)

设 a, b 是两个整数, 其中 $b > 0$, 则对任意的整数 c, 存在唯一的整数 q, r 使得

$$a = q \cdot b + r,\ c \leqslant r < b + c. \tag{1.1.3}$$

证：(存在性) 考虑一个整数序列

$$\cdots, -3 \cdot b + c, -2 \cdot b + c, -b + c, c, b + c, 2 \cdot b + c, 3 \cdot b + c, \cdots,$$

它们将实数轴分成长度为 b 的区间, 而 a 必定落在其中的一个区间中. 因此存在一个整数 q 使得 $q \cdot b + c \leqslant a < (q + 1) \cdot b + c$. 令 $r = a - q \cdot b$, 则有 $a = q \cdot b + r,\ c \leqslant r < b + c$.

(唯一性) 如果分别有整数 q, r 和 q_1, r_1 满足式 (1.1.3), 则

$$a = q \cdot b + r,\ c \leqslant r < b + c.$$

$$a = q_1 \cdot b + r_1,\ c \leqslant r_1 < b + c.$$

两式相减得 $(q - q_1) \cdot b = -(r - r_1)$. 当 $q \neq q_1$ 时, 左边的绝对值 $\geqslant b$, 而右边的绝对值 $< b$, 这是不可能的, 故 $q = q_1, r = r_1$.

(1) 当 $c = 0$ 时, 有 $b + c = b$ 及 $0 \leqslant r \leqslant b - 1 < b$.

这时 r 叫做**最小非负余数**.

(1) 当 $c=0$ 时, 有 $b+c=b$ 及 $0 \leqslant r \leqslant b-1<b$.

这时 r 叫做**最小非负余数**.

(2) 当 $c=1$ 时, 有 $b+c=b+1$ 及 $1 \leqslant r \leqslant b$. 这时 r 叫做**最小正余数**.

(1) 当 $c=0$ 时, 有 $b+c=b$ 及 $0 \leqslant r \leqslant b-1<b$.

这时 r 叫做**最小非负余数**.

(2) 当 $c=1$ 时, 有 $b+c=b+1$ 及 $1 \leqslant r \leqslant b$. 这时 r 叫做**最小正余数**.

(3) 当 $c=-b+1$ 时, 有 $b+c=1$ 及 $-b<-b+1 \leqslant r \leqslant 0$.

这时 r 叫做**最大非正余数**.

(1) 当 $c=0$ 时, 有 $b+c=b$ 及 $0 \leqslant r \leqslant b-1<b$.

这时 r 叫做**最小非负余数**.

(2) 当 $c=1$ 时, 有 $b+c=b+1$ 及 $1 \leqslant r \leqslant b$. 这时 r 叫做**最小正余数**.

(3) 当 $c=-b+1$ 时, 有 $b+c=1$ 及 $-b<-b+1 \leqslant r \leqslant 0$.

这时 r 叫做**最大非正余数**.

(4) 当 $c=-b$ 时, 有 $b+c=0$ 及 $-b \leqslant r \leqslant -1<0$.

这时 r 叫做**最大负余数**.

(1) 当 $c=0$ 时, 有 $b+c=b$ 及 $0 \leqslant r \leqslant b-1<b$.

这时 r 叫做**最小非负余数**.

(2) 当 $c=1$ 时, 有 $b+c=b+1$ 及 $1 \leqslant r \leqslant b$. 这时 r 叫做**最小正余数**.

(3) 当 $c=-b+1$ 时, 有 $b+c=1$ 及 $-b<-b+1 \leqslant r \leqslant 0$.

这时 r 叫做**最大非正余数**.

(4) 当 $c=-b$ 时, 有 $b+c=0$ 及 $-b \leqslant r \leqslant -1<0$.

这时 r 叫做**最大负余数**.

