密码与技术

–计算机密码学理论与应用

第一部分：数学基础（1）

$$ed = 1 \bmod \varphi(N)$$

$$Y = M^e \bmod N$$

$$M = Yd \bmod N$$

计算机安全理论的数学基础

- 整数的算术理论
- （1）同余等价关系及其基本性质
- （2）基本定理和公式：
- Euclid定理及等价形式、一次同余式方程；
- 中国余数定理；
- Fermat公式和Euler公式；
- 二次剩余理论及应用
- 有限域的基本理论及应用
- 素域F_p和扩域F_{p^d}的重要性质

Euclid定理的同余等价关系(1)

- 关于整数的一些基本概念：

- (1) Z表示全体整数的集合。
- (2)对任何整数a和b，符号(a,b)表示其最高公因子，$a|b$表示b能被a整除，$|a|$表示a的位数。
- 例：2|6, 17|51, 9|81；(4,6)=2, (24, 36)=6, (16,35)=1等。
- (3)多个整数的最高公因子$(a_1,\ldots,a_N)$

Euclid定理的同余等价关系(2)

- Euclid第一定理
- 任给整数a和b，必存在唯一的整数q和r满足$a=bq+r$及$0\le r<b$。

- 更完整的陈述
- 存在多项式算法A，任给整数a和b，A计算出整数q和r满足$a=bq+r$及$0\le r<b$，且A的计算复杂度不超过$\max(|a|^3,|b|^3)$次乘法运算。

Euclid定理的同余等价关系(3)

- (1) Euclid第二定理
- 任给整数a和b，总存在整数x和y(但不唯一)满足 $ax+by=(a,b)$

- (2) 更完整的陈述
- 存在多项式算法A，任给整数a和b，A计算出整数x和y满足 $ax+by=(a,b)$ ，且A的计算复杂度不超过$max(|a|^3,|b|^3)$次乘法运算。

- (3) 有用的特例
- 对互素的整数a和b，存在整数x和y(但不唯一)满足 $ax+by = 1$

- (4) 推广的形式：
- 任给整数$a_1,\ldots,a_N$，总存在整数$x_1,\ldots,x_N$满足 $a_1x_1+\ldots+a_Nx_N=(a_1,\ldots,a_N)$。

- 例：$2x+7y=1$ 有解$x=-3$，$y=1$； $4x+6y=2$有解$x=-1$，$y=1$.

- 注：本节相应的算法，可参阅教程第四章。

Euclid定理的同余等价关系(4)

- Euclid第二定理的证明
- 对整数a和b，考虑集合$M_{a,b}=\{ax+by: x$和y取遍所有整数$\}$，**d^***是$M_{a,b}$中的最小正数。于是：
- (1)d^*是a的因子。事实上，由Euclid第一定理，总存在整数q和$0\le r<d^*$且使$a=qd^*+r$，进而
- $r=a-qd^*=a-q(ax^*+by^*)=(1-qx^*)a-(qy^*)b$ 属于$M_{a,b}$（为什么？）
- 但这是不可能的，除非r=0（为什么？），即d^*是b的因子。
- (2)同理，d^*也是b的因子。因此d^*是a、b的公因子。
- (3)对a和b的任何公因子d，d必是d^*的因子（为什么？）。
- 因此，$(a,b)=d^*=ax^*+by^*$，x^*、y^*是某两个整数。证毕。

- 【习题】沿袭以上论证，证明推广形式的Euclid第二定理。

Euclid定理的同余等价关系(5)

- 为表述Euclid定理的第二个等价形式，先引进同余等价的概念和同余符号。
- 同余等价关系的定义：
- 任给整数N、a和b，如果存在整数q满足$a=qN+b$，则称“a和b模N同余”，记做$a=b \bmod N$，N称为模数或模。

- 注：这里不要求$0 \le b < N$。
- 例子：$11=3 \bmod 8=-5 \bmod 8$，$7 = -1 \bmod 8 = 23 \bmod 8$，$12=30 \bmod 9$；
- $7 \neq 24 \bmod 8$，$12 \neq -5 \bmod 9$.

Euclid定理的同余等价关系(6)

- 同余等价关系的重要性质【习题：验证之】
- (1) 同余关系是一个等价关系，即
-     a = a mod N; 若a=b mod N则b=a mod N；
-     若a=b mod N且b=c mod N则a=c mod N。
- (2)同余等价关系保持算术运算，即若$a_i=b_i$ mod N, $m\in$Z，i=1,2, 则
-     (i) $(a_1\pm a_2)$ mod N = (a_1 mod N $\pm$ a_2 mod N) mod N = $(b_1\pm b_2)$ mod N;
-     (ii) (a_1a_2) mod N = ((a_1 mod N)(a_2 mod N)) mod N，
-     (iii) $a_1a_2= b_1b_2$ mod N;
-     (iv) $f(a)=f(b)$ mod N，f(x)是任意给定的整系数多项式。

Euclid定理的同余等价关系(7)

- Euclid第三定理是关于求解一次同余方程式的规律。
- (1)例： $4x = 3 \bmod 5$ 在Z_5={0,1,2,3,4}内的解x=2且唯一。
- $4x = 3 \bmod 6$ 在Z_7={0,1,2,3,4}内的无解。
- $4x = 4 \bmod 8$ 在Z_8={0,1,2,3,4,5,6,7}内有多个解x=3和x=7。
- (2)Euclid第三定理：
- 任给整数N、a和b，线性同余式$ax=b \bmod N$存在整数解x当且仅当$(a,N)|b$，且这时恰有(a,N)个解$0\le x<N$。
- 特别地，若a、N互素则$ax=b \bmod N$总存在且有唯一的整数解x，满足$0\le x<N$。
- (3)注：存在多项式复杂度算法A求解方程$ax=b \bmod N$，参见教程第四章。
- (4)练习 (i)根据上述定理，重新检验(1)中的例子。
- (ii)应用上述定理，判定以下方程是否有解：
- $15x = 5 \bmod 25$， $15x = 6 \bmod 25$， $12x = 7 \bmod 19$， $12x = 7 \bmod 21$.

Euclid定理的同余等价关系(8)

- Euclid第三定理的证明概要：

- (1)如果$(a,\mathrm{N})|b$，记$d=(a,\mathrm{N})$，根据Euclid第二定理，存在u和v使得au+Nv=d，两端乘以整数k=b/d（为什么k是整数？）得
- $$a(ku) + (kv)N = kd = b$$
- 因此方程ax=b modN有解x=ku（为什么？）

- (2)若存在x满足方程$ax=b$ mod N，根据同余等价关系的涵义，这意味着存在整数x和y满足$ax - b$ = yN，即b = ax – yN，因此a和N的任何公因
- 子d整除 b（为什么？）。

- 注：在$(a,\mathrm{N})=1$的情形，经常记$ax=1$ mod N 的解x为a^{-1} *mod* N，称为a的逆。
- 例：3·7 = 1 mod 20，9·9 = 1 mod 10，5x=1mod 7, 16y=1mod 9，x和y=？
- 【用试探性算法即可】

中国余数定理（1）

-
- (1) 考虑以下问题：任意给定两两互素的一组整数m_1、…、m_n以及整数a_1、…、a_n，令$M=m_1\ldots m_n$，在集合$Z_M=\{0,1,2,\ldots,M-1\}$上求整数x，使之满足线性同余式组
- $$x = a_i \bmod m_i,\ i=1,\ldots,n。$$
- (2) x的求解公式：
- $$\boxed{x = \sum_{i=1}^{n} a_i M_i y_i \bmod M}$$
- 其中$M_i=m_1\ldots m_{i-1}m_{i+1}\ldots m_n$, y_i是方程$M_i y_i=1 \bmod m_i$的整数解。
- 注意M_i和m_i互素（为什么？），因此由关于线性同余方程的Euclid定理知$M_i y_i=1 \bmod m_i$必有解y_i而且y_i唯一。
-

中国余数定理（2）

- 求解公式的证明：
- $(a_1M_1y_1 + a_2M_2y_2 + \ldots + a_nM_ny_n) \bmod m_1$
- $= a_1M_1y_1 \bmod m_1 + a_2M_2y_2 \bmod m_1 + \ldots + a_nM_ny_n \bmod m_1$
- $= a_1\ (M_1y_1 \bmod m_1) \bmod m_1$
- $+\ a_2y_2(M_2 \bmod m_1) + \ldots + a_ny_n(M_n \bmod m_1)$
- $= a_1 + 0 + \ldots + 0 = a_1$
- 同理 $(a_1M_1y_1 + a_2M_2y_2 + \ldots + a_nM_ny_n) \bmod m_i = a_i$
- 对任何i成立，因此$a_1M_1y_1 + a_2M_2y_2 + \ldots + a_nM_ny_n$确是一个解。
- 例：求在$Z_M=\{0,1,2,\ldots,M-1\}$集合内求整数x使得 x=2 mod4, x=3 mod5。
- 解：M=4乘以5=20，$M_1=5$，$M_2=4$；
- 解$5y_1 = 1 \bmod 4$，$4y_2 = 1 \bmod 5$，得$y_1=1$，$y_2=4$；
- 代入中国余数定理的前述公式计算得x=(2·5·1+3·4·4) mod 20 = 58 mod 20 = 18.

中国余数定理（3）

- 习题【每周的习题，在下周五前提交到指定的信箱】
- 1 用中国余数定理求解以下方程（任意选做三题），解法参阅下页的例题：

(1) x=1 mod 7, x=5 mod 9, x=3 mod 11

(2) x=4 mod 7, x=1 mod 9, x=2 mod 11

(3) x=3 mod 5, x=5 mod 7, x=3 mod 12

(4) x=2 mod 5, x=3 mod 7, x=1 mod 12

(5) x=1 mod 5, x=1 mod 7, x=1 mod 19

2 m_1、…、m_n是两两互素的一组正整数，f(x)是一个整系数多项式，整数a_1、…、a_n使$f(a_i)=0$ mod m_i, i=1,…,n。令$M=m_1…m_n$，证明：若整数x满足线性同余式组$x=a_i$ mod m_i, i=1,…,n，则$f(x)=0$ mod M。

- 提示：利用前述同余关系保持算术运算这一性质，并注意x的多项式无非就是对x实施乘法和加法运算的结果。
-
- 3 运用Euclid定理判定一下方程是否存在解：

(1) 7x= 1 mod 11　(2) 9x=7 mod 10　(3) 5x=3 mod 12　(4) 2x=3 mod 16　(5) 6x=3 mod 19

应用CRT(chinese Remainder Theorem)的例题

- **例一**：求满足一元线性同余式组的整数x：
- $x=1 \bmod 2,\ x=2 \bmod 3,\ x=3 \bmod 5;$

- 第一步：$M_1=m_2m_3=3\cdot5=15$; $M_2=m_1m_3=2\cdot5=10$; $M_3=m_1m_2=2\cdot3=6$;
- 第二步：解线性同余式 $M_1y_1=1 \bmod m_1$，即 $15\,y_1 = 1 \bmod 2$ 得 $y_1 = 1$;
- 解线性同余式 $M_2y_2=1 \bmod m_2$，即 $10y_2 = 1 \bmod 3$ 得 $y_2 = 1$;
- 解线性同余式 $M_3y_3=1 \bmod m_3$，即 $6y_3 = 1 \bmod 5$ 得 $y_3 = 1$;
- 第三步：计算$X = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$
- $= 1\cdot15\cdot1 + 2\cdot10\cdot1 + 3\cdot6\cdot1 = 15+20+18 = 53$。
- 第四步：计算$\boldsymbol{x} = X \bmod m_1m_2m_3 = 53 \bmod 30 = \underline{23}$.

- **例二**：给定两两互素的一组整数m_1、…、m_n以及任意的整数a_1、…、a_n，令$M=m_1\ldots m_n$，在集合$Z_M=\{0,1,2,\ldots,M-1\}$ 上满足CRT方程组$a_i \bmod m_i,\ i=1,\ldots,n$的整数$x$是唯一的。
- 证明概要：首先，这等价于证明在以上条件下 $x = 0 \bmod m_i,\ i=1,\ldots,n$ 在Z_M上仅有唯一的解$x=0$（为什么？）；其次，根据同余等价关系的定义和m_j彼此互素，说明 $M|x$ 必成立。