网络空间安全学院

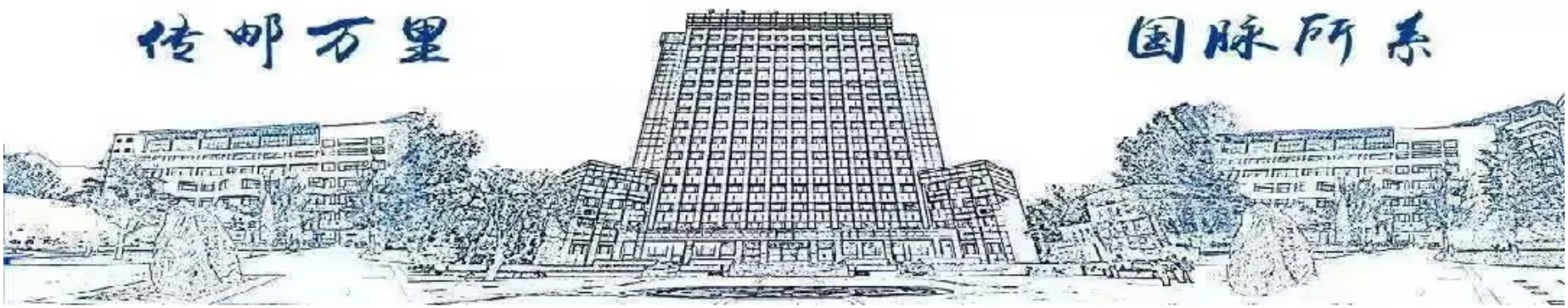
School of Cyberspace Security, BUPT

信息安全数学基础

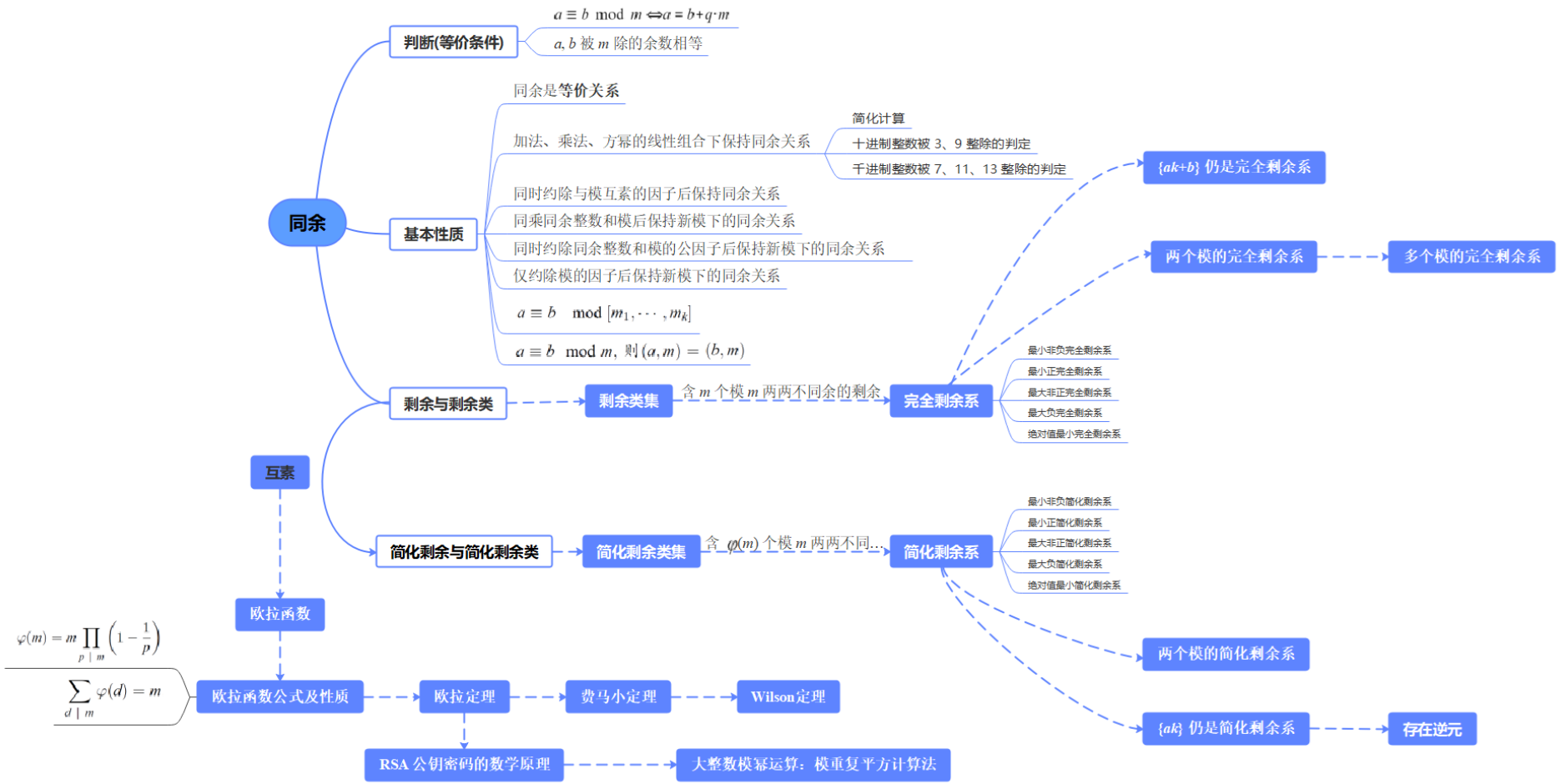
—— 同余方程 (1)

信数课题组

北京邮电大学



上次课回顾


同余
判断(等价条件)
$a \equiv b \mod m \Leftrightarrow a = b+q\cdot m$
a, b 被 m 除的余数相等
基本性质
同余是等价关系
加法、乘法、方幂的线性组合下保持同余关系
简化计算
十进制整数被 3、9 整除的判定
千进制整数被 7、11、13 整除的判定
同时约除与模互素的因子后保持同余关系
同乘同余整数和模后保持新模下的同余关系
同时约除同余整数和模的公因子后保持新模下的同余关系
仅约除模的因子后保持新模下的同余关系
$a \equiv b \mod [m_1, \cdots, m_k]$
$a \equiv b \mod m$, 则 $(a, m) = (b, m)$
剩余与剩余类
剩余类集
含 m 个模 m 两两不同余的剩余
完全剩余系
$\{ak+b\}$ 仍是完全剩余系
两个模的完全剩余系
多个模的完全剩余系
最小非负完全剩余系
最小正完全剩余系
最大非正完全剩余系
最大负完全剩余系
绝对值最小完全剩余系
互素
简化剩余与简化剩余类
简化剩余类集
含 $\varphi(m)$ 个模 m 两两不同...
简化剩余系
最小非负简化剩余系
最小正简化剩余系
最大非正简化剩余系
最大负简化剩余系
绝对值最小简化剩余系
两个模的简化剩余系
$\{ak\}$ 仍是简化剩余系
存在逆元
欧拉函数
$\varphi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$
$\sum_{d \mid m} \varphi(d) = m$
欧拉函数公式及性质
欧拉定理
费马小定理
Wilson定理
RSA 公钥密码的数学原理
大整数模幂运算：模重复平方计算法

目录

目录

定义 3.1.1

(i) 设 m 是一个正整数, $f(x)$ 为多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$, 其中 a_i 是整数, $i=0,1,\cdots,n$, 则 $f(x)\equiv 0 \mod m$ 叫做模 m **同余方程**. 若 $a_n\not\equiv 0 \mod m$, 则 n 叫做 $f(x)$ 的**次数**, 记作 $\deg f$. 此时, 该式又叫做模 m 的 n **次同余方程**, $a_n \mod m$ 称为其**首项系数**.

(ii) 如果整数 a 使得 $f(a)\equiv 0 \mod m$ 成立, 则 a 叫做同余方程 $f(x)\equiv 0 \mod m$ 的 **解**. 此时, 满足 $x\equiv a \mod m$ 的所有整数都使得同余方程 $f(x)\equiv 0 \mod m$ 成立, 即 a 所在的剩余类 $C_a=\{c\in\mathbb{Z}\mid c\equiv a \mod m\}$ 中的每个剩余都使得同余方程 $f(x)\equiv 0 \mod m$ 成立. 因此, 同余方程 $f(x)\equiv 0 \mod m$ 的解 a 通常写成 $x\equiv a \mod m$.

(iii) 在模 m 的完全剩余系中, 使得同余方程成立的剩余个数叫做同余方程的 **解数**.

例 3.1.1 同余方程 $2x^4 + x^3 + 2 \equiv 0 \mod 7$ 是首项系数为 2 的模 7 的四次同余方程. 而 $x \equiv 2 \mod 7$ 是该同余方程的解. 事实上, 我们有

$$2 \cdot 2^4 + 2^3 + 2 \equiv 4 + 1 + 2 \equiv 0 \mod 7.$$

而其他剩余均不满足, 故解数为 1.

例 3.1.1 同余方程 $2x^4 + x^3 + 2 \equiv 0 \mod 7$ 是首项系数为 2 的模 7 的四次同余方程. 而 $x \equiv 2 \mod 7$ 是该同余方程的解. 事实上, 我们有

$$2 \cdot 2^4 + 2^3 + 2 \equiv 4 + 1 + 2 \equiv 0 \mod 7.$$

而其他剩余均不满足, 故解数为 1.

注: 如例 3.1.1 所示, 当模 m 比较小时, 我们可以依次将剩余代入验算是否满足来求解同余方程. 但对于一般的模 m, 我们需要探索新的求解思路. 下面我们将针对一次、二次和高次同余方程, 分别介绍其求解及相关结果.

目录

首先, 考虑常数项为 1 的一次同余方程的求解, 我们有下面的结果.

定理 3.1.1

设 m 是一个正整数, a 是满足 $m \nmid a$ 的整数, 则一次同余方程

$$ax \equiv 1 \mod m$$

有解的充要条件是 $(a, m) = 1$. 而且, 当同余方程有解时, 其解是唯一的.

首先, 考虑常数项为 1 的一次同余方程的求解, 我们有下面的结果.

定理 3.1.1

设 m 是一个正整数, a 是满足 $m \nmid a$ 的整数, 则一次同余方程

$$ax \equiv 1 \mod m$$

有解的充要条件是 $(a, m) = 1$. 而且, 当同余方程有解时, 其解是唯一的.

证：充分性. (存在性) 因为 $(a, m) = 1$, 根据广义欧几里德除法或贝祖等式 (定理 1.2.4), 可得到整数 s, t 使得 $s \cdot a + t \cdot m = (a, m) = 1$.