(5) ① 当 b 为偶数, $c=-\frac{b}{2}$ 时, 有 $b+c=\frac{b}{2}$ 及 $-\frac{b}{2} \leqslant r \leqslant \frac{b-2}{2}<\frac{b}{2}$;

② 当 b 为偶数, $c=-\frac{b-2}{2}$ 时,

有 $b+c=\frac{b+2}{2}$ 及 $-\frac{b}{2}<-\frac{b-2}{2} \leqslant r \leqslant \frac{b}{2}$;

③ 当 b 为奇数, $c=-\frac{b-1}{2}$ 时,

有 $b+c=\frac{b+1}{2}$ 及 $-\frac{b}{2}<-\frac{b-1}{2} \leqslant r \leqslant \frac{b-1}{2}<\frac{b}{2}$;

总之, 有 $-\frac{b}{2} \leqslant r<\frac{b}{2}$ 或 $-\frac{b}{2}<r \leqslant \frac{b}{2}$. 这时 r 叫做**绝对值最小余数**.

例 1.1.12　设 $b = 7$, 则

$r = 0, 1, 2, 3, 4, 5, 6$ 为最小非负余数.

$r = 1, 2, 3, 4, 5, 6, 7$ 为最小正余数.

$r = 0, -1, -2, -3, -4, -5, -6$ 为最大非正余数.

$r = -1, -2, -3, -4, -5, -6, -7$ 为最大负余数.

$r = -3, -2, -1, 0, 1, 2, 3$ 为绝对值最小余数.

例 1.1.12　设 $b = 7$, 则

$r = 0, 1, 2, 3, 4, 5, 6$ 为最小非负余数.

$r = 1, 2, 3, 4, 5, 6, 7$ 为最小正余数.

$r = 0, -1, -2, -3, -4, -5, -6$ 为最大非正余数.

$r = -1, -2, -3, -4, -5, -6, -7$ 为最大负余数.

$r = -3, -2, -1, 0, 1, 2, 3$ 为绝对值最小余数.

例 1.1.13　设 $b = 12$, 则

$r = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ 为最小非负余数.

$r = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ 为最小正余数.

$r = 0, -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11$ 为最大非正余数.

$r = -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, -12$ 为最大负余数.

$r = -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5$ 或

$r = -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6$ 为绝对值最小余数.

目录

1. 整除　欧几里德除法　整数表示
   - 整除的概念
   - 素数及其平凡判别
   - Eratoshenes 筛法
   - 欧几里德除法
   - 整数 b 进制表示

平时遇到的整数通常是以十进制表示的. 中国是世界上最早采用十进制的国家, 春秋战国时期已经普遍使用的算筹就严格遵循十进位制, 见《孙子算经》. 但在计算机中, 需要用二进制、八进制或十六进制表示. 为此, 考虑一般的 b 进制. 运用欧几里德除法, 可得到:

平时遇到的整数通常是以十进制表示的. 中国是世界上最早采用十进制的国家, 春秋战国时期已经普遍使用的算筹就严格遵循十进位制, 见《孙子算经》. 但在计算机中, 需要用二进制、八进制或十六进制表示. 为此, 考虑一般的 b 进制. 运用欧几里德除法, 可得到:

定理 1.1.13

设 b 是大于 1 的整数, 则每个正整数 n 可唯一地表示成

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

其中 a_i 是整数, $0 \leqslant a_i \leqslant b-1, i = 1, \cdots, k$, 且首项系数 $a_k \neq 0$.

平时遇到的整数通常是以十进制表示的. 中国是世界上最早采用十进制的国家, 春秋战国时期已经普遍使用的算筹就严格遵循十进位制, 见《孙子算经》. 但在计算机中, 需要用二进制、八进制或十六进制表示. 为此, 考虑一般的 b 进制. 运用欧几里德除法, 可得到:

定理 1.1.13

设 b 是大于 1 的整数, 则每个正整数 n 可唯一地表示成

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

其中 a_i 是整数, $0 \leqslant a_i \leqslant b-1, i = 1, \cdots, k$, 且首项系数 $a_k \neq 0$.

证明思路：逐次运用欧几里得除法得到

$$n = q_0 b + a_0,\ 0 \leqslant a_0 \leqslant b-1;$$

$$q_i = q_{i+1} + a_{i+1},\ 0 \leqslant a_i \leqslant b-1,\ i = 0, 1, \cdots, k-1.$$

直到 $a_{k+1} = 0$. 再依次代入 $n = q_0 b + a_0$ 即得 n 的表达式.

