蘇州大學
SOOCHOW UNIVERSITY

Chap4 Number Theory

Part II: Congruence and Cryptography

Jin-Hui Wu

2026-03-27

大纲

- 整除和模
- 整数表示和算法
- 素数和最大公约数
- 同余方程
- 同余的应用
- 密码学

大纲

- 整除和模
- 整数表示和算法
- 素数和最大公约数
- 同余方程 (4.4)
- 同余的应用
- 密码学

线性同余方程

- 线性同余方程 (linear congruence)
  - 形如 $ax \equiv b \pmod{m}$ 的关于x的方程
  - 有解时有无穷多个解，$x_0 + km$

线性同余方程

- 线性同余方程 (linear congruence)
  - 形如 $ax \equiv b \pmod{m}$ 的关于x的方程

- 逆 (inverse)
  - 若$\bar{a}a \equiv 1 \pmod{m}$，则称$\bar{a}$为$a$模$m$的逆
  - 例
    - 5 is an inverse of 3 modulo 7

线性同余方程

- 线性同余方程 (linear congruence)
  - 形如 $ax \equiv b \pmod{m}$ 的关于x的方程
- 逆 (inverse)
  - 若$\bar{a}a \equiv 1 \pmod{m}$，则称$\bar{a}$为$a$模$m$的逆
- 解法
  - $\gcd(a, m) = 1$时，a的逆存在
  - 方程两侧同乘$\bar{a}$，即$x \equiv \bar{a}b \pmod{m}$

例

- Find an inverse of 3 modulo 7
- Find solutions of $3x \equiv 4 \pmod 7$

- Find an inverse of 101 modulo 4620
  - 在欧几里得算法计算$\gcd(a,b)$过程中，每个数字都用a,b表示

“物不知数”问题

- 出现于南北朝时期（约公元5世纪）的数学著作《孙子算经》中：

  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？

“物不知数”问题

- 出现于南北朝时期（约公元5世纪）的数学著作《孙子算经》中：

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？

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

中国剩余定理

- 中国剩余定理 (Chinese remainder theorem)

$m_1, m_2, \ldots, m_n$是大于1且两两互素的整数，

$a_1, a_2, \ldots, a_n \in \mathbb{Z}$，则同余方程组

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

有唯一的模$m = m_1 m_2 \ldots m_n$的解

例

- 求解“物不知数”问题

$$x \equiv 2 \ (\mathrm{mod}\ 3)$$
$$x \equiv 3 \ (\mathrm{mod}\ 5)$$
$$x \equiv 2 \ (\mathrm{mod}\ 7)$$

- 中国剩余定理
- 反向替换法 (back substitution)

费马小定理

- 费马小定理 (Fermat's little theorem)
  - 若p为素数，
    - $p \nmid a$，则$a^{p-1} \equiv 1 \pmod{p}$
    - 对任意整数a，$a^p \equiv a \pmod{p}$

例

- 用费马小定理计算 $7^{222} \bmod 11$

- 若p为素数，
  - $p \nmid a$，则$a^{p-1} \equiv 1 \pmod{p}$
  - 对任意整数a，$a^p \equiv a \pmod{p}$

素数的判定

- 若n不能被任何$\leq \sqrt{n}$的素数整除，则n是素数
  - 效率较低，需要得到$\sqrt{n}$以内所有素数
- 筛法
  - 可以求出n以内所有素数，但效率更低

素数的判定

- 若n不能被任何$\leq \sqrt{n}$的素数整除，则n是素数
  - 效率较低，需要得到$\sqrt{n}$以内所有素数
- 筛法
  - 可以求出n以内所有素数，但效率更低
- 素数测试方法
  - 古代数学家认为满足 $2^{n-1} \equiv 1 \pmod{n}$ 的都是素数
  - 费马小定理：素数都满足
  - 满足上式的合数称作以2为基数的伪素数 (pseudoprime)
  - 如：341

伪素数

- 伪素数 (pseudoprime)
  - b是正整数，若n是合数且$b^{n-1} \equiv 1 \pmod{n}$，则称$n$是以$b$为基数的伪素数
  - 费马小定理：素数一定满足
  - 用不同的b进行测试，可以筛选掉更多的合数
  - 伪素数比素数稀疏得多，小于10^{10}的素数超过4×10^8个，伪素数不到2×10^4个

卡米切尔数

- 卡米切尔数 (Carmichael number)
  - 设n为合数，若$b^{n-1} \equiv 1 \pmod{n}$对满足$\gcd(n, b) = 1$的$b$都成立，则称$n$是卡米切尔数

例

- 证明561是卡米切尔数

- 设n为合数，若$b^{n-1} \equiv 1 \pmod{n}$对满足$\gcd(n, b) = 1$的$b$都成立，则称$n$是卡米切尔数

卡米切尔数

- 卡米切尔数 (Carmichael number)
  - 设n为合数，若$b^{n-1} \equiv 1 \pmod{n}$对满足$\gcd(n, b) = 1$的$b$都成立，则称$n$是卡米切尔数
  - 几乎可以通过所有$b^{n-1} \equiv 1 \pmod{n}$型的测试
  - 只有找到n的因子才会不通过测试
    - 比遍历$\leq \sqrt{n}$的素数更低效

原根

- 原根 (primitive root)
  - p为素数，若$\mathbb{Z}_p$中每个非零数都可以写成r的幂次，则r是模素数p的一个原根

例

- Prove that 2 is a primitive root of 11.
- Prove that 3 is not a primitive root of 11.

- p为素数，若$\mathbb{Z}_p$中每个非零数都可以写成r的幂次，则r是模素数p的一个原根

原根

- 原根 (primitive root)
  - p为素数，若$\mathbb{Z}_p$中每个非零数都可以写成r的幂次，则r是模素数p的一个原根
  - 性质：每个素数都有原根

离散对数

- 离散对数 (discrete logarithm)
  - p为素数，r是其原根，$a \in \mathbb{Z}_p$且非零
  - 若$r^e \bmod p = a$且$e \in \mathbb{Z}_p$，则称e是以r为底a模p的离散对数
  - 记作$\log_r a = e$ (需指定p)

- 原根的定义保证了离散对数的存在性

例

- 计算模11下$\log_2 3$和$\log_2 5$

- p为素数，r是其原根，$a \in \mathbb{Z}_p$且非零
- 若$r^e \bmod p = a$且$e \in \mathbb{Z}_p$，则称e是以r为底a模p的离散对数
- 记作$\log_r a = e$ (需指定p)

离散对数

- 离散对数 (discrete logarithm)
  - p为素数，r是其原根，$a \in \mathbb{Z}_p$且非零
  - 若$r^e \bmod p = a$且$e \in \mathbb{Z}_p$，则称e是以r为底a模p的离散对数
  - 记作$\log_r a = e$ (需指定p)

- 离散对数至今没有高效算法
  - 可以用于密码学中

大纲

- 整除和模
- 整数表示和算法
- 素数和最大公约数
- 同余方程
- 同余的应用 (4.5)
- 密码学

散列函数

- 散列函数 (hashing function)
  - 将键 (key, 可理解为一种编号) 映射到内存地址的函数
  - 若内存大小为m，$h(k) = k \bmod m$是一类常用的散列函数，满射可以用到所有内存

例：冲突

- Let $h(k) = k$ **mod** 111. This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:
  - h(064212848) = 064212848 **mod** 111 = 14
  - h(037149212) = 037149212 **mod** 111 = 65
  - h(107405723) = 107405723 **mod** 111 = 14
    - 有冲突，存在下一个空余内存是一种可行的方法

伪随机数

- 伪随机数 (Pseudorandom Number)
  - 通过特定方法生成的看起来像随机数的数

伪随机数

- 线性同余法 (linear congruential method)
  - 选择4个整数
    - 模数m
    - 倍数a：$2 \le a < m$
    - 增量c：$0 \le c < m$
    - 种子x_0：$0 \le x_0 < m$
  - 生成伪随机数序列
    - $x_{n+1} = (ax_n + c) \bmod m$
  - 调整范围
    - 如需[0,1]之间随机数，则取x_n/m即可

伪随机数

- 线性同余法 (linear congruential method)
  - 选择4个整数
    - 模数m
    - 倍数a：$2 \leq a < m$
    - 增量c：$0 \leq c < m$
    - 种子x_0：$0 \leq x_0 < m$
  - 生成伪随机数序列
    - $x_{n+1} = (ax_n + c) \bmod m$
  - $m = 2^{31} - 1, a = 7^5, c = 0$是计算机中使用的一种参数选取，可以不重复地生成$2^{32} - 2$个数

校验码

- 校验码 (check digit)
  - 为了检查数字串正确性而额外添加的数字

例：身份证

步骤1：加权求和

对前17位数字，分别乘以对应的**权重因子**。

权重因子从左到右为：

$$[2^{17}, 2^{16}, 2^{15}, \ldots, 2^{1}] \mod 11$$

实际使用的固定权重数组为：

$$[7, 9, 10, 5, 8, 4, 2, 1, 6, 3, 7, 9, 10, 5, 8, 4, 2]$$

步骤2：计算余数

$$Y = S \mod 11$$

步骤3：根据余数确定校验码

表格

Y 值	0	1	2	3	4	5	6	7	8	9	10
校验码	1	0	X	9	8	7	6	5	4	3	2

大纲

- 整除和模
- 整数表示和算法
- 素数和最大公约数
- 同余方程
- 同余的应用
- 密码学 (4.6)

古典密码学

- 加密 (encryption)
  - 尤利乌斯·恺撒把每个字母正向移动三位
  - 字母B移到E，而字母X移到A
  - 加密是对信息进行保密处理的过程
  - 称为恺撒密码 (Caesar cipher)

  - 将字母对应到$\mathbb{Z}_{26}$，就得到了数字密文
  - 加密函数是 $f(p) = (p + 3) \bmod 26$

例

例 1 用恺撒密码从消息“MEET YOU IN THE PARK”产生的秘密消息是什么？

解 首先用数代替消息中的字母。得到

12 4 4 19　　24 14 20　　8 13　　19 7 4　　15 0 17 10

现在，再把每个数 p 替换成 $f(p)=(p+3) \bmod 26$。可得

15 7 7 22　　1 17 23　　11 16　　22 10 7　　18 3 20 13

再把这个翻译成字母产生加密消息“PHHW BRX LQ WKH SDUN”。

古典密码学

- 加密 (encryption)
  - 尤利乌斯·恺撒把每个字母正向移动三位
  - 字母B移到E，而字母X移到A
  - 加密是对信息进行保密处理的过程

- 解密 (decryption)
  - 把每个字母反向移动三位
  - 解密是从密文恢复原消息的过程

古典密码学

- 位移密码 (shift ciphers)
  - 加密： $f(p) = (p + k) \bmod 26$
  - 解密： $f^{-1}(p) = (p - k) \bmod 26$

古典密码学

- 位移密码 (shift ciphers)
  - 加密：$f(p) = (p + k)$ **mod** 26
  - 解密：$f^{-1}(p) = (p-k)$ **mod** 26

- 仿射密码 (affine ciphers)
  - 加密：$f(p) = (ap + b)$ **mod** 26
  - 当且仅当$\gcd(a, 26) = 1$时f可逆
    - 解密：$f^{-1}(p) = \bar{a}(p - b) \bmod 26$
  - 解密的结果可能不唯一，需要通过语义判断

古典密码学

- 密码分析 (cryptanalysis)
  - 不知道加密方法及其密钥时，破译密码的过程
  - 密钥：比如位移密码中的位移位数
  - 不知道加密方法时，破译极其困难
  - 知道使用了位移加密时可以遍历26种密钥，通过明文语义判断哪种是正确的
  - 也可以利用字母频率：E 13%、T9%、A8%、08%、17%、N7%、S7%、H 6%、R6%

古典密码学

- 换位密码 (transposition cipher)
  - 取一个正整数m
  - 取一个{1,2,…,m}上的一个置换σ（双射）
  - 将明文每m位作为一组，组内用σ打乱位置

例

例 6 利用基于集合{1，2，3，4}上的置换 σ 的换位密码，其中 $\sigma(1)=3$，$(2)=1$，$\sigma(3)=4$，$\sigma(4)=2$。

(a)加密明文消息 PIRAT E ATTACK。

(b)解密密文消息 SWUE TRAE OEHS，这是由该密码加密的。

解 (a)首先将明文中的字母划分为 4 个字母一组。得到 PIRA TEAT TACK。要加密每个分组，我们把第一个字母移到第三位，把第二个字母移到第一位，把第三个字母移到第四位，再把第四个字母移到第二位。得到 IAPR ETTA AKTC。

(b)注意，σ 的逆置换 σ^{-1} 把 1 变为 2，2 变为 4，3 变为 1，4 变为 3。对每个分组应用 σ^{-1} (m)可得明文 USEW ATER HOSE。(将这些字母重新分组形成常用词汇，我们猜测明文是 USE WATER HOSE。)

古典密码学

- 换位密码 (transposition cipher)
  - 取一个正整数m
  - 取一个{1,2,…,m}上的一个置换σ（双射）
  - 将明文每m位作为一组，组内用σ打乱位置
  - 当明文长度不是m倍数时，可以用随机字母补足
  - 不能用词频进行破译
  - 是一种特殊的分组密码 (Block Ciphers)

密码系统

- 密码系统 (Cryptosystems)
  - 密码系统是五元组 (P,C,K,E,D)
    - P (plaintext)：明文串的集合
    - C (ciphertext)：密文串的集合
    - K (key space)：密钥的集合
    - E (encryption)：加密函数的集合
    - D (decryption)：解密函数的集合

- $D_k\left(E_k(p)\right) = p$

公钥密码学

- 私钥密码系统 (private key cryptosystems)
  - A使用密文向B发送信息时，A和B需要共享一个密钥，A用于加密，B用于解密
  - 该密钥不能被其他人知道，否则可以很快破译密文
  - 需要消息发送人和接收人同时保密

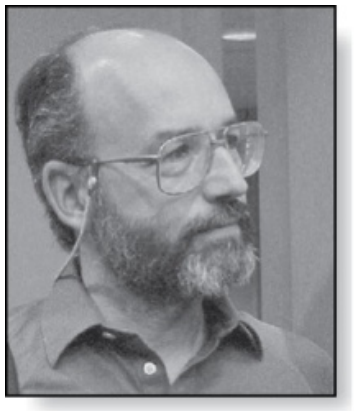
公钥密码学

- 私钥密码系统 (private key cryptosystems)
  - A使用密文向B发送信息时，A和B需要共享一个密钥，A用于加密，B用于解密
  - 该密钥不能被其他人知道，否则可以很快破译密文
  - 需要消息发送人和接收人同时保密
- 公钥密码系统 (Public Key Cryptography)
  - 知道加密密钥后，无法解密密文
  - 可以公开加密密钥，只要消息接收人保密解密密钥即可

公钥密码学

- RSA密码系统
  - 1976年由MIT的三位研究者发明

Ronald Rivest
(Born 1948)



Adi Shamir
(Born 1952)

Leonard Adelman
(Born 1945)

公钥密码学

- RSA加密
  - 选取加密密钥(n, e)
    - $n = pq$是两个大素数的乘积
    - e满足$\gcd\big(e, (p-1)(q-1)\big) = 1$
  - 明文翻译为整数序列
    - A -> 00 , … , Z -> 25
    - 2N位一组，N尽量大，但2N位的2525…25不超过n
  - 计算密文
    - 明文整数M的密文C为

$$C = M^e \bmod n$$

例

例 8 用 RSA 密码系统及密钥(2537，13)为消息 STOP 加密。注意 $2537=43\cdot 59$，$p=43$ 和 $q=59$ 是素数，并且

$$\gcd(e,(p-1)(q-1)) = \gcd(13,42\cdot 58) = 1$$

解 为了加密，先把 STOP 的字母翻译成等价的数字。然后按 4 位数字一组对这些数字分组(因为 $2525<2537<252\,525$)，得到

$$1819 \quad 1415$$

用下面的映射对每组加密

$$C = M^{13} \bmod 2537$$

用快速模乘法计算，可得 $1819^{13} \bmod 2537=2081$ 及 $1415^{13} \bmod 2537=2182$。加密后的消息为 2081 2182。 ◀

公钥密码学

- $n = pq$，$\gcd\big(e, (p-1)(q-1)\big) = 1$
- $C = M^e \bmod n$

- RSA解密
  - 若已知$de \equiv 1 \big(\bmod (p-1)(q-1)\big)$，则

$$C^d \equiv M \ (\bmod n)$$

公钥密码学

- RSA密码系统
  - 加密容易
    - 找300多位的素数p和q
    - 找与(p-1)(q-1)互素的e
  - 知道p和q时解密容易
    - 用欧几里得算法计算e的逆
    - 用快速模幂算法解密
  - 知道(n,e)很难计算p和q
    - 600多位的n，截止2017年最高效的质因数分解方法需十亿年

密码协议

- 密码协议 (Cryptographic Protocols)
  - 安全完成公用密钥交换的过程
  - Alice和Bob可以如下生成共享密钥

1) Alice 和 Bob 同意使用一个素数 p 和 p 的一个原根 a。
2) Alice 选择一个秘密整数 k_1，并将 $a^{k_1} \bmod p$ 发送给 Bob。
3) Bob 选择一个秘密整数 k_2，并将 $a^{k_2} \bmod p$ 发送给 Alice。
4) Alice 计算 $(a^{k_2})^{k_1} \bmod p$。
5) Bob 计算 $(a^{k_1})^{k_2} \bmod p$。

  - 共享的$p, a, a^{k_1} \bmod p, a^{k_2} \bmod p$都可以公开
  - 私有的$k_1, k_2, a^{k_1 k_2} \bmod p$都保密

数字签名

- 数字签名 (Digital Signatures)
  - A声称向B发送了消息，B如何确认的确是A发的？
  - A用解密函数加密信息M，将$D_{(n,e)}(M)$发送给B
  - B有公钥(n, e)，可以使用加密函数计算

$$E_{(n,e)}\left(D_{(n,e)}(M)\right) = M$$

从而得到密文，密文即可确认是A发送

总结

- 同余方程
  - 线性同余方程
    - 两侧同乘逆
  - 线性同余方程组
    - 中国剩余定理
    - 反向替换法
  - 费马小定理
    - 可快速计算幂的模
  - 原根和离散对数