因此, $x = s \mod m$ 是同余方程 $ax \equiv 1 \mod m$ 的解.

首先, 考虑常数项为 1 的一次同余方程的求解, 我们有下面的结果.

定理 3.1.1

设 m 是一个正整数, a 是满足 $m \nmid a$ 的整数, 则一次同余方程

$$ax \equiv 1 \mod m$$

有解的充要条件是 $(a, m) = 1$. 而且, 当同余方程有解时, 其解是唯一的.

证：充分性. (存在性) 因为 $(a, m) = 1$, 根据广义欧几里德除法或贝祖等式 (定理 1.2.4), 可得到整数 s, t 使得 $s \cdot a + t \cdot m = (a, m) = 1$.

因此, $x = s \mod m$ 是同余方程 $ax \equiv 1 \mod m$ 的解.

(唯一性) 若还有解 x', 即 $ax' \equiv 1 \mod m$, 则有 $a(x - x') \equiv 0 \mod m$. 而 $(a, m) = 1$, 所以 $x \equiv x' \mod m$, 即解是唯一的.

首先, 考虑常数项为 1 的一次同余方程的求解, 我们有下面的结果.

定理 3.1.1

设 m 是一个正整数, a 是满足 $m \nmid a$ 的整数, 则一次同余方程

$$ax \equiv 1 \mod m$$

有解的充要条件是 $(a, m) = 1$. 而且, 当同余方程有解时, 其解是唯一的.

证：充分性. (存在性) 因为 $(a, m) = 1$, 根据广义欧几里德除法或贝祖等式 (定理 1.2.4), 可得到整数 s, t 使得 $s \cdot a + t \cdot m = (a, m) = 1$.

因此, $x = s \mod m$ 是同余方程 $ax \equiv 1 \mod m$ 的解.

(唯一性) 若还有解 x', 即 $ax' \equiv 1 \mod m$, 则有 $a(x - x') \equiv 0 \mod m$. 而 $(a, m) = 1$, 所以 $x \equiv x' \mod m$, 即解是唯一的.

必要性. 若同余方程 $ax \equiv 1 \mod m$ 有解, 不妨设为 $x \equiv x_0 \mod m$, 则存在整数 q, 使得 $a \cdot x_0 = 1 + q \cdot m$. 根据定理 1.2.5, 有 $(a, m) = 1$.

定义 3.1.2

设 m 是一个正整数, a 是一个整数. 如果存在整数 a' 使得

$$a \cdot a' \equiv a' \cdot a \equiv 1 \mod m$$

成立, 则 a 叫做模 m **可逆元**. 这时 a' 叫做 a 的模 m **逆元**, 记作 $a' = a^{-1} \mod m$.

定义 3.1.2

设 m 是一个正整数, a 是一个整数. 如果存在整数 a' 使得

$$a \cdot a' \equiv a' \cdot a \equiv 1 \mod m$$

成立, 则 a 叫做模 m **可逆元**. 这时 a' 叫做 a 的模 m **逆元**, 记作 $a' = a^{-1} \mod m$.

注：根据定理 3.1.1, 在模 m 的意义下, a' 是唯一存在的.

定义 3.1.2

设 m 是一个正整数, a 是一个整数. 如果存在整数 a' 使得

$$a \cdot a' \equiv a' \cdot a \equiv 1 \mod m$$

成立, 则 a 叫做模 m **可逆元**. 这时 a' 叫做 a 的模 m **逆元**, 记作 $a' = a^{-1} \mod m$.

注：根据定理 3.1.1, 在模 m 的意义下, a' 是唯一存在的.

现在我们给出模简化剩余的一个等价描述.

定理 3.1.2

设 m 是一个正整数, 则整数 a 是模 m 简化剩余的充要条件是整数 a 是模 m 可逆元.

定义 3.1.2

设 m 是一个正整数, a 是一个整数. 如果存在整数 a' 使得

$$a \cdot a' \equiv a' \cdot a \equiv 1 \mod m$$

成立, 则 a 叫做模 m **可逆元**. 这时 a' 叫做 a 的模 m **逆元**, 记作 $a' = a^{-1} \mod m$.

注：根据定理 3.1.1, 在模 m 的意义下, a' 是唯一存在的.

现在我们给出模简化剩余的一个等价描述.

定理 3.1.2

设 m 是一个正整数, 则整数 a 是模 m 简化剩余的充要条件是整数 a 是模 m 可逆元.

证：必要性. 如果整数 a 是模 m 简化剩余, 则 $(a, m) = 1$.

根据定理 3.1.1, 存在整数 a' 使得 $a \cdot a' \equiv 1 \mod m$.

因此, 由定义 3.1.2 知, a 是模 m 可逆元.

充分性. 如果整数 a 是模 m 可逆元, 则存在整数 a' 使得 $a \cdot a' \equiv 1 \mod m$. 即同余方程 $ax \equiv 1 \mod m$ 有解 $x \equiv a' \mod m$. 根据定理 3.1.1, 有 $(a, m) = 1$. 因此, 整数 a 是模 m 简化剩余.

充分性. 如果整数 a 是模 m 可逆元, 则存在整数 a' 使得 $a \cdot a' \equiv 1 \mod m$. 即同余方程 $ax \equiv 1 \mod m$ 有解 $x \equiv a' \mod m$. 根据定理 3.1.1, 有 $(a, m) = 1$. 因此, 整数 a 是模 m 简化剩余.

其次, 考虑通常的一次同余方程的求解. 实际上, 一次同余方程求解的思路是:

$$(a, m) = 1, ax \equiv 1 \mod m.$$

$$\Downarrow$$

$$(a, m) = 1, ax \equiv b \mod m.$$

$$\Downarrow$$

$$ax \equiv 1 \mod m.$$

我们有以下结果.

定理 3.1.3

设 m 是一个正整数, a 是满足 $m \nmid a$ 的整数, 则一次同余方程

$$ax \equiv b \mod m$$

有解的充要条件是 $(a, m) \mid b$. 且该同余方程有解时, 其解为

$$x \equiv \left(\frac{b}{(a,m)} \cdot \left(\left(\frac{a}{(a,m)} \right)^{-1} \mod \frac{m}{(a,m)} \right) + t \cdot \frac{m}{(a,m)} \right) \mod m,$$

$t = 0, 1, \cdots, (a, m) - 1.$

定理 3.1.3

设 m 是一个正整数, a 是满足 $m \nmid a$ 的整数, 则一次同余方程

$$ax \equiv b \mod m$$

有解的充要条件是 $(a,m) \mid b$. 且该同余方程有解时, 其解为

$$x \equiv \left(\frac{b}{(a,m)} \cdot \left(\left(\frac{a}{(a,m)} \right)^{-1} \mod \frac{m}{(a,m)} \right) + t \cdot \frac{m}{(a,m)} \right) \mod m,$$

$t = 0, 1, \cdots, (a,m) - 1.$

证：必要性.

设同余方程 $ax \equiv b \mod m$ 有解 $x \equiv x_0 \mod m$, 即存在整数 y_0 使得 $ax_0 - my_0 = b$.

因为 $(a,m) \mid a, (a,m) \mid m$, 所以根据定理 1.1.3 有 $(a,m) \mid ax_0 - my_0$, 即 $(a,m) \mid b$.

充分性. 设 $(a,m) \mid b$, 则 $\frac{b}{(a,m)}$ 为整数.

首先, 考虑同余方程

$$\frac{a}{(a,m)}x \equiv 1 \mod \frac{m}{(a,m)}.$$

因为 $\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$, 根据定理 3.1.1, 存在唯一解 x_0 (或运用广义欧几里德除法求出该整数 x_0), 使得同余方程 $\frac{a}{(a,m)}x \equiv 1 \mod \frac{m}{(a,m)}$ 成立, 而且有唯一解

$$x \equiv x_0 \mod \frac{m}{(a,m)}.$$

事实上, 若同余方程 $\frac{a}{(a,m)}x_0 \equiv 1 \mod \frac{m}{(a,m)}$ 和 $\frac{a}{(a,m)}x_0' \equiv 1 \mod \frac{m}{(a,m)}$ 同时成立, 两式相减得到

$$\frac{a}{(a,m)}(x_0 - x_0') \equiv 0 \mod \frac{m}{(a,m)}.$$

因为 $\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$, 我们立即得到

$$x_0 \equiv x_0' \mod \frac{m}{(a,m)}.$$

其次, 求出同余方程 $\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \mod \frac{m}{(a,m)}$ 的唯一解

$$x \equiv x_1 \equiv \frac{b}{(a,m)} \cdot x_0 \mod \frac{m}{(a,m)}.$$

而且, 该解是同余方程 $ax \equiv b \mod m$ 的一个特解.

其次, 求出同余方程 $\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \mod \frac{m}{(a,m)}$ 的唯一解

$$x \equiv x_1 \equiv \frac{b}{(a,m)} \cdot x_0 \mod \frac{m}{(a,m)}.$$

而且, 该解是同余方程 $ax \equiv b \mod m$ 的一个特解.

最后, 求出同余方程 $ax \equiv b \mod m$ 的全部解

$$x \equiv x_1 + t \cdot \frac{m}{(a,m)} \mod m,\ t = 0, 1, \cdots, (a,m) - 1.$$

其次, 求出同余方程 $\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \mod \frac{m}{(a,m)}$ 的唯一解

$$x \equiv x_1 \equiv \frac{b}{(a,m)} \cdot x_0 \mod \frac{m}{(a,m)}.$$

而且, 该解是同余方程 $ax \equiv b \mod m$ 的一个特解.

最后, 求出同余方程 $ax \equiv b \mod m$ 的全部解

$$x \equiv x_1 + t \cdot \frac{m}{(a,m)} \mod m,\ t = 0, 1, \cdots, (a,m) - 1.$$

事实上, 如果同时有同余方程 $ax_1 \equiv b \mod m$ 和 $ax_1' \equiv b \mod m$ 成立, 则两式相减得 $a(x_1 - x_1') \equiv 0 \mod m$. 性质 2.1.5 和性质 2.1.3, 这等价于

$$x_1 \equiv x_1' \mod \frac{m}{(a,m)}.$$

其次, 求出同余方程 $\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \mod \frac{m}{(a,m)}$ 的唯一解

$$x \equiv x_1 \equiv \frac{b}{(a,m)} \cdot x_0 \mod \frac{m}{(a,m)}.$$

而且, 该解是同余方程 $ax \equiv b \mod m$ 的一个特解.