若有两种表示, 则两式相减后可得 $a_i - a_i^* = 0, i = 0, \cdots, k$, 故 n 的表达式唯一.

如果展开式 $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$, 其中 a_i 是整数, $0 \leqslant a_i \leqslant b-1, i = 1, \cdots, k-1$, 且首项系数 $a_k \neq 0$, 则称符号 $n = (a_k a_{k-1} \cdots a_1 a_0)_b$ 为整数 n 的 b **进制表示**.

如果展开式 $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$, 其中 a_i 是整数, $0 \leqslant a_i \leqslant b-1, i = 1, \cdots, k-1$, 且首项系数 $a_k \neq 0$, 则称符号 $n = (a_k a_{k-1} \cdots a_1 a_0)_b$ 为整数 n 的 b **进制表示**.

当 $b = 2$ 时, 系数 a_i 为 0 或 1, 因此有

推论 1.1.3

每个正整数都可以表示成不同的 2 的方幂的和.

如果展开式 $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$, 其中 a_i 是整数, $0 \leqslant a_i \leqslant b-1, i = 1, \cdots, k-1$, 且首项系数 $a_k \neq 0$, 则称符号 $n = (a_k a_{k-1} \cdots a_1 a_0)_b$ 为整数 n 的 b **进制表示**.

当 $b = 2$ 时, 系数 a_i 为 0 或 1, 因此有

推论 1.1.3

每个正整数都可以表示成不同的 2 的方幂的和.

例 1.1.14　将整数 404 表示为二进制.

解：逐次运用欧几里德除法, 我们有

$$404 = 2 \cdot 202 + 0, \quad 202 = 2 \cdot 101 + 0, \quad 101 = 2 \cdot 50 + 1,$$
$$50 = 2 \cdot 25 + 0, \quad 25 = 2 \cdot 12 + 1, \quad 12 = 2 \cdot 6 + 0,$$
$$6 = 2 \cdot 3 + 0, \quad 3 = 2 \cdot 1 + 1, \quad 1 = 2 \cdot 0 + 1.$$

因此, $404 = (110010100)_2$, 或者

$$404 = 1 \cdot 2^8 + 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0.$$

计算机也常用八进制, 或十六进制, 或六十四进制等. 在十六进制中, 我们用 $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$ 分别表示 $0, 1, \cdots, 15$ 共 16 个数, 其中 A, B, C, D, E, F 分别对应于 $10, 11, 12, 13, 14, 15$.

计算机也常用八进制, 或十六进制, 或六十四进制等. 在十六进制中, 我们用 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F 分别表示 $0, 1, \cdots, 15$ 共 16 个数, 其中 A, B, C, D, E, F 分别对应于 10, 11, 12, 13, 14, 15.

例 1.1.15　转换十六进制 $(ABCD)_{16}$ 为十进制.

$$(ABCD)_{16} = 10 \cdot 16^3 + 11 \cdot 16^2 + 12 \cdot 16 + 13 = (43981)_{10}.$$

计算机也常用八进制, 或十六进制, 或六十四进制等. 在十六进制中, 我们用 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F 分别表示 $0, 1, \cdots, 15$ 共 16 个数, 其中 A, B, C, D, E, F 分别对应于 10, 11, 12, 13, 14, 15.

例 1.1.15　转换十六进制 $(ABCD)_{16}$ 为十进制.

$$(ABCD)_{16} = 10 \cdot 16^3 + 11 \cdot 16^2 + 12 \cdot 16 + 13 = (43981)_{10}.$$

注：当 $b = 100, 2^{15} = 32768, 10^8$ 或 $2^{32} = 4294967296$ 时, n 可分别表示为不同进制的多重精度整数, 并进一步用于基于“大整数”的密码系统.

计算机也常用八进制, 或十六进制, 或六十四进制等. 在十六进制中, 我们用 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F 分别表示 $0, 1, \cdots, 15$ 共 16 个数, 其中 A, B, C, D, E, F 分别对应于 10, 11, 12, 13, 14, 15.

