Discrete Mathematics

2019~2020 (第一学期)

Department of Computer Science, East China Normal University

September 10, 2019

Chapter 2 NUMBER THEORY

一次同余方程

Definition (同余方程)

同余方程(congruence equation): 形如 $f(x) \equiv 0 \pmod{m}$ 的方程, 其中 $f \in \mathbb{Z}[x]$ 和 $m \in \mathbb{N}$.
同余方程的解: $x_0 \in \mathbb{Z}$, 满足$f(x_0) \equiv 0 \pmod{m}$.

若 $\deg_x(f) = 1$, 即 $f(x) = a \cdot x + b$ $(a, b \in \mathbb{Z})$, 则称同余方程是一次的 (线性的, linear).

同余方程的解定理

Theorem

设 $(a, m) = d$.
同余方程 $a \cdot x \equiv b \pmod{m}$ 有解的充分必要条件是 $d \mid b$.

Recall that

Example

$0, 1, \ldots, 10$ 中的哪些数可表示为 $12m + 20n$ 的形式, 其中 m 和 n 是整数?

同余方程的解定理

证明 $a \cdot x \equiv b \pmod{m}$ 有解 $\Leftrightarrow d \mid b$.

$a \cdot x \equiv b \pmod{m}$ 有解 $\Leftrightarrow a \cdot x + m \cdot y = b$ 有整数解.

$\Rightarrow$ $a \cdot x + m \cdot y = b$ 有整数解 $\Rightarrow d \mid b$.

$\Leftarrow$ $d \mid b \Rightarrow$ 存在 $k \in \mathbb{Z}$, 使得 $b = d \cdot k$

$\Rightarrow$ 存在 $s, t \in \mathbb{Z}$, 使得 $a \cdot s \cdot k + m \cdot t \cdot k = d \cdot k = b$

$\Rightarrow x = s \cdot k, y = t \cdot k$ 是 $a \cdot x + m \cdot y = b$ 的整数解.

$\square$

同余方程的解定理

Theorem

设 $(a, m) = d$.
同余方程 $a \cdot x \equiv b \pmod{m}$ 有解的充分必要条件是 $d \mid b$.

其解共有 d 个:

$$x \equiv x_0 + t \cdot \frac{m}{d} \pmod{m}, \qquad (t = 0, 1, 2, \ldots, d-1), \tag{1}$$

其中 x_0 是满足同余方程 $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ 的任意一个特解.

Recall that

若 $a \cdot c \equiv b \cdot c \pmod{m}$, 则 $a \equiv b \pmod{\frac{m}{(c,m)}}$.

同余方程的解法

求解同余方程 $a \cdot x \equiv b \pmod{m}$ 的步骤.

1. 用欧几里德算法求 (a, m). 若 $(a, m) \mid b$, 则方程有解.
2. 计算$a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $m' = \frac{m}{d}$, 其中 $d = (a, m)$.
3. 用扩展的欧几里德算法求 $p, q \in \mathbb{Z}$, 使得 $p \cdot a' + q \cdot m' = 1$.
   由 $p \cdot a' \equiv 1 \pmod{m'}$, 即 $b' \cdot p \cdot a' \equiv b' \pmod{m'}$,
   可得 $a' \cdot x \equiv b' \pmod{m'}$ 的特解 $x_0 = b' \cdot p$.
4. 将 x_0 代入 (1) 得到同余方程 $a \cdot x \equiv b \pmod{m}$ 的解.

同余方程的解法

Example

求同余方程 $1215 \cdot x \equiv 560 \pmod{2755}$ 的解.

1. $(a, m) = (1215, 2755) = 5$, $5 \mid 560$, 所以方程有解.
2. $a' = \frac{1215}{5} = 243$, $b' = \frac{560}{5} = 112$, $m' = \frac{2755}{5} = 551$.
3. 扩展欧几里得算法可求得 $p = -195$ 和 $q = 86$, 满足 $p \cdot a' + q \cdot m' = 1$.
   特解 $x_0 = p \cdot b' = -195 \cdot 112$.
4. 解为

$$x \equiv -195 \cdot 112 + t \cdot 551 \pmod{2755}, \qquad (t = 0, 1, \ldots, 4).$$

一次同余方程组

Example (一次同余方程组(出自孙子算经))

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.
答案是下列一次同余方程组的解:

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

一般形式

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv a_k \pmod{m_k}. \end{cases}$$

同余方程组的解定理

Theorem (孙子定理)

设 $m_1, m_2, \ldots, m_k \in \mathbb{N}$ 两两互素.
令 $M = m_1 \cdot m_2 \cdot \cdots \cdot m_k, M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \ldots, M_k = \frac{M}{m_k}$.
则同余方程组关于模 M 有唯一解 (即有且仅有一个满足 $0 \le x < M$ 的解):

$$x \equiv a_1 \cdot c_1 \cdot M_1 + a_2 \cdot c_2 \cdot M_2 + \cdots + a_k \cdot c_k \cdot M_k \pmod{M}, \tag{2}$$

其中 c_i 是同余方程$M_i \cdot x \equiv 1 \pmod{m_i}$ 的特解, $i = 1, 2, \ldots, k$.

同余方程组的解定理

Example

求解同余方程组

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

$m_1 = 3, m_2 = 5, m_3 = 7, M = 105, M_1 = 35, M_2 = 21, M_3 = 15.$
$35 \cdot x \equiv 1 \pmod 3), 21 \cdot x \equiv 1 \pmod 5), 15 \cdot x \equiv 1 \pmod 7)$ 的特解分别是:
$c_1 = 2, c_2 = 1, c_3 = 1.$
那么原同余方程组的一般解:

$$\begin{aligned} x &\equiv 2 \cdot 2 \cdot 35 + 3 \cdot 21 + 2 \cdot 15 = 140 + 63 + 30 \\ &\equiv 23 \pmod{105}. \end{aligned}$$

同余方程组的解法

求解规范的同余方程组的步骤:

1. 计算$M = m_1 \cdot m_2 \cdot \cdots \cdot m_k, M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \ldots, M_k = \frac{M}{m_k}$.
2. 求解同余方 $M_i \cdot x \equiv 1 \pmod{m_i}$ 的特解 c_i, $i = 1, 2, \ldots, k$.
3. 代入 (2) 得到通解:

$$x \equiv a_1 \cdot c_1 \cdot M_1 + a_2 \cdot c_2 \cdot M_2 + \cdots + a_k \cdot c_k \cdot M_k \pmod{M}.$$

QUIZ: 如若同余方程组不规范呢?

同余方程组的规范化

Example

求解同余方程组:

$$\begin{cases} 5 \cdot x \equiv 14 \pmod{17} \\ 3 \cdot x \equiv 2 \pmod{13}. \end{cases}$$

我们有:

$5 \cdot x \equiv 14 \pmod{17} \Rightarrow 35 \cdot x \equiv 98 \pmod{17} \Rightarrow x \equiv 13 \pmod{17}$.

$3 \cdot x \equiv 2 \pmod{13} \Rightarrow 27 \cdot x \equiv 18 \pmod{13} \Rightarrow x \equiv 5 \pmod{13}$.

原方程组与规范方程组

$$\begin{cases} x \equiv 13 \pmod{17} \\ x \equiv 5 \pmod{13} \end{cases}$$

同解. (注意: 两端所乘之数必须分别与 17 和 13 互素.)

QUIZ: 如若 $m_1, m_2, \ldots, m_k$ 不俩俩互素呢?

同余方程组的规范化

Example

求解同余方程组: $5 \cdot x \equiv 7 \pmod{12}$, $7 \cdot x \equiv 1 \pmod{10}$.

$$\begin{aligned}
5 \cdot x \equiv 7 \pmod{12} &\Leftrightarrow 12 \mid (5 \cdot x - 7) \\
&\Leftrightarrow 3 \mid (5 \cdot x - 7) \text{ 且 } 4 \mid (5 \cdot x - 7) \\
&\Leftrightarrow 5 \cdot x \equiv 7 \pmod{3} \text{ 且 } 5 \cdot x \equiv 7 \pmod{4} \\
7 \cdot x \equiv 1 \pmod{10} &\Leftrightarrow 7 \cdot x \equiv 1 \pmod{2} \text{ 且 } 7 \cdot x \equiv 1 \pmod{5}
\end{aligned}$$

原方程组等价于方程组:

$$5 \cdot x \equiv 7 \pmod{3},\ 5 \cdot x \equiv 7 \pmod{4},\ 7 \cdot x \equiv 1 \pmod{2},\ 7 \cdot x \equiv 1 \pmod{5}.$$

大整数的剩余表示法

大整数 (biginteger) 在的计算机科学中的应用: 数据加密和解密

表示大整数的基本方法: 用多个字

- 常规表示法: r 进制数

  不便作并行计算

- 剩余表示法

  基于孙子定理

  取 $m_1, m_2, \ldots, m_r \in \mathbb{N}$, 两两互素, 令 $M = m_1 \cdot m_2 \cdot \cdots \cdot m_r$

  x 的剩余表示: 用 x 关于 $m_1, m_2, \ldots, m_r$ 的余数表示 x

  $(a_1, a_2, \ldots, a_r),\ x \equiv a_i \pmod{m_i},\ i = 1, 2, \ldots, r$

大整数的剩余表示法

Example

取 $m_1 = 2, m_2 = 3, m_3 = 5$, 则 $M = m_1 \cdot m_2 \cdot m_3 = 30$.
对于任意 $x \in \{0, 1, \ldots, 29\}$, 可用剩余表示法唯一地表示为三元组: $(x \mod 2, x \mod 3, x \mod 5)$.

例如:

$$\begin{aligned} 0 &\mapsto (0,0,0), \\ 5 &\mapsto (1,2,0), \\ 13 &\mapsto (1,1,3). \end{aligned}$$

大整数的剩余表示法

Theorem

对于任意 $x \in \{0, 1, 2, \ldots, M-1\}$, x 与其剩余表示 (r 元组) 一一对应.

剩余表示下的运算

分别对剩余表示中的各个分量独立地进行相应的模运算,
得到的是运算结果的剩余表示, 可通过求解同余方程组求原数 (假如没有溢出).

大整数的剩余表示法

Example (continued)

已知 $4 \mapsto (0,1,4), \qquad 7 \mapsto (1,1,2)$, 则

$$4+7 \mapsto (0,1,4)+(1,1,2) = (0+1, 1+1, 4+2 \mod 5) = (1,2,1)$$
$$4\times 7 \mapsto (0,1,4)\times(1,1,2) = (0\times 1, 1\times 1, 4\times 2 \mod 5) = (0,1,3).$$

可反过来验证 $11 = 4+7$ 和 $28 = 4\times 7$ 的剩余表示就是下面同余方程组的解 (限定在 $0 \le x < 30$).

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5, \end{cases} \qquad \begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5. \end{cases}$$

Homework

1. P. 33: Exercises 14(2),16,*17.

RSA 公钥密码体制

Caesar 密码

加密方法 (明文→密文): 模 26, 密文为明文后的第 3 个字符

$A \to D,\ B \to E, \ldots, W \to Z,\ X \to A,\ Y \to B,\ Z \to C$

私钥密码体制 (对称密码)

加密和解密的密钥相同或彼此容易推出

加密和解密的密钥都必须保密

公钥密码体制 (非对称密码)

加密和解密的密钥不同，无法或很难相互推算

加密用公开的公钥，解密用保密的私钥

解决了密钥的发布和管理问题，是目前商业密码体制的核心

RSA 公钥密码体制

RSA 公钥密码概述

R. L. Rivest, A. Shamir 和 L. Adleman 于 1978 年提出, 2002 年获 Turing Award.
安全性源于大整数素因数分解的困难性.

RSA 公钥密码设计

选取大素数 p, q $(p \neq q)$.
令 $n = p \cdot q$, $\varphi(n) = (p-1) \cdot (q-1)$.
选取 $e \in \mathbb{N}$, 使得 $(e, \varphi(n)) = 1$.
同余方程 $e \cdot x \equiv 1 \pmod{\varphi(n)}$ 有唯一解 d (限定在 $0 \leq d < \varphi(n)$).
公钥 (加密密钥): (e, n);
私钥 (解密密钥): (d, n).

RSA 公钥密码体制

RSA 加密

明文数字化编码, 再分段, 一个段就是一个整数 m $(0 \leq m < n)$.
加密按段进行, 明文段 m 的密文: $c = \mathrm{Encode}(m) = m^e \mod n$.

RSA 解密

密文 c 解密为明文 $m = \mathrm{Decode}(c) = c^d \mod n$.

RSA 公钥密码体制

取小素数 $p = 3, q = 11$ (实际中取大素数).
$n = p \cdot q = 33, \varphi(n) = (p-1)(q-1) = 20.$
取 $e = 3, (3, 20) = 1$, 解同余方程 $3 \cdot d \equiv 1 \pmod{20}$, 得到唯一解 $d = 7$.
公钥: $(e, n) = (3, 33)$;
私钥: $(d, n) = (7, 33)$.

明文信息由 26 个小写字母构成, 数字化编码:
字母的序号 $a \mapsto 01,\ e \mapsto 05,\ k \mapsto 11,\ y \mapsto 25$.
如明文: "*key*" $\mapsto 110525$,
取段长为 2, 明文 "110525" 分为 3 段: $m_1 = 11, m_2 = 05, m_3 = 25$.

RSA公钥密码体制

用公钥 $(3, 33)$ 加密得到 3 个密文:

$$\begin{aligned} c_1 &= m_1^e \mod n = 11^3 \mod 33 = 11 \\ c_2 &= m_2^e \mod n = 5^3 \mod 33 = 26 \\ c_3 &= m_3^e \mod n = 25^3 \mod 33 = 16. \end{aligned}$$

用私钥 $(7, 33)$ 解密还原为 3 个明文:

$$\begin{aligned} m_1 &= c_1^d \mod n = 11^7 \mod 33 = 11 \\ m_2 &= c_2^d \mod n = 26^7 \mod 33 = 5 \\ m_3 &= c_3^d \mod n = 16^7 \mod 33 = 25. \end{aligned}$$

组合所得到的明文为 110525, 经由编码表得到明文信息 “key”.

RSA 公钥密码体制的几个关键问题*

(1) **解密算法的正确性**

证明 $m = D(c)$.

$D(c) = c^d mod\ n = (m^e mod\ n)^d mod\ n = m^{ed} mod\ n$
$ed \equiv 1(mod\ \varphi(n)) \Rightarrow \exists k \in \mathbb{Z}$, 使 $ed = k\varphi(n) + 1$
根据 m 分两种情况分别证明

(a) $(m, n) = 1$

$$
\begin{aligned}
&(m, n) = 1 \\
\Rightarrow & m^{\varphi(n)} \equiv 1(mod\ n) \qquad \text{(欧拉定理)} \\
\Rightarrow & m^{ed} = m^{k\varphi(n)+1} = m(m^{\varphi(n)})^k \equiv m(1)^k \equiv m(mod\ n)
\end{aligned}
$$

□

RSA 公钥密码体制的几个关键问题*

(2) **解密算法的正确性**

证明.

(b) $(m,n) \neq 1$

$$
\begin{aligned}
& 0 \le m < n, n = pq, p, q \text{是素数}, p \neq q, (m,n) \neq 1 \\
\Rightarrow & m\text{含且仅含}p\text{和}q\text{中的一个为因数} \\
& \text{不妨设} m = sp, s \in \mathbb{N}, q \nmid m \\
\Rightarrow & m^{q-1} \equiv 1 (mod\ q) \qquad (\text{欧拉定理或费马小定理}) \\
\Rightarrow & m^{k\varphi(n)} = m^{k(p-1)(q-1)} = (m^{(q-1)})^{k(p-1)} \equiv (1)^{k(p-1)} \equiv 1 (mod\ q) \\
\Rightarrow & t \in \mathbb{Z}, \text{使}\ m^{k\varphi(n)} = tq + 1 \\
\Rightarrow & m^{k\varphi(n)+1} = tqm + m = tqsp + m = tsn + m \\
\Rightarrow & m^{ed} \equiv m (mod\ n)
\end{aligned}
$$

RSA 公钥密码体制的几个关键问题

(2) **安全性(破译的可能性)**
$ed \equiv 1(mod\, \varphi(n))$, 公钥 (e, n) 公开, 解同余方程即可得到私钥 (d, n) 难点在于计算 $\varphi(n) = (p-1)(q-1)$, p, q 不公开, 需对 n 进行素分解
以目前的技术分解一个400位的整数需要数千年
若p,q是200位的素数，则RSA密码是安全的

Homework

1. 已知 RSA 密码体制的公钥$(e, n) = (5, 35)$,
   1. 请按本小节例题所示的方式将明文信息“rsa”加密;
   2. 请破解出私钥.