最后, 求出同余方程 $ax \equiv b \mod m$ 的全部解

$$x \equiv x_1 + t \cdot \frac{m}{(a,m)} \mod m,\ t = 0, 1, \cdots, (a,m) - 1.$$

事实上, 如果同时有同余方程 $ax_1 \equiv b \mod m$ 和 $ax_1' \equiv b \mod m$ 成立, 则两式相减得 $a(x_1 - x_1') \equiv 0 \mod m$. 性质 2.1.5 和性质 2.1.3, 这等价于

$$x_1 \equiv x_1' \mod \frac{m}{(a,m)}.$$

因此, 同余方程 $ax \equiv b \mod m$ 的全部解可写成

$$x \equiv \frac{b}{(a,m)} \cdot \left(\left(\frac{a}{(a,m)} \right)^{-1} \mod \frac{m}{(a,m)} \right) + t \cdot \frac{m}{(a,m)} \mod m,$$

$t = 0, 1, \cdots, (a,m) - 1.$

例 3.1.2 求解一次同余式 $39x \equiv 65 \mod 91$.

例 3.1.2 求解一次同余式 $39x \equiv 65 \mod 91$.

解：首先, 计算最大公因数 $(39, 65) = 13$, 并且有 $(39, 65) \mid 91$, 所以原同余方程有解.

其次, 运用广义欧几里德除法, 求出同余方程

$$3x \equiv 1 \mod 7$$

的一个特解 $x_0' \equiv 5 \mod 7$.

再次, 求出同余方程

$$3x \equiv 5 \mod 7$$

的一个特解 $x_0 \equiv 5 \cdot x_0' \equiv 5 \cdot 5 \equiv 4 \mod 7$.

最后, 求出原同余方程的全部解

$$x \equiv 4 + t \cdot \frac{91}{(39, 65)} \equiv 4 + t \cdot 7 \mod 91, \ t = 0, 1, \cdots, 12$$

或

$$x \equiv 4, 11, 18, 25, 32, 39, 46, 53, 60, 67, 74, 81, 88 \mod 91.$$

目录

定理 3.2.1

设 $m_1, \cdots, m_k$ 是 k 个两两互素的正整数, $m = m_1 \cdots m_k$, 则同余方程

$$f(x) \equiv 0 \mod m \tag{3.2.1}$$

与同余方程组

$$\begin{cases} f(x) \equiv 0 \mod m_1 \\ \vdots \\ f(x) \equiv 0 \mod m_k \end{cases} \tag{3.2.2}$$

等价.

定理 3.2.1

设 $m_1, \cdots, m_k$ 是 k 个两两互素的正整数, $m = m_1 \cdots m_k$, 则同余方程

$$f(x) \equiv 0 \mod m \tag{3.2.1}$$

与同余方程组

$$\begin{cases} f(x) \equiv 0 \mod m_1 \\ \quad \vdots \\ f(x) \equiv 0 \mod m_k \end{cases} \tag{3.2.2}$$

等价.

证：设 x_0 是同余方程 (3.2.1) 的解, 则 $f(x_0) \equiv 0 \mod m$. 由性质 2.1.6, 我们有 $f(x_0) \equiv 0 \mod m_i$, $i = 1, \cdots, k$, 即 x_0 是同余方程组 (3.2.2) 的解.

定理 3.2.1

设 $m_1, \cdots, m_k$ 是 k 个两两互素的正整数, $m = m_1 \cdots m_k$, 则同余方程

$$f(x) \equiv 0 \mod m \tag{3.2.1}$$

与同余方程组

$$\begin{cases} f(x) \equiv 0 \mod m_1 \\ \quad \vdots \\ f(x) \equiv 0 \mod m_k \end{cases} \tag{3.2.2}$$

等价.

证：设 x_0 是同余方程 (3.2.1) 的解, 则 $f(x_0) \equiv 0 \mod m$. 由性质 2.1.6, 我们有 $f(x_0) \equiv 0 \mod m_i$, $i = 1, \cdots, k$, 即 x_0 是同余方程组 (3.2.2) 的解.

反过来, 设 $f(x_0) \equiv 0 \mod m_i$, $i = 1, \cdots, k$, 根据性质 2.1.7, 我们有 $f(x_0) \equiv 0 \mod m$, 即同余方程组 (3.2.2) 的解 x_0 也是同余方程 (3.2.1) 的解.

目录

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?

答曰：二十三.

术曰：三三数之剩二, 置一百四十. 五五数之剩三, 置六十三. 七七数之剩二, 置三十. 并之, 得二百三十三, 以二百一十减之, 即得. 凡三三数之剩一, 则置七十. 五五数之剩一, 则置二十一. 七七数之剩一, 则置十五. 即得.

——《孙子算经》卷下第 26 “物不知数”题

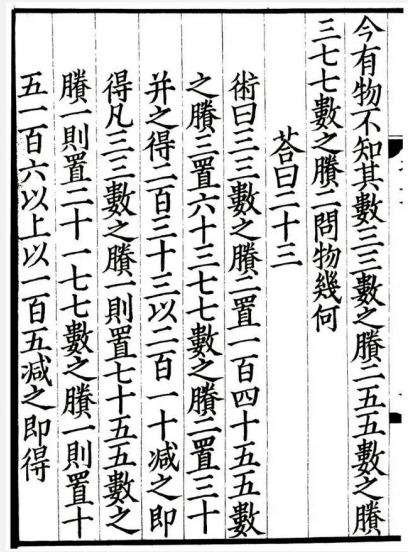
今有物, 不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二. 问物几何?

答曰：二十三.

术曰：三三数之剩二, 置一百四十. 五五数之剩三, 置六十三. 七七数之剩二, 置三十. 并之, 得二百三十三, 以二百一十减之, 即得. 凡三三数之剩一, 则置七十. 五五数之剩一, 则置二十一. 七七数之剩一, 则置十五. 即得. ——《孙子算经》卷下第 26 “物不知数”题

《孙子算经》

中国古代重要的数学著作, 成书大约在四、五世纪, 也就是大约一千五百年前. 南北朝数术著作,《算经十书》之一. 作者生平和编写年不详. 传本的《孙子算经》共三卷. 卷上叙述算筹记数的纵横相间制度和筹算乘除法, 卷中举例说明筹算分数算法和筹算开平方法, 卷下包括线性方程组等实用的、趣味的问题. 对后世的影响较为深远, 如著名的“鸡兔同笼”问题、具有重大意义的“物不知数”问题等.


今有物不知其數三三數之賸二五五數之賸三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五數之賸三置六十三七七數之賸二置三十并之得二百三十三以二百一十減之即得凡三三數之賸一則置七十五五數之賸一則置二十一七七數之賸一則置十五一百六以上以一百五減之即得

将其用同余方程组表示就是：

$$\begin{cases} x \equiv 2 \mod 3, \\ x \equiv 3 \mod 5, \\ x \equiv 2 \mod 7. \end{cases}$$

将其用同余方程组表示就是：

$$\begin{cases} x \equiv 2 \mod 3, \\ x \equiv 3 \mod 5, \\ x \equiv 2 \mod 7. \end{cases}$$

而解答过程就是

$$\begin{aligned} 2 \cdot 2 \cdot 5 \cdot 7 = & \quad 2 \cdot 70 = 140, \\ 3 \cdot 1 \cdot 3 \cdot 7 = & \quad 3 \cdot 21 = 63, \\ 2 \cdot 1 \cdot 3 \cdot 5 = & \quad 2 \cdot 15 = 30. \end{aligned}$$

$$140 + 63 + 30 = 233,$$

$$(-2) \cdot 3 \cdot 5 \cdot 7 = (-2) \cdot 105 = -210,$$

$$233 - 210 = 23.$$

将其用同余方程组表示就是：

$$\begin{cases} x \equiv \underset{\blacktriangle\, b_1}{2} \mod 3, \\ x \equiv \underset{\blacktriangle\, b_2}{3} \mod 5, \\ x \equiv \underset{\blacktriangle\, b_3}{2} \mod 7. \end{cases}$$

而解答过程就是

$$\begin{aligned} 2 \cdot 2 \cdot 5 \cdot 7 &= \quad 2 \cdot 70 \quad = 140, \\ 3 \cdot 1 \cdot 3 \cdot 7 &= \quad 3 \cdot 21 \quad = 63, \\ 2 \cdot 1 \cdot 3 \cdot 5 &= \quad 2 \cdot 15 \quad = 30. \end{aligned}$$

$$140 + 63 + 30 = 233,$$

$$(-2) \cdot 3 \cdot 5 \cdot 7 = (-2) \cdot 105 = -210,$$

$$233 - 210 = 23.$$

将其用同余方程组表示就是：

$$\begin{cases} x \equiv 2 \mod 3, \\ \quad \blacktriangle\, b_1 \quad \blacktriangle\, m_1 \\ x \equiv 3 \mod 5, \\ \quad \blacktriangle\, b_2 \quad \blacktriangle\, m_2 \\ x \equiv 2 \mod 7. \\ \quad \blacktriangle\, b_3 \quad \blacktriangle\, m_3 \end{cases}$$

而解答过程就是

$$2 \cdot 2 \cdot 5 \cdot 7 = \quad 2 \cdot 70 \quad = 140,$$

$$3 \cdot 1 \cdot 3 \cdot 7 = \quad 3 \cdot 21 \quad = 63,$$

$$2 \cdot 1 \cdot 3 \cdot 5 = \quad 2 \cdot 15 \quad = 30.$$

$$140 + 63 + 30 = 233,$$

$$(-2) \cdot 3 \cdot 5 \cdot 7 = (-2) \cdot 105 = -210,$$

$$233 - 210 = 23.$$

将其用同余方程组表示就是：

$$\begin{cases} x \equiv 2 \mod 3, \\ \quad\blacktriangle\ b_1 \quad\blacktriangle\ m_1 \\ x \equiv 3 \mod 5, \\ \quad\blacktriangle\ b_2 \quad\blacktriangle\ m_2 \\ x \equiv 2 \mod 7. \\ \quad\blacktriangle\ b_3 \quad\blacktriangle\ m_3 \end{cases}$$

而解答过程就是

$$\begin{aligned} 2 \cdot 2 \cdot \underbrace{5 \cdot 7}_{M_1} &= 2 \cdot 70 = 140, \\ 3 \cdot 1 \cdot \underbrace{3 \cdot 7}_{M_2} &= 3 \cdot 21 = 63, \\ 2 \cdot 1 \cdot \underbrace{3 \cdot 5}_{M_3} &= 2 \cdot 15 = 30. \end{aligned}$$

$$140 + 63 + 30 = 233,$$

$$(-2) \cdot 3 \cdot 5 \cdot 7 = (-2) \cdot 105 = -210,$$

$$233 - 210 = 23.$$

将其用同余方程组表示就是：

$$\begin{cases} x \equiv 2 \mod 3, \\ \quad\ \blacktriangle\, b_1 \quad \blacktriangle\, m_1 \\ x \equiv 3 \mod 5, \\ \quad\ \blacktriangle\, b_2 \quad \blacktriangle\, m_2 \\ x \equiv 2 \mod 7. \\ \quad\ \blacktriangle\, b_3 \quad \blacktriangle\, m_3 \end{cases}$$

而解答过程就是

$$\begin{aligned} 2 \cdot \underbrace{\widehat{2}}_{M_1'} \cdot \underbrace{5 \cdot 7}_{M_1} &= 2 \cdot 70 = 140, \\ 3 \cdot \underbrace{\widehat{1}}_{M_2'} \cdot \underbrace{3 \cdot 7}_{M_2} &= 3 \cdot 21 = 63, \\ 2 \cdot \underbrace{\widehat{1}}_{M_3'} \cdot \underbrace{3 \cdot 5}_{M_3} &= 2 \cdot 15 = 30. \end{aligned}$$

$$140 + 63 + 30 = 233,$$

$$(-2) \cdot 3 \cdot 5 \cdot 7 = (-2) \cdot 105 = -210,$$

$$233 - 210 = 23.$$

将其用同余方程组表示就是：

$$\begin{cases} x \equiv \underset{\blacktriangle\, b_1}{2} \mod \underset{\blacktriangle\, m_1}{3}, \\ x \equiv \underset{\blacktriangle\, b_2}{3} \mod \underset{\blacktriangle\, m_2}{5}, \\ x \equiv \underset{\blacktriangle\, b_3}{2} \mod \underset{\blacktriangle\, m_3}{7}. \end{cases}$$

而解答过程就是

$$\begin{aligned} 2 \cdot \underbrace{\widehat{2}}_{M_1'} \cdot \underbrace{5 \cdot 7}_{M_1} &= 2 \cdot 70 = 140, \\ 3 \cdot \underbrace{\widehat{1}}_{M_2'} \cdot \underbrace{3 \cdot 7}_{M_2} &= 3 \cdot 21 = 63, \\ 2 \cdot \underbrace{\widehat{1}}_{M_3'} \cdot \underbrace{3 \cdot 5}_{M_3} &= 2 \cdot 15 = 30. \\ 140 + 63 + 30 = \underset{\bigstar}{233}, &= \sum_{i=1}^{3} b_i \cdot M_i' \cdot M_i \\ (-2) \cdot 3 \cdot 5 \cdot 7 &= (-2) \cdot 105 = -210, \\ 233 - 210 &= 23. \end{aligned}$$

将其用同余方程组表示就是：

$$\begin{cases} x \equiv \underset{\blacktriangle\, b_1}{2} \mod \underset{\blacktriangle\, m_1}{3}, \\ x \equiv \underset{\blacktriangle\, b_2}{3} \mod \underset{\blacktriangle\, m_2}{5}, \\ x \equiv \underset{\blacktriangle\, b_3}{2} \mod \underset{\blacktriangle\, m_3}{7}. \end{cases}$$

而解答过程就是

$$\begin{aligned} 2 \cdot \underbrace{\widehat{2}}_{M_1'} \cdot \underbrace{5 \cdot 7}_{M_1} &= 2 \cdot 70 = 140, \\ 3 \cdot \underbrace{\widehat{1}}_{M_2'} \cdot \underbrace{3 \cdot 7}_{M_2} &= 3 \cdot 21 = 63, \\ 2 \cdot \underbrace{\widehat{1}}_{M_3'} \cdot \underbrace{3 \cdot 5}_{M_3} &= 2 \cdot 15 = 30. \\ 140 + 63 + 30 = \underset{\bigstar}{233}, &= \sum_{i=1}^{3} b_i \cdot M_i' \cdot M_i \\ (-2) \cdot \underbrace{3 \cdot 5 \cdot 7}_{m = m_1 \cdot m_2 \cdot m_3} &= (-2) \cdot 105 = -210, \\ 233 - 210 &= 23. \end{aligned}$$

将其用同余方程组表示就是：

$$\begin{cases} x \equiv \underset{\blacktriangle\, b_1}{2} \mod \underset{\blacktriangle\, m_1}{3}, \\ x \equiv \underset{\blacktriangle\, b_2}{3} \mod \underset{\blacktriangle\, m_2}{5}, \\ x \equiv \underset{\blacktriangle\, b_3}{2} \mod \underset{\blacktriangle\, m_3}{7}. \end{cases}$$

而解答过程就是

$$\begin{aligned} 2 \cdot \underbrace{\widehat{2}}_{M_1'} \cdot \underbrace{5 \cdot 7}_{M_1} &= 2 \cdot 70 = 140, \\ 3 \cdot \underbrace{\widehat{1}}_{M_2'} \cdot \underbrace{3 \cdot 7}_{M_2} &= 3 \cdot 21 = 63, \\ 2 \cdot \underbrace{\widehat{1}}_{M_3'} \cdot \underbrace{3 \cdot 5}_{M_3} &= 2 \cdot 15 = 30. \\ 140 + 63 + 30 &= \underset{\bigstar}{233}, \quad = \sum_{i=1}^{3} b_i \cdot M_i' \cdot M_i \\ \underbrace{(-2)}_{q} \cdot \underbrace{3 \cdot 5 \cdot 7}_{m = m_1 \cdot m_2 \cdot m_3} &= (-2) \cdot 105 = -210, \\ 233 - 210 &= 23. \end{aligned}$$

将其用同余方程组表示就是：

$$\begin{cases} x \equiv \underset{\blacktriangle\, b_1}{2} \mod \underset{\blacktriangle\, m_1}{3}, \\ x \equiv \underset{\blacktriangle\, b_2}{3} \mod \underset{\blacktriangle\, m_2}{5}, \\ x \equiv \underset{\blacktriangle\, b_3}{2} \mod \underset{\blacktriangle\, m_3}{7}. \end{cases}$$

而解答过程就是

$$\begin{aligned} 2 \cdot \underbrace{\widehat{2}}_{M_1'} \cdot \underbrace{5 \cdot 7}_{M_1} &= 2 \cdot 70 = 140, \\ 3 \cdot \underbrace{\widehat{1}}_{M_2'} \cdot \underbrace{3 \cdot 7}_{M_2} &= 3 \cdot 21 = 63, \\ 2 \cdot \underbrace{\widehat{1}}_{M_3'} \cdot \underbrace{3 \cdot 5}_{M_3} &= 2 \cdot 15 = 30. \\ 140 + 63 + 30 = \underset{\bigstar}{233}, &= \sum_{i=1}^{3} b_i \cdot M_i' \cdot M_i \\ \underbrace{(-2)}_{q} \cdot \underbrace{3 \cdot 5 \cdot 7}_{m = m_1 \cdot m_2 \cdot m_3} &= (-2) \cdot 105 = -210, \\ 233 - 210 &= 23. \end{aligned}$$

进一步, 可表示成 $x = b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + b_3 \cdot M_3' \cdot M_3 + q \cdot m$,

其中 $m = m_1 \cdot m_2 \cdot m_3$, $M_i = \frac{m}{m_i}$, $M_i' \cdot M_i \equiv 1 \mod m_i$, $i = 1, 2, 3$.

明朝数学家程大位的《孙子歌》：

三人同行七十稀，五树梅花廿一枝，

七子团圆正月半，除百零五便得知。

明朝数学家程大位的《孙子歌》：

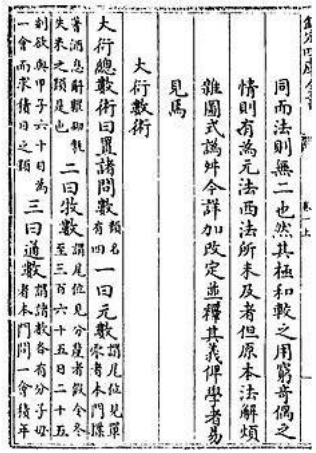
三人同行七十稀，五树梅花廿一枝，

七子团圆正月半，除百零五便得知。

秦九韶与“大衍求一术”

秦九韶 (1208 年 -1268 年), 南宋著名数学家. 1247 年完成著作《数书九章》，其中的大衍求一术、三斜求积术和秦九韶算法是有世界意义的重要贡献.

大衍问题源于《孙子算经》中的“物不知数”问题, 秦九韶在《数书九章》中明确系统地叙述了求解的一般性计算步骤, 并称之为“大衍求一术”. 这比高斯 1801 年建立的同余理论早 554 年, 被西方称为“中国剩余定理”, 即现代数论中一次同余方程组解法, 是中世纪世界数学的重要成就之一.



数学史家梁宗巨评价道：秦九韶的《数书九章》是一部划时代的巨著, 内容丰富, 精湛绝伦. 特别是大衍求一术（不定方程的中国独特解法）及高次代数方程的数值解法, 在世界数学史上占有崇高的地位. 那时欧洲漫长的黑夜犹未结束, 中国人的创造却像旭日一般在东方发出万丈光芒.

相关历史背景

在欧洲最早接触一次同余方程的, 是和秦九韶同时代的意大利数学家裴波那契 (1170 年 - 1250 年), 他在《算法之书》中给出了两个一次同余问题, 但是没有一般的算法. 这两个问题从形式到数据都和" 物不知数" 题相仿, 整个水平没有超过《孙子算经》.

相关历史背景

在欧洲最早接触一次同余方程的, 是和秦九韶同时代的意大利数学家裴波那契 (1170 年 - 1250 年), 他在《算法之书》中给出了两个一次同余问题, 但是没有一般的算法. 这两个问题从形式到数据都和" 物不知数" 题相仿, 整个水平没有超过《孙子算经》.

直到十八、十九世纪, 大数学家欧拉于 1743 年、高斯于 1801 年对一般一次同余方程进行了详细研究, 才重新获得和秦九韶“大衍求一术”相同的定理, 并对模数两两互素的情形给出了严格证明. 欧拉和高斯事先并不知道中国人的工作.

相关历史背景

在欧洲最早接触一次同余方程的, 是和秦九韶同时代的意大利数学家裴波那契 (1170 年 - 1250 年), 他在《算法之书》中给出了两个一次同余问题, 但是没有一般的算法. 这两个问题从形式到数据都和" 物不知数" 题相仿, 整个水平没有超过《孙子算经》.

直到十八、十九世纪, 大数学家欧拉于 1743 年、高斯于 1801 年对一般一次同余方程进行了详细研究, 才重新获得和秦九韶“大衍求一术”相同的定理, 并对模数两两互素的情形给出了严格证明. 欧拉和高斯事先并不知道中国人的工作.

1852 年英国传教士伟烈亚力发表《中国科学摘记》, 介绍了《孙子算经》物不知数题和秦九韶的解法, 引起了欧洲学者的重视. 1876 年, 德国马蒂生首先指出孙子问题的解法和高斯方法一致. 当时德国著名数学史家康托（1829 年 - 1920 年）看到马蒂生的文章后, 高度评价了“大衍术”, 并称赞发现这一方法的中国数学家是“最幸运的天才”. 直到今天, “大衍求一术”仍然引起西方数学史家浓厚的研究兴趣.

现在我们考虑“物不知数”问题的推广形式, 即非常重要的中国剩余定理或孙子定理.

定理 3.2.2 (中国剩余定理, Chinese Remainder Theorem)

设 $m_1, \cdots, m_k$ 是 k 个两两互素的正整数, 则对任意的整数 $b_1, \cdots, b_k$, 同余方程组

$$\begin{cases} x \equiv b_1 \mod m_1 \\ \quad \vdots \\ x \equiv b_k \mod m_k \end{cases} \tag{3.2.3}$$

一定有解, 且解是唯一的, 即

(i) 若令 $m = m_1 \cdots m_k$, $m = m_i \cdot M_i$, $i = 1, \cdots, k$, 则同余方程组 (3.2.3) 的解可表示为

$$x \equiv b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \mod m,$$

其中 $M_i' \cdot M_i \equiv 1 \mod m_i$, $i = 1, 2, \cdots, k$.

(ii) 若令 $N_i = m_1 \cdots m_i,\ i = 1, \cdots, k-1$, 则同余方程组 (3.2.3) 的解可表示为

$$x \equiv x_k \mod (m_1 \cdots m_k),$$

其中 $N_i' \cdot N_i \equiv 1 \mod m_{i+1},\ i = 1, 2, \cdots, k-1$, 而 x_i 是同余方程组

$$\begin{cases} x \equiv b_1 \mod m_1 \\ \quad \vdots \\ x \equiv b_i \mod m_i \end{cases}$$

的解, $i = 1, \cdots, k$, 并满足递归关系式

$$x_i \equiv x_{i-1} + ((b_i - x_{i-1}) N_{i-1}' \mod m_i) \cdot N_{i-1} \mod (m_1 \cdots m_i),\ i = 2, \cdots, k.$$

证：(i) 构造法证明.

首先, 证明解的存在性. 直接构造同余方程组的解：

根据假设条件, 对任意给定的 $i, 1 \leqslant i \leqslant k$, 有

$$(m_i, M_j) = 1,\ 1 \leqslant j \leqslant k, j \neq i.$$

又根据推论 1.2.1 有 $(m_i, M_i) = 1$. 再运用广义欧几里德除法, 可分别求出整数 $M_i',\ i = 1, 2, \cdots, k$, 使得 $M_i' \cdot M_i \equiv 1 \mod m_i,\ i = 1, 2, \cdots, k.$

证：(i) 构造法证明.

首先, 证明解的存在性. 直接构造同余方程组的解：

根据假设条件, 对任意给定的 $i, 1 \leqslant i \leqslant k$, 有

$$(m_i, M_j) = 1,\ 1 \leqslant j \leqslant k, j \neq i.$$

又根据推论 1.2.1 有 $(m_i, M_i) = 1$. 再运用广义欧几里德除法, 可分别求出整数 $M_i',\ i = 1, 2, \cdots, k$, 使得 $M_i' \cdot M_i \equiv 1 \mod m_i,\ i = 1, 2, \cdots, k.$

这样, 我们构造出一个如下的整数, 即

$$x = b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \mod m.$$

因为 $m = m_i \cdot M_i$ 及 $m_i \mid M_j,\ 1 \leqslant j \leqslant k, j \neq i,$

所以, 这个整数 x 满足同余方程

$$x \equiv 0 + \cdots + 0 + b_i \cdot M_i' \cdot M_i + 0 + \cdots + 0 \equiv b_i \mod m_i,\ i = 1, 2, \cdots, k.$$

也就是说, $x = b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \mod m$ 是同余方程组 (3.2.3) 的解.

其次, 证明解的唯一性. 设 x, x' 都是满足同余方程组 (3.2.3) 的解, 则 $x \equiv b_i \equiv x' \mod m_i,\ i = 1, 2, \cdots, k$. 因为 $m_1, \cdots, m_k$ 是两两互素的正整数, 根据性质 2.1.7, 我们得到 $x \equiv x' \mod m$.

其次, 证明解的唯一性. 设 x, x' 都是满足同余方程组 (3.2.3) 的解, 则 $x \equiv b_i \equiv x' \mod m_i,\ i = 1, 2, \cdots, k$. 因为 $m_1, \cdots, m_k$ 是两两互素的正整数, 根据性质 2.1.7, 我们得到 $x \equiv x' \mod m$.

（ii）递归法证明.

$k = 1$ 时, 同余方程 $x \equiv b_1 \mod m_1$ 的解为 $x \equiv x_1 \equiv b_1 \mod m_1$.

$k = 2$ 时, 原同余方程组等价于

$$\begin{cases} x \equiv b_1 \mod N_1, \\ x \equiv b_2 \mod m_2. \end{cases} \tag{3.2.4}$$

其次, 证明解的唯一性. 设 x, x' 都是满足同余方程组 (3.2.3) 的解, 则 $x \equiv b_i \equiv x' \mod m_i,\ i = 1, 2, \cdots, k$. 因为 $m_1, \cdots, m_k$ 是两两互素的正整数, 根据性质 2.1.7, 我们得到 $x \equiv x' \mod m$.

（ii）递归法证明.

$k = 1$ 时, 同余方程 $x \equiv b_1 \mod m_1$ 的解为 $x \equiv x_1 \equiv b_1 \mod m_1$.

$k = 2$ 时, 原同余方程组等价于

$$\begin{cases} x \equiv b_1 \mod N_1, \\ x \equiv b_2 \mod m_2. \end{cases} \tag{3.2.4}$$

由同余方程组 (3.2.4) 的第一个同余方程有解 $x \equiv x_1 \equiv b_1 \mod N_1$, 其中 $N_1 = m_1$, 可将同余方程组的解表示为 (y_1 为待定参数) $x = x_1 + y_1 \cdot N_1$.

其次, 证明解的唯一性. 设 x, x' 都是满足同余方程组 (3.2.3) 的解, 则 $x \equiv b_i \equiv x' \mod m_i,\ i = 1, 2, \cdots, k$. 因为 $m_1, \cdots, m_k$ 是两两互素的正整数, 根据性质 2.1.7, 我们得到 $x \equiv x' \mod m$.

（ii）递归法证明.

$k = 1$ 时, 同余方程 $x \equiv b_1 \mod m_1$ 的解为 $x \equiv x_1 \equiv b_1 \mod m_1$.

$k = 2$ 时, 原同余方程组等价于

$$\begin{cases} x \equiv b_1 \mod N_1, \\ x \equiv b_2 \mod m_2. \end{cases} \tag{3.2.4}$$

由同余方程组 (3.2.4) 的第一个同余方程有解 $x \equiv x_1 \equiv b_1 \mod N_1$, 其中 $N_1 = m_1$, 可将同余方程组的解表示为 (y_1 为待定参数) $x = x_1 + y_1 \cdot N_1$.

将 x 代入同余方程组 (3.2.4) 的第二个同余方程, 有

$$x_1 + y_1 \cdot N_1 \equiv b_2 \mod m_2,$$

即

$$y_1 \cdot N_1 \equiv b_2 - x_1 \mod m_2. \tag{3.2.5}$$

其次, 证明解的唯一性. 设 x, x' 都是满足同余方程组 (3.2.3) 的解, 则 $x \equiv b_i \equiv x' \mod m_i,\ i = 1, 2, \cdots, k$. 因为 $m_1, \cdots, m_k$ 是两两互素的正整数, 根据性质 2.1.7, 我们得到 $x \equiv x' \mod m$.

（ii）递归法证明.

$k = 1$ 时, 同余方程 $x \equiv b_1 \mod m_1$ 的解为 $x \equiv x_1 \equiv b_1 \mod m_1$.

$k = 2$ 时, 原同余方程组等价于

$$\begin{cases} x \equiv b_1 \mod N_1, \\ x \equiv b_2 \mod m_2. \end{cases} \tag{3.2.4}$$

由同余方程组 (3.2.4) 的第一个同余方程有解 $x \equiv x_1 \equiv b_1 \mod N_1$, 其中 $N_1 = m_1$, 可将同余方程组的解表示为 (y_1 为待定参数) $x = x_1 + y_1 \cdot N_1$.

将 x 代入同余方程组 (3.2.4) 的第二个同余方程, 有

$$x_1 + y_1 \cdot N_1 \equiv b_2 \mod m_2,$$

即

$$y_1 \cdot N_1 \equiv b_2 - x_1 \mod m_2. \tag{3.2.5}$$

运用广义欧几里德除法, 对整数 N_1 及模 m_2, 可求出整数 N_1' 使得

$$N_1' \cdot N_1 \equiv 1 \mod m_2.$$

$$N_1' \cdot N_1 \equiv 1 \mod m_2.$$

将同余方程 (3.2.5) 的两端同乘以 N_1', 得

$$y_1 \equiv (b_2 - x_1) \cdot N_1' \mod m_2.$$

$$N_1' \cdot N_1 \equiv 1 \mod m_2.$$

将同余方程 (3.2.5) 的两端同乘以 N_1', 得

$$y_1 \equiv (b_2 - x_1) \cdot N_1' \mod m_2.$$

故同余方程组 (3.2.4) 的解为

$$x = x_2 = x_1 + ((b_2 - x_1) \cdot N_1' \mod m_2) \cdot N_1 \mod (m_1 m_2).$$

$$N_1' \cdot N_1 \equiv 1 \mod m_2.$$

将同余方程 (3.2.5) 的两端同乘以 N_1', 得

$$y_1 \equiv (b_2 - x_1) \cdot N_1' \mod m_2.$$

故同余方程组 (3.2.4) 的解为

$$x = x_2 = x_1 + ((b_2 - x_1) \cdot N_1' \mod m_2) \cdot N_1 \mod (m_1 m_2).$$

假设 $i-1$ $(i \geqslant 2)$ 时, 结论成立. 即

$$\begin{cases} x \equiv b_1 \mod m_1 \\ \quad \vdots \\ x \equiv b_{i-1} \mod m_{i-1} \end{cases}$$

有解 $x \equiv x_{i-1} \mod (m_1 \cdots m_{i-1})$.

$$N_1' \cdot N_1 \equiv 1 \mod m_2.$$

将同余方程 (3.2.5) 的两端同乘以 N_1', 得

$$y_1 \equiv (b_2 - x_1) \cdot N_1' \mod m_2.$$

故同余方程组 (3.2.4) 的解为

$$x = x_2 = x_1 + ((b_2 - x_1) \cdot N_1' \mod m_2) \cdot N_1 \mod (m_1 m_2).$$

假设 $i-1$ $(i \geqslant 2)$ 时, 结论成立. 即

$$\begin{cases} x \equiv b_1 \mod m_1 \\ \quad \vdots \\ x \equiv b_{i-1} \mod m_{i-1} \end{cases}$$

有解 $x \equiv x_{i-1} \mod (m_1 \cdots m_{i-1})$.

对于 i, 同余方程组

$$\begin{cases} x \equiv b_1 \mod m_1 \\ \quad \vdots \\ x \equiv b_i \mod m_i \end{cases}$$

等价于同余方程组
$$\begin{cases} x \equiv x_{i-1} \mod N_{i-1}, \\ x \equiv b_i \mod m_i. \end{cases} \tag{3.2.6}$$

等价于同余方程组 $\begin{cases} x \equiv x_{i-1} \mod N_{i-1}, \\ x \equiv b_i \mod m_i. \end{cases}$ (3.2.6)

类似于 $k = 2$ 的情形, 由同余方程组 (3.2.6) 的第一个同余方程有解 $x \equiv x_{i-1} \mod N_{i-1}$, 可将同余方程组的解表示为 ($y_{i-1}$ 为待定参数)

$$x = x_{i-1} + y_{i-1} \cdot N_{i-1}.$$

等价于同余方程组
$$\begin{cases} x \equiv x_{i-1} \mod N_{i-1}, \\ x \equiv b_i \mod m_i. \end{cases} \tag{3.2.6}$$

类似于 $k = 2$ 的情形, 由同余方程组 (3.2.6) 的第一个同余方程有解 $x \equiv x_{i-1} \mod N_{i-1}$, 可将同余方程组的解表示为 ($y_{i-1}$ 为待定参数)

$$x = x_{i-1} + y_{i-1} \cdot N_{i-1}.$$

将 x 代入同余方程组 (3.2.6) 的第二个同余方程, 有

$$x_{i-1} + y_{i-1} \cdot N_{i-1} \equiv b_i \mod m_i,$$

即
$$y_{i-1} \cdot N_{i-1} \equiv b_i - x_{i-1} \mod m_i. \tag{3.2.7}$$

等价于同余方程组
$$\begin{cases} x \equiv x_{i-1} \mod N_{i-1}, \\ x \equiv b_i \mod m_i. \end{cases} \tag{3.2.6}$$

类似于 $k=2$ 的情形, 由同余方程组 (3.2.6) 的第一个同余方程有解 $x \equiv x_{i-1} \mod N_{i-1}$, 可将同余方程组的解表示为 ($y_{i-1}$ 为待定参数)

$$x = x_{i-1} + y_{i-1} \cdot N_{i-1}.$$

将 x 代入同余方程组 (3.2.6) 的第二个同余方程, 有

$$x_{i-1} + y_{i-1} \cdot N_{i-1} \equiv b_i \mod m_i,$$

即
$$y_{i-1} \cdot N_{i-1} \equiv b_i - x_{i-1} \mod m_i. \tag{3.2.7}$$

运用广义欧几里德除法, 对整数 N_{i-1} 及模 m_i, 可求出整数 N'_{i-1} 使得

$N'_{i-1} \cdot N_{i-1} \equiv 1 \mod m_i$,

等价于同余方程组 $\begin{cases} x \equiv x_{i-1} \mod N_{i-1}, \\ x \equiv b_i \mod m_i. \end{cases}$ (3.2.6)

类似于 $k = 2$ 的情形, 由同余方程组 (3.2.6) 的第一个同余方程有解 $x \equiv x_{i-1} \mod N_{i-1}$, 可将同余方程组的解表示为 ($y_{i-1}$ 为待定参数)

$$x = x_{i-1} + y_{i-1} \cdot N_{i-1}.$$

将 x 代入同余方程组 (3.2.6) 的第二个同余方程, 有

$$x_{i-1} + y_{i-1} \cdot N_{i-1} \equiv b_i \mod m_i,$$

即

$$y_{i-1} \cdot N_{i-1} \equiv b_i - x_{i-1} \mod m_i. \tag{3.2.7}$$

运用广义欧几里德除法, 对整数 N_{i-1} 及模 m_i, 可求出整数 N'_{i-1} 使得 $N'_{i-1} \cdot N_{i-1} \equiv 1 \mod m_i$, 将同余方程 (3.2.7) 的两端同乘以 N'_{i-1}, 得

$$y_{i-1} \equiv (b_i - x_{i-1}) \cdot N'_{i-1} \mod m_i.$$

等价于同余方程组
$$\begin{cases} x \equiv x_{i-1} \mod N_{i-1}, \\ x \equiv b_i \mod m_i. \end{cases} \tag{3.2.6}$$

类似于 $k=2$ 的情形, 由同余方程组 (3.2.6) 的第一个同余方程有解 $x \equiv x_{i-1} \mod N_{i-1}$, 可将同余方程组的解表示为 ($y_{i-1}$ 为待定参数)
$$x = x_{i-1} + y_{i-1} \cdot N_{i-1}.$$

将 x 代入同余方程组 (3.2.6) 的第二个同余方程, 有
$$x_{i-1} + y_{i-1} \cdot N_{i-1} \equiv b_i \mod m_i,$$

即
$$y_{i-1} \cdot N_{i-1} \equiv b_i - x_{i-1} \mod m_i. \tag{3.2.7}$$

运用广义欧几里德除法, 对整数 N_{i-1} 及模 m_i, 可求出整数 N'_{i-1} 使得 $N'_{i-1} \cdot N_{i-1} \equiv 1 \mod m_i$, 将同余方程 (3.2.7) 的两端同乘以 N'_{i-1}, 得
$$y_{i-1} \equiv (b_i - x_{i-1}) \cdot N'_{i-1} \mod m_i.$$

故同余方程组 (3.2.6) 的解为
$$x = x_i = x_{i-1} + ((b_i - x_{i-1}) \cdot N'_{i-1} \mod m_i) \cdot N_{i-1} \mod (m_1 m_2 \cdots m_i).$$

根据数学归纳法原理, 结论成立.

例 3.2.1 求解同余方程组

$$\begin{cases} x \equiv b_1 \mod 5, \\ x \equiv b_2 \mod 6, \\ x \equiv b_3 \mod 7, \\ x \equiv b_4 \mod 11. \end{cases}$$

例 3.2.1 求解同余方程组

$$\begin{cases} x \equiv b_1 \mod 5, \\ x \equiv b_2 \mod 6, \\ x \equiv b_3 \mod 7, \\ x \equiv b_4 \mod 11. \end{cases}$$

解：令 $m = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$,

$M_1 = 6 \cdot 7 \cdot 11 = 462$, $M_2 = 5 \cdot 7 \cdot 11 = 385$,

$M_3 = 5 \cdot 6 \cdot 11 = 330$, $M_4 = 5 \cdot 6 \cdot 7 = 210$.

分别求解同余方程

$$M_i' \cdot M_i \equiv 1 \mod m_i, i = 1, 2, 3, 4.$$

得到 $M_1' = 3, M_2' = 1, M_3' = 1, M_4' = 1$.

故同余方程组的解为

$$x \equiv 3 \cdot 462 \cdot b_1 + 385 \cdot b_2 + 330 \cdot b_3 + 210 \cdot b_4 \mod 2130.$$

例 3.2.2 韩信点兵: 有兵一队. 若列成五行纵队, 则末行一人; 成六行纵队, 则末行五人; 成七行纵队, 则末行四人; 成十一行纵队, 则末行十人. 求兵数.

例 3.2.2 韩信点兵: 有兵一队. 若列成五行纵队, 则末行一人; 成六行纵队, 则末行五人; 成七行纵队, 则末行四人; 成十一行纵队, 则末行十人. 求兵数.

解：韩信点兵问题可转化为同余方程组:

$$\begin{cases} x \equiv 1 \mod 5, \\ x \equiv 5 \mod 6, \\ x \equiv 4 \mod 7, \\ x \equiv 10 \mod 11. \end{cases}$$

例 3.2.2 韩信点兵: 有兵一队. 若列成五行纵队, 则末行一人; 成六行纵队, 则末行五人; 成七行纵队, 则末行四人; 成十一行纵队, 则末行十人. 求兵数.

解：韩信点兵问题可转化为同余方程组:

$$\begin{cases} x \equiv 1 \mod 5, \\ x \equiv 5 \mod 6, \\ x \equiv 4 \mod 7, \\ x \equiv 10 \mod 11. \end{cases}$$

解一. 对 $b_1 = 1, b_2 = 5, b_3 = 4, b_4 = 10$, 应用例 3.2.1, 得到

$$\begin{aligned} x &\equiv 3 \cdot 462 + 385 \cdot 5 + 330 \cdot 4 + 210 \cdot 10 \\ &\equiv 6731 \\ &\equiv 2111 \mod 2310. \end{aligned}$$

解二. 归纳构造同余方程的解.

令 $N_1 = 5$, 同余方程组的第一个同余方程有解 $x \equiv x_1 \equiv 1 \mod 5$, 可将同余方程组的解表示为 ($y$ 为待定参数) $x = 1 + 5y$.

令 $N_1 = 5$, 同余方程组的第一个同余方程有解 $x \equiv x_1 \equiv 1 \mod 5$, 可将同余方程组的解表示为 ($y$ 为待定参数) $x = 1 + 5y$.

将 x 代入同余方程组的第二个同余方程, 有 $1 + 5y \equiv 5 \mod 6$, 即 $5y \equiv 4 \mod 6$.

令 $N_1 = 5$, 同余方程组的第一个同余方程有解 $x \equiv x_1 \equiv 1 \mod 5$, 可将同余方程组的解表示为 ($y$ 为待定参数) $x = 1 + 5y$.

将 x 代入同余方程组的第二个同余方程, 有 $1 + 5y \equiv 5 \mod 6$, 即 $5y \equiv 4 \mod 6$.

运用广义欧几里德除法, 对整数 $N_1 = 5$ 及模 $m_2 = 6$, 可求出整数 $N_1' = N_1^{-1} \equiv 5 \mod 6$, 进而有 $y \equiv 5 \cdot 4 \equiv 2 \mod 6$.

故同余方程组的解为 $x = x_2 = 1 + 5 \cdot 2 \equiv 11 \mod 30$.

令 $N_1 = 5$, 同余方程组的第一个同余方程有解 $x \equiv x_1 \equiv 1 \mod 5$, 可将同余方程组的解表示为 ($y$ 为待定参数) $x = 1 + 5y$.

将 x 代入同余方程组的第二个同余方程, 有 $1 + 5y \equiv 5 \mod 6$, 即 $5y \equiv 4 \mod 6$.

运用广义欧几里德除法, 对整数 $N_1 = 5$ 及模 $m_2 = 6$, 可求出整数 $N_1' = N_1^{-1} \equiv 5 \mod 6$, 进而有 $y \equiv 5 \cdot 4 \equiv 2 \mod 6$.

故同余方程组的解为 $x = x_2 = 1 + 5 \cdot 2 \equiv 11 \mod 30$.

可将它表示为 (y 为待定参数) $x = x_2 = 11 + 30y$.

令 $N_1 = 5$, 同余方程组的第一个同余方程有解 $x \equiv x_1 \equiv 1 \mod 5$, 可将同余方程组的解表示为 ($y$ 为待定参数) $x = 1 + 5y$.

将 x 代入同余方程组的第二个同余方程, 有 $1 + 5y \equiv 5 \mod 6$, 即 $5y \equiv 4 \mod 6$.

运用广义欧几里德除法, 对整数 $N_1 = 5$ 及模 $m_2 = 6$, 可求出整数 $N_1' = N_1^{-1} \equiv 5 \mod 6$, 进而有 $y \equiv 5 \cdot 4 \equiv 2 \mod 6$.

故同余方程组的解为 $x = x_2 = 1 + 5 \cdot 2 \equiv 11 \mod 30$.

可将它表示为 (y 为待定参数) $x = x_2 = 11 + 30y$.

将 x 代入同余方程组的第三个同余方程, 有 $11 + 30y \equiv 4 \mod 7$, 即 $30y \equiv 4 - 11 \equiv 0 \mod 7$.

令 $N_1 = 5$, 同余方程组的第一个同余方程有解 $x \equiv x_1 \equiv 1 \mod 5$, 可将同余方程组的解表示为 ($y$ 为待定参数) $x = 1 + 5y$.

将 x 代入同余方程组的第二个同余方程, 有 $1 + 5y \equiv 5 \mod 6$, 即 $5y \equiv 4 \mod 6$.

运用广义欧几里德除法, 对整数 $N_1 = 5$ 及模 $m_2 = 6$, 可求出整数 $N_1' = N_1^{-1} \equiv 5 \mod 6$, 进而有 $y \equiv 5 \cdot 4 \equiv 2 \mod 6$.

故同余方程组的解为 $x = x_2 = 1 + 5 \cdot 2 \equiv 11 \mod 30$.

可将它表示为 (y 为待定参数) $x = x_2 = 11 + 30y$.

将 x 代入同余方程组的第三个同余方程, 有 $11 + 30y \equiv 4 \mod 7$, 即 $30y \equiv 4 - 11 \equiv 0 \mod 7$.

运用广义欧几里德除法, 对整数 $N_2 = 30$ 及模 $m_3 = 7$, 可求出整数 $N_2' = N_2^{-1} \equiv 4 \mod 7$, 进而有 $y \equiv 4 \cdot 0 \equiv 0 \mod 7$.

故同余方程组的解为 $x = x_3 = 11 + 30 \cdot 0 \equiv 11 \mod 210$.

可将它表示为 (y 为待定参数) $x = 11 + 210y$.

可将它表示为 (y 为待定参数) $x = 11 + 210y$.

将 x 代入同余方程组的第四个同余方程, 有 $11 + 210y \equiv 10 \mod 11$, 即 $210y \equiv 10 - 11 \equiv 10 \mod 11$.

可将它表示为 (y 为待定参数) $x = 11 + 210y$.

将 x 代入同余方程组的第四个同余方程, 有 $11 + 210y \equiv 10 \mod 11$, 即 $210y \equiv 10 - 11 \equiv 10 \mod 11$.

运用广义欧几里德除法, 对整数 $N_3 = 210$ 及模 $m_4 = 11$, 可求出整数 $N_3' = N_3^{-1} \equiv 1 \mod 11$, 进而有 $y \equiv 1 \cdot 10 \equiv 10 \mod 11$.

故同余方程组的解为 $x = x_4 = 11 + 210 \cdot 10 \equiv 2111 \mod 2310$.

目录

利用中国剩余定理, 可以将一些复杂的运算转化为较简单的运算.

利用中国剩余定理, 可以将一些复杂的运算转化为较简单的运算.

例 3.2.3 计算 $2^{1000000} \mod 77$.

利用中国剩余定理, 可以将一些复杂的运算转化为较简单的运算.

例 3.2.3 计算 $2^{1000000} \mod 77$.

解一：利用定理 2.2.13（欧拉定理）及模重复平方计算法进行求解.

因为 $77 = 7 \cdot 11, \varphi(77) = \varphi(7)\varphi(11) = 60$, 所以由定理 2.2.13（欧拉定理）得, $2^{60} \equiv 1 \mod 77$. 又 $1000000 = 16666 \cdot 60 + 40$, 所以

$$2^{1000000} = (2^{60})^{16666} \cdot 2^{40} \equiv 2^{40} \mod 77.$$

利用中国剩余定理, 可以将一些复杂的运算转化为较简单的运算.

例 3.2.3 计算 $2^{1000000} \mod 77$.

解一：利用定理 2.2.13（欧拉定理）及模重复平方计算法进行求解.

因为 $77 = 7 \cdot 11, \varphi(77) = \varphi(7)\varphi(11) = 60$, 所以由定理 2.2.13（欧拉定理）得, $2^{60} \equiv 1 \mod 77$. 又 $1000000 = 16666 \cdot 60 + 40$, 所以

$$2^{1000000} = (2^{60})^{16666} \cdot 2^{40} \equiv 2^{40} \mod 77.$$

设 $m = 77, b = 2$, 令 $a = 1$. 将 40 写成二进制 $40 = 2^3 + 2^5$.

运用模重复平方法, 我们依次计算如下:

(1) $n_0 = 0$, 计算 $a_0 = a \equiv 1, b_1 = b^2 \equiv 4 \mod 77$.

(2) $n_1 = 0$, 计算 $a_1 = a_0 \equiv 1, b_2 = b_1^2 \equiv 16 \mod 77$.

(3) $n_2 = 0$, 计算 $a_2 = a_1 \equiv 1, b_3 = b_2^2 \equiv 25 \mod 77$.

(4) $n_3 = 1$, 计算 $a_3 = a_2 \cdot b_3 \equiv 25, b_4 = b_3^2 \equiv 9 \mod 77$.

(5) $n_4 = 0$, 计算 $a_4 = a_3 \equiv 25, b_5 = b_4^2 \equiv 4 \mod 77$.

(6) $n_5 = 1$, 计算 $a_5 = a_4 \cdot b_5 \equiv 23 \mod 77$.

最后计算得出, $2^{1000000} \equiv 23 \mod 77$.

最后计算得出, $2^{1000000} \equiv 23 \mod 77$.

解二：利用中国剩余定理进行优化求解.

令 $x = 2^{1000000}$. 因为 $77 = 7 \cdot 11$, 所以计算 $x \mod 77$ 等价于求解同余方程组

$$\begin{cases} x \equiv b_1 \mod 7, \\ x \equiv b_2 \mod 11. \end{cases}$$

最后计算得出, $2^{1000000} \equiv 23 \mod 77$.

解二：利用中国剩余定理进行优化求解.

令 $x = 2^{1000000}$. 因为 $77 = 7 \cdot 11$, 所以计算 $x \mod 77$ 等价于求解同余方程组

$$\begin{cases} x \equiv b_1 \mod 7, \\ x \equiv b_2 \mod 11. \end{cases}$$

由欧拉定理知, $2^{\varphi(7)} = 2^6 \equiv 1 \mod 7$, 而 $1000000 = 166666 \cdot 6 + 4$, 所以 $b_1 \equiv 2^{1000000} = (2^6)^{166666} \cdot 2^4 \equiv 2 \mod 7$.

类似地, 因为 $2^{\varphi(11)} = 2^{10} \equiv 1 \mod 11$, 而 $1000000 = 100000 \cdot 10$, 所以 $b_2 \equiv 2^{1000000} = (2^{10})^{100000} \equiv 1 \mod 11$.

最后计算得出, $2^{1000000} \equiv 23 \mod 77$.

解二：利用中国剩余定理进行优化求解.

令 $x = 2^{1000000}$. 因为 $77 = 7 \cdot 11$, 所以计算 $x \mod 77$ 等价于求解同余方程组

$$\begin{cases} x \equiv b_1 \mod 7, \\ x \equiv b_2 \mod 11. \end{cases}$$

由欧拉定理知, $2^{\varphi(7)} = 2^6 \equiv 1 \mod 7$, 而 $1000000 = 166666 \cdot 6 + 4$, 所以 $b_1 \equiv 2^{1000000} = (2^6)^{166666} \cdot 2^4 \equiv 2 \mod 7$.

类似地, 因为 $2^{\varphi(11)} = 2^{10} \equiv 1 \mod 11$, 而 $1000000 = 100000 \cdot 10$, 所以 $b_2 \equiv 2^{1000000} = (2^{10})^{100000} \equiv 1 \mod 11$.

即求下列同余方程组的解.

$$\begin{cases} x \equiv 2 \mod 7, \\ x \equiv 1 \mod 11. \end{cases}$$

令 $m_1 = 7, m_2 = 11, m = m_1 \cdot m_2 = 77$, 以及 $M_1 = m_2 = 11, M_2 = m_1 = 7$, 分别求解同余方程

$$11M_1' \equiv 1 \mod 7, \quad 7M_2' \equiv 1 \mod 11.$$

得到

$$M_1' = 2, M_2' = 8.$$

故

$$x \equiv 2 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 1 \equiv 100 \equiv 23 \mod 77.$$

因此, $2^{1000000} \equiv 23 \mod 77$.

令 $m_1 = 7, m_2 = 11, m = m_1 \cdot m_2 = 77$, 以及 $M_1 = m_2 = 11, M_2 = m_1 = 7$, 分别求解同余方程

$$11M_1' \equiv 1 \mod 7, \quad 7M_2' \equiv 1 \mod 11.$$

得到

$$M_1' = 2, M_2' = 8.$$

故

$$x \equiv 2 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 1 \equiv 100 \equiv 23 \mod 77.$$

因此, $2^{1000000} \equiv 23 \mod 77$.

例 3.2.4 (RSA 公钥密码系统原型)

令 $m_1 = 7, m_2 = 11, m = m_1 \cdot m_2 = 77$, 以及 $M_1 = m_2 = 11, M_2 = m_1 = 7$, 分别求解同余方程

$$11M_1' \equiv 1 \mod 7, \quad 7M_2' \equiv 1 \mod 11.$$

得到

$$M_1' = 2, M_2' = 8.$$

故

$$x \equiv 2 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 1 \equiv 100 \equiv 23 \mod 77.$$

因此, $2^{1000000} \equiv 23 \mod 77$.

例 3.2.4 (RSA 公钥密码系统原型)

系统建立.

假设公钥密码系统使用 $N = 26$ 字符集 $\mathcal{N}$. 明文信息空间为 $k = 4$-字符组成的集合 $\mathcal{M} = \mathcal{N}^k$. 密文信息空间为 $l = 5$-字符组成的集合 $\mathcal{C} = \mathcal{N}^l$. 针对每个用户 (譬如信息接收方 A), 选取素数对 $p = 2017, q = 2027$.

(1) 计算 $n = pq = 4088459$ 和 $\varphi(n) = (p-1)(q-1) = 4084416$.

(1) 计算 $n = pq = 4088459$ 和 $\varphi(n) = (p-1)(q-1) = 4084416$.

(2) 随机选取整数 $e = 365, 1 < e < \varphi(n)$, 使得 $(e, \varphi(n)) = 1$.

(1) 计算 $n = pq = 4088459$ 和 $\varphi(n) = (p-1)(q-1) = 4084416$.

(2) 随机选取整数 $e = 365, 1 < e < \varphi(n)$, 使得 $(e, \varphi(n)) = 1$.

(3) 运用广义欧几里德算法计算唯一的整数 $d = 1051877, 1 < d < \varphi(n)$, 使得 $e \cdot d \equiv 1 \mod \varphi(n)$.

(1) 计算 $n = pq = 4088459$ 和 $\varphi(n) = (p-1)(q-1) = 4084416$.

(2) 随机选取整数 $e = 365, 1 < e < \varphi(n)$, 使得 $(e, \varphi(n)) = 1$.

(3) 运用广义欧几里德算法计算唯一的整数 $d = 1051877, 1 < d < \varphi(n)$, 使得 $e \cdot d \equiv 1 \mod \varphi(n)$.

则用户 A 的公钥 K_e 是数组 $(n, e) = (4088459, 365)$, 私钥是 $K_d = d = 1051877$.

(1) 计算 $n = pq = 4088459$ 和 $\varphi(n) = (p-1)(q-1) = 4084416$.

(2) 随机选取整数 $e = 365, 1 < e < \varphi(n)$, 使得 $(e, \varphi(n)) = 1$.

(3) 运用广义欧几里德算法计算唯一的整数 $d = 1051877, 1 < d < \varphi(n)$, 使得 $e \cdot d \equiv 1 \mod \varphi(n)$.

则用户 A 的公钥 K_e 是数组 $(n, e) = (4088459, 365)$, 私钥是 $K_d = d = 1051877$.

加密算法.

为加密信息 $m =$ math, 将明文 math 转换成数字信息:

$$m = 13 \cdot 26^3 + 1 \cdot 26^2 + 20 \cdot 26 + 8 = 229692.$$

任意发送方 B, 利用接收方 A 的公钥 K_e 计算出

$$c = m^e \mod n = 229692^{365} \equiv 3937358 \mod 4088459.$$

再将其转换成字符信息

$$c = 3937358 = 8 \cdot 26^4 + 16 \cdot 26^3 + 0 \cdot 26^2 + 12 \cdot 26 + 22 = \text{hpzlv},$$

即为待发送的密文.

(1) 计算 $n = pq = 4088459$ 和 $\varphi(n) = (p-1)(q-1) = 4084416$.

(2) 随机选取整数 $e = 365, 1 < e < \varphi(n)$, 使得 $(e, \varphi(n)) = 1$.

(3) 运用广义欧几里德算法计算唯一的整数 $d = 1051877, 1 < d < \varphi(n)$, 使得 $e \cdot d \equiv 1 \mod \varphi(n)$.

则用户 A 的公钥 K_e 是数组 $(n, e) = (4088459, 365)$, 私钥是 $K_d = d = 1051877$.

加密算法.

为加密信息 $m =$ math, 将明文 math 转换成数字信息:

$$m = 13 \cdot 26^3 + 1 \cdot 26^2 + 20 \cdot 26 + 8 = 229692.$$

任意发送方 B, 利用接收方 A 的公钥 K_e 计算出

$$c = m^e \mod n = 229692^{365} \equiv 3937358 \mod 4088459.$$

再将其转换成字符信息

$$c = 3937358 = 8 \cdot 26^4 + 16 \cdot 26^3 + 0 \cdot 26^2 + 12 \cdot 26 + 22 = \text{hpzlv},$$

即为待发送的密文.

解密算法.

为解密接收到的信息 hpzlv, 用户 A 将其转换成数字信息

$$c = 8 \cdot 26^4 + 16 \cdot 26^3 + 0 \cdot 26^2 + 12 \cdot 26 + 22 = 3937358.$$

解密算法.

为解密接收到的信息 hpzlv, 用户 A 将其转换成数字信息

$$c = 8 \cdot 26^4 + 16 \cdot 26^3 + 0 \cdot 26^2 + 12 \cdot 26 + 22 = 3937358.$$

再利用自己的私钥 K_d 计算出

$$c^d \mod n = 3937358^{1051877} \equiv 229692 \mod 4088459.$$

解密算法.

为解密接收到的信息 hpzlv, 用户 A 将其转换成数字信息

$$c = 8 \cdot 26^4 + 16 \cdot 26^3 + 0 \cdot 26^2 + 12 \cdot 26 + 22 = 3937358.$$

再利用自己的私钥 K_d 计算出

$$c^d \mod n = 3937358^{1051877} \equiv 229692 \mod 4088459.$$

并将其转换成字符信息 $229692 = 13 \cdot 26^3 + 1 \cdot 26^2 + 20 \cdot 26 + 8 = \text{math}$, 即为明文.

解密算法.

为解密接收到的信息 hpzlv, 用户 A 将其转换成数字信息

$$c = 8 \cdot 26^4 + 16 \cdot 26^3 + 0 \cdot 26^2 + 12 \cdot 26 + 22 = 3937358.$$

再利用自己的私钥 K_d 计算出

$$c^d \mod n = 3937358^{1051877} \equiv 229692 \mod 4088459.$$

并将其转换成字符信息 $229692 = 13 \cdot 26^3 + 1 \cdot 26^2 + 20 \cdot 26 + 8 =$ math, 即为明文.

注: 需要强调的是, 在加密算法中因发送方 B 不知道用户 A 的公钥中 n 的整数分解, 即 p 和 q, 所以在计算 $c = m^e \mod n$ 时无法使用中国剩余定理进行优化运算.

但在解密算法中, 用户 A 知道自己的私钥, 进而可等同于知道 n 的整数分解, 所以可以利用中国剩余定理简化计算 $c^d \mod n$.

事实上, 令 $x = 3937358^{1051877}$, 因为 $4088459 = 2017 \cdot 2027$, 所以计算 $x \mod 4088459$ 等价于求解同余方程组

$$\begin{cases} x \equiv b_1 \mod 2017, \\ x \equiv b_2 \mod 2027. \end{cases}$$

事实上, 令 $x = 3937358^{1051877}$, 因为 $4088459 = 2017 \cdot 2027$, 所以计算 $x \mod 4088459$ 等价于求解同余方程组

$$\begin{cases} x \equiv b_1 \mod 2017, \\ x \equiv b_2 \mod 2027. \end{cases}$$

由同余性质、费马小定理和模重复平方计算法得,

$$b_1 \equiv 3937358^{1051877} \equiv 174^{1541} \equiv 1771 \mod 2017,$$

$$b_2 \equiv 3937358^{1051877} \equiv 924^{383} \equiv 641 \mod 2027.$$

根据中国剩余定理, 先分别求出 $qq' \equiv 1 \mod p$ 和 $pp' \equiv 1 \mod q$, 即 $2027q' \equiv 1 \mod 2017$ 和 $2017p' \equiv 1 \mod 2027$, 亦即 $q' \equiv 1412 \mod 2017$ 和 $p' \equiv 608 \mod 2027$.

再得出同余方程组的解

$$x \equiv 1771 \cdot 1412 \cdot 2027 + 641 \cdot 608 \cdot 2017 \equiv 229692 \mod 4088459.$$

定理 2.2.4 的推广.

定理 3.2.3

在定理 3.2.2 的条件下, 若整数 $b_1, \cdots, b_k$ 分别遍历模 $m_1, \cdots, m_k$ 的完全剩余系, 则

$$x \equiv b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \mod m$$

遍历模 $m = m_1 \cdot m_2 \cdots m_k$ 的完全剩余系.

定理 2.2.4 的推广.

定理 3.2.3

在定理 3.2.2 的条件下, 若整数 $b_1, \cdots, b_k$ 分别遍历模 $m_1, \cdots, m_k$ 的完全剩余系, 则

$$x \equiv b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \mod m$$

遍历模 $m = m_1 \cdot m_2 \cdots m_k$ 的完全剩余系.

证：令

$$x_0 = b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \mod m,$$

则当 $b_1, \cdots, b_k$ 分别遍历模 $m_1, \cdots, m_k$ 的完全剩余系时, x_0 遍历 $m_1 m_2 \cdots m_k$ 个数.

下证它们模 m 两两不同余, 则结论成立.

事实上, 若

$$b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k$$

$$\equiv b_1' \cdot M_1' \cdot M_1 + b_2' \cdot M_2' \cdot M_2 + \cdots + b_k' \cdot M_k' \cdot M_k \mod m,$$

则根据性质 2.1.6,

$$b_i \cdot M_i' \cdot M_i \equiv b_i' \cdot M_i' \cdot M_i \mod m_i,\ i = 1, \cdots, k.$$

而 $M_i' \cdot M_i \equiv 1 \mod m_i,\ i = 1, \cdots, k$, 所以,

$$b_i \equiv b_i' \mod m_i,\ i = 1, \cdots, k.$$

但 b_i, b_i' 是同一个完全剩余系中的两个数, 故

$$b_i = b_i',\ i = 1, \cdots, k.$$

本课作业

1. 求解同余方程：$256x \equiv 179 \mod 337$.
2. 求解同余方程：$28x \equiv 21 \mod 35$.
3. 一个数被 3 除余 1, 被 4 除余 2, 被 5 除余 4, 这个数最小是几?
4. 利用中国剩余定理计算 $2^{2024} \mod 77$.

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