例 1.1.15　转换十六进制 $(ABCD)_{16}$ 为十进制.

$$(ABCD)_{16} = 10 \cdot 16^3 + 11 \cdot 16^2 + 12 \cdot 16 + 13 = (43981)_{10}.$$

注：当 $b = 100, 2^{15} = 32768, 10^8$ 或 $2^{32} = 4294967296$ 时, n 可分别表示为不同进制的多重精度整数, 并进一步用于基于“大整数”的密码系统.

为了方便各进制之间的转换, 并提高转换效率, 我们可以预先制作一个换算表, 再根据换算表作转换. 下图就是二进制、八进制、十进制和十六进制之间的换算表.

二进制、八进制、十进制、十六进制换算表

十进制	二进制	八进制	十六进制	十进制	二进制	八进制	十六进制
0	0000	00	0	8	1000	10	8
1	0001	01	1	9	1001	11	9
2	0010	02	2	10	1010	12	A
3	0011	03	3	11	1011	13	B
4	0100	04	4	12	1100	14	C
5	0101	05	5	13	1101	15	D
6	0110	06	6	14	1110	16	E
7	0111	07	7	15	1111	17	F

例 1.1.16　转换十六进制 $(ABCD)_{16}$ 为二进制.

解: 由上述换算表可得

$$A = (1010)_2, B = (1011)_2, C = (1100)_2, D = (1101)_2.$$

从而 $(ABCD)_{16} = (1010101111001101)_2$.

例 1.1.16　转换十六进制 $(ABCD)_{16}$ 为二进制.

解: 由上述换算表可得

$$A = (1010)_2, B = (1011)_2, C = (1100)_2, D = (1101)_2.$$

从而 $(ABCD)_{16} = (1010101111001101)_2$.

例 1.1.17　转换二进制 $(110111101111)_2$ 为十六进制数.

解: 由上述换算表可得到 $(1111)_2 = F$, $(1110)_2 = E$, $(1101)_2 = D$, 从而 $(110111101111)_2 = DEF$.

例 1.1.16　转换十六进制 $(ABCD)_{16}$ 为二进制.

解: 由上述换算表可得

$$A = (1010)_2, B = (1011)_2, C = (1100)_2, D = (1101)_2.$$

从而 $(ABCD)_{16} = (1010101111001101)_2$.

例 1.1.17　转换二进制 $(110111101111)_2$ 为十六进制数.

解: 由上述换算表可得到 $(1111)_2 = F$, $(1110)_2 = E$, $(1101)_2 = D$, 从而 $(110111101111)_2 = DEF$.

因二进制的转换比十六进制要容易些, 故可以先将数作二进制表示, 再运用二进制与十六进制之间的换算表, 将二进制转换成十六进制.

例 1.1.16　转换十六进制 $(ABCD)_{16}$ 为二进制.

解: 由上述换算表可得

$$A = (1010)_2, B = (1011)_2, C = (1100)_2, D = (1101)_2.$$

从而 $(ABCD)_{16} = (1010101111001101)_2$.

例 1.1.17　转换二进制 $(110111101111)_2$ 为十六进制数.

解: 由上述换算表可得到 $(1111)_2 = F$, $(1110)_2 = E$, $(1101)_2 = D$, 从而 $(110111101111)_2 = DEF$.

因二进制的转换比十六进制要容易些, 故可以先将数作二进制表示, 再运用二进制与十六进制之间的换算表, 将二进制转换成十六进制.

例 1.1.18　表示整数 404 为十六进制.

解: 根据例 1.1.14, 我们有 $404 = (110010100)_2$.

查换算表得到 $(0100)_2 = 4$, $(1001)_2 = 9$, $(0001)_2 = 1$.

故 $404 = 1 \cdot 16^2 + 9 \cdot 16 + 4 = (194)_{16}$.

本课作业

1. 证明: 若 a 是整数, 则 $3 \mid a^3 - a$.

2. 证明: 若三个大于 10 的素数成等差数列, 其公差为 d, 则 $6 \mid d$.

3. 有一个 2024 位的数 A 能被 9 整除，它的各位数字和为 a, a 的各位数字和为 b, b 的各位数字和为 c, 求 c 等于多少？

4. 是否存在这样的整数 a, b, c, 使得 $a \mid bc$, 但 $a \nmid b, a \nmid c$, 若有, 举两例说明; 若无, 给出证明.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn