网络空间安全数学基础复习纲要

> *---NonoTion*

根据考试范围整理，主要是基础知识和老师考前发的练习题

一、整除、同余的基本性质

PartI 整除

1. 整除的概念

设a,b是两个任意的整数，其中b≠0，如果存在一个整数q使得

$$a = q \cdot b$$

成立，则称b整除a，记作b|a，否则则称b不整除a。

2. 整除的基本性质

- 传递性

$a|b, c|b,$ 则$c|a$

- 加减法运算中，整除性质保持

$c|a$，$c|b,$ 则$c|a \pm b$

- 线性组合中，整除性质保持

$c|a, c|b$，则$c|sa \pm tb$

- a|b,b|a,则a=±b

3. 素数以及相关性质

素数的概念

设整数n≠ $0, \pm 1$。除了显然因数±$1, \pm n$以外没有其他因数，那么，n就叫做**素数**，否则n叫做合数

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

Eratoshenes筛法

设n是正整数，如果对所有的素数$p \le \sqrt{n}$, 都有p不整除n，则n一定是素数

素数的平凡判别

对于给定的整数N，设不大于$\sqrt{N}$的所有素数$p_1, \ldots p_s$都不能整除N，则N是素数

4. 最大公因数

最大公因数的概念

设$a_1 \ldots a_n$是n个整数，若整数d是它们中每一个数的因数，则d叫做它们的一个公因数，其中最大的一个叫做最大公因数，记作$(a_1, \ldots, a_n)$

性质:

- (0,b)=b
- 设a,b,c是不全为0的三个整数，如果a=q·b+c，则(a,b)=(b,c)

证明:

设d=(a,b),d`=(b,c)

则有 d|a,d|b,c=a-qb,所以d|d`

同理可得d`|d

所以d=d`

5. 最大公因数的进一步性质

- a,b是任意两个不全为0的整数，则d是整数a，b的最大公因数的充要条件是

(I)d|a,d|b

(II)若e|a,e|b,则e|d

- 设a,b是任意两个不全为0的整数，则有

(I)若m是任一正整数，则(ma,mb)=m(a,b)

(II)若非零整数d满足,d|a,d|b,则$\left(\frac{a}{d},\frac{b}{d}\right)=\frac{(a,b)}{|d|}$

证明：

(I)

设d=(ma,mb),d`=(a,b);

d`=sa+tb;

md`=sma+tmb;

则有d=md`

(II)

(a,b)=($|d|\frac{a}{|d|}$, $|d|\frac{b}{|d|}$)=|d|($\frac{a}{|d|}$, $\frac{b}{|d|}$)

将|d|移到左边，则II得证

- 设a,b,c是三个整数，其中b，c不等于0，如果(a,c)=1,则(ab,c)=(b,c)
- 形如$2^\alpha-1$的整数及其最大公因数

$(2^\alpha-1,2^\beta-1)=2^{(\alpha,\ \beta)}-1$

6. 整除的进一步性质及最小公倍数

性质:

- c|ab,(a,c)=1,则c|b
- p是素数，p|ab，则p|a或p|b

最小公倍数

a,b的最小公倍数记作[a,b]

性质:

- (a,b)=1,则[a,b]=ab
- 最小公倍数和最大公因数的关系

(a,b)[a,b]=a·b

证明：

设(a,b)=d

则$(a/d,b/d)=1$

[a/d,b/d]=a*b/(d^2)*

*进而[a,b]=a*b/d

7. 素数的算术基本定理

任一一个大于1的整数可以表示为素数的成绩

素数的标准分解式

任一整数n>1可以唯一地表示成

$$n=p_1^{\alpha_1}....p_s^{\alpha_s}$$

应用：

$$n=p_1^{\alpha_1}....p_s^{\alpha_s}$$

d是n的正因数当且仅当有因数分解式

$$d=p_1^{\beta_1}....p_s^{\beta_s}$$

- 求最大公因数和最小公倍数

$a=p_1^{\alpha_1}....p_s^{\alpha_s}$

$b=p_1^{\beta_1}....p_s^{\beta_s}$

(a,b)=$\prod_{i=1}^{s}p_i^{min(\alpha_i,\beta_i)}$

[a,b]=$\prod_{i=1}^{s}p_i^{max(\alpha_i,\beta_i)}$

素数定理

$\pi(x)$表示小于x的素数个数

Part II 同余

1. 同余的概念

给定一个正整数m，两个整数a，b关于模m同余，当且仅当m|a-b

记作a=b(mod m)（等号书写时一般为三条横线，为了方便用=代替）

2. 性质

- 模同余是一种等价关系，具有自反性，对称性，传递性
- a，b模m同余当且仅当a，b被m除得的余数相同
- 设m是一个正整数，设a_1,a_2,b_1,b_2是四个整数且$a_1=b_1$(mod m), $a_2=b_2$(mod m)

则:

$a_1+a_2=b_1+b_2$(mod m)

$a_1\times a_2=b_1\times b_2$(mod m)

- d·a=d·b（mod m) ,如果(d,m)=1,则a=b(mod m)

证明：

m|da-db

因为(d,m)=1

所以m|a-b

则a=b(mod m)

- a=b(mod m),如果整数d|(a,b,m),则

$$\frac{a}{d}=\frac{b}{d}(mod\frac{m}{d})$$

证明:

m|a-b

d|a d|b d|m

m/d |a/d-b/d

得证

- 设a=b(mod m),如果d|m,则 a=b(mod d)

证明:

m|a-b

d|m

所以d|a-b（整除的传递性）

得证

- a=b(mod m)，则(a,m)=(b,m)

设(a,m)=d (b,m)=d`

d|a,d|m

a-b=qm

b=a-qm

所以d|b

d|d`

同理可得d`|d

则d=d`

3. 剩余类及完全剩余系

借助同余对全体整数进行分类

剩余类和剩余系

C_a叫做模m的a的剩余类，一个剩余类中的任一数叫做该类的剩余或代表元，若$r_0...r_{m-1}$是m个整数，且两两不在同一个剩余类中，则称这m个整数为模m的剩余系

$C_a=[c|c\in Z,c=a(modm)]$

模m的剩余类有m个

完全剩余系

设m是一个正整数，则m个整数

$r_0...r_{m-1}$为模m的一个完全剩余系的充要条件是它们模m两两不同余

设m是正整数，（a,m)=1，b为任一整数，若k遍历m的一个完全剩余系，则

ak+b也遍历m的一个完全剩余系

简化剩余系

一个模m的剩余类叫做简化剩余类，当且仅当该类中存在一个与m互素的剩余，这时这个类中的剩余叫做简化剩余

在模m的所有简化剩余类（φ(m)个,欧拉函数后面会提到）中，从每个类任取一个数组成的整数的集合叫做模m的一个简化剩余系

Part III 练习题

1. 正合数n的最小正因子p，则p一定是素数，且p≤ $\sqrt{n}$

证明:

先用反证法证明p一定是素数

假设p不是素数

根据素数的基本算数定理

存在一个素数q<p 使得q|p

根据整除的传递性

因为p|n

所以q|p,这与p是正合数n的最小正因子矛盾

所以p一定是素数

再证$p \leq \sqrt{n}$

p|n 所以n=$n_1 \times$q

$0 < p \leq n_1 < n$

所以$n \geq p^2$

进而 p≤ $\sqrt{n}$

---

2. 用厄尔托斯筛法寻找200以内的素数

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

101 103 107 109 113 127 131 137 139 149

151 157 163 167 173 179 181 191 193 197 199

---

3. 7 | n, 5 | n,则 35|n

证明:

解法1:

7|n,5|n，且(7,5)=1

则合数n的标准分解式中含有项

7^{α_1}和5^{α_2}

$\alpha_1 \geq 1, \alpha_2 \geq 1$

所以

$n = q \times 7^{\alpha_1 - 1} \times 5^{\alpha_2 - 1} \times 35$(q为正整数)

所以35|n

解法2：

7|n,5|n

n=7q1

5|7q1

所以5|q1

q1=5q

所以n=35q

所以35|n

---

4. 假设n，a，b是三个c≠0，如果c|an,c|bn,如果(a,b)=1,求证c|n

证明:

使用反证法证明

假设c不整除n

c|an,则c|a

因为(a,b)=1

所以c不整除bn

这与题设矛盾

故c整除n

---

5. 如果a是整数，则a^3-a被3整除

解法1：

证明:

设$n=a^3-a=(a-1)a(a+1)$

n的一个因数分解式为三个连续的整数相乘

三个连续的整数一定有一个数会被三整除

所以3|n

即3|a^3-a

解法2：

证明

3的一个完全剩余系为0,1,2

$a^3-a=(a-1)a(a+1)$

a-1,a,a+1 模3两两不同余，是3的一个完全剩余系

故a-1，a，a+1中一定有一个数x与0属于同一个剩余类，即3|x

所以$3|a^3-a$

---

6. 奇整数的平方具有形式8k+1

证明:

设一个奇整数m,一个偶数n

m=2n+1

m*m=(2n+1)(2n+1)=$4n^2+4n+1$

证明 m具有形式8k+1

只需证明8|$4n^2+4n$即可

当n=0，8|0显然成立

假设n=h时，8|$4h^2+4h$成立

当n=h+1时

$4(h+1)^2+4(h+1)=4h^2+4h+8h+8$

由归纳假设可知8|$4h^2+4h$,并且显然8|8h+8

所以8|$4(h+1)^2+4(h+1)$

所以8|$4n^2+4n$

$4n^2+4n=8k$

$m^2=4n^2+4n+1=8k+1$

得证

---

7. a,b,q,r是整数，如果a=q*b+r,证明(a,b)=(b,r)

证明：

设d=(a,b),d`=(b,r)

r=a-q*b,所以d|r 所以d|d`

a=q*b+r,所以d`|r

所以d`|d

所以d=d`

即(a,b)=(b,r)

得证

---

8. 假设 a，b 是两个非零正整数，证明（a , b）*[a , b] = a * b。

设(a,b)=d

因为$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

所以$\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{ab}{d^2}$

进而[a,b]=$\frac{ab}{d}$

即(a,b)[a,b]=ab

得证

二.欧几里得除法求最大公因数

Part I 欧几里得除法

1. 欧几里得除法

设a,b是两个整数，其中b>0,则存在唯一整数q，r使得

$$a = q \times b + r$$

设a.b.c是三个不完全为0的整数，如果

$$a = q \times b + c$$

则(a,b)=(b,c)

2. 广义欧几里得除法

设a,b是两个整数，记$r_{-2} = a, r{-}1 = b$，反复运用欧几里得除法 有

$$r_{-2} = q_0 r_{-1} + r_0$$

$$r_{-1} = q_1 r_0 + r_1$$

$$\ldots$$

$$r_{n-1} = q_{n+1} r_n + r_{n+1} \;\; r_{n+1} = 0$$

r_n就是a，b的最大公因数

3.贝祖等式

设a,b是任意两个正整数，则存在整数s，t使得

$$sa + tb = (a, b)$$

贝祖等式的证明过程(求解s,t)

j	s_j	t_j	q_{j+1}	r_{j+1}
-3				a
-2	1	0		b
-1	0	1	q_0	r_0
0	s_0	t_0	q_1	r_1
...	...	...	...	...
n-1	s_{n-1}	t_{n-1}	q_n	r_n
n	s_n	t_n	q_{n+1}	$r_{n+1} = 0$

$s = s_n, t = t_n$

对于j=0,1,2...n

$s_j = -q_j s_{j-1} + s_{j-2}$

$t_j = -q_j t_{j-1} + t_{j-2}$

$q_{j+1} = [\frac{r_{j-1}}{r_j}]$

$r_{j+1} = -q_{j+1} r_j + r_{j-1}$

Part II 练习题

9. 运用广义欧几里得除法求整数 s，t 使得 *s167* + *t*335 = （167，335）

列表求解:

j	s_j	t_j	q_{j+1}	r_{j+1}
-3				335
-2	1	0		167
-1	0	1	2	1
0	1	-2	167	0

所以s=-2,t=1 这里因为s在较小数前面，所以要换一下位置

三、如何构造两个互素的整数

$$(\frac{a}{(a,b)},\frac{b}{(a,b)})=1$$

四、逆元计算方法

$$ab=1\ (mod\ m)$$

则称b为a模m的逆元

如何求解逆元，扩展欧几里得除法

sa+tm=1 s就为a模m的逆元

五、欧拉函数计算

Part I 欧拉函数

设m是一个正整数，则m各整数1，2，3，...,m-1,m中与m互素的元素个数，记作$\varphi(m)$

通常叫做欧拉函数

对于素数幂有$\varphi(m) = p^{\alpha} - p^{\alpha-1} = m\prod_{p|m}(1-\frac{1}{p})$

Part II 欧拉函数的性质

设m,n是互素的两个正整数,则

$$\varphi(mn) = \varphi(m)\varphi(n)$$

设正整数的标准因数分解式为

$$m = \prod_{p|m} p^{\alpha} = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$$

则

$$\varphi(m) = m\prod_{P|m}(1-\frac{1}{p})$$

设m是一个正整数，则

$$\sum_{d|m} \varphi(d) = m$$

用于原根的构造

六、欧拉定理、费马小定理

Part I欧拉定理

若(a,m)=1 则有

$$a^{\varphi(m)} = 1(mod\, m)$$

Part II 费马小定理

对于任意整数a

$$a^p = a(mod\, p)$$

Part III 练习题

12. p,q是两个不相等的大素数,n=pq,选择整数e使得(e,φ(n))=1,计算d使得ed=1(mod φ(n)),对于任意的整数

$m \in [1, n-1]$证明$m^{ed} = m(mod\, n)$

证明:

φ(n)=(p-1)(q-1)

ed=k(p-1)(q-1)+1

由欧拉定理有

$m^{\varphi(p)} = m^{(p-1)} = m(mod\, p)$

$m^{ed} = m^{k(p-1)(q-1)+1} = [m^{(p-1)}]^{k(q-1)} m = 1^{(q-1)} m = m(mod\, p)$

同理可得

$m^{ed} = m(mod\, q)$

又因为p,q都为素数

所以

$m^{ed} = m(mod\, pq)$即$m^{ed} = m(mod\, n)$

七、RSA 加密解密过程及证明

Step I 生成公钥和私钥

1. 寻找两个不相等的大素数p，q
2. 将p，q相乘，得到一个大合数N
3. 计算N的欧拉函数T=$\varphi(N) = (p-1)(q-1)$
4. 选择一个整数E<T,使得E，T互质，作为一个密钥
5. 求出EmodT的逆元D，作为另一个密钥
6. 计算得出N,E,D三个数据，(N,E)作为公钥，(N,D)作为私钥

Step II 用公钥加密信息

设所需加密的明文为M，密文为C

$$M^E(mod\, N) = C$$

Step III 用私钥解密信息

$$C^D(mod\, N) = M$$

证明：证明$M^{ED} = M(mod\, N)$即可，就是上面的练习题12

八、中国剩余定理求解同余方程

Part I 同余式

1. 同余式的基本概念

设m是一个正整数，有多项式

$$f(x) = a_n x^n + \ldots + a_1 x + a_0$$

其中ai是整数则

$$f(x) = 0 \ (mod\ m)$$

叫做模m同余式，n叫做f(x)的次数，记作degf

2. 一次同余式的求解

设m是一个正整数,m不整除正整数a，则

$$ax = 1(mod\ m)$$

有解的充分必要条件是(a,m)=1,且其解为1

$$ax = b(mod\ m)$$

有解的充分必要条件是(a,m)|b,其解为

$$x = \frac{b}{(a,m)}((\frac{a}{(a,m)})^{-1}(mod\ \frac{m}{(a,m)})) + t\frac{m}{(a.m)}(mod\ m)$$

Part II 中国剩余定理

设$m_1....m_k$是k各两两互素的正整数，则对任意的整数$b_1...b_k$同余式组

$$x=b_1(mod\,m_1)$$

$$x=b_2(mod\,m_2)$$

$$\dots$$

$$x=b_k(mod\,m_k)$$

一定有解，且解是唯一的，其解的形式为:

（1）令M_i=$\prod_{j\neq i}m_j$

(2)$M_i^`$为M_i模m_i的逆元

(3)m=$\prod_{i=1}^{k}m_i$

$$x=\sum_{i=1}^{k}b_iM_iM_i^`\ (mod\,m)$$

Part III 练习题

11. x=2 mod 7, x=3 mod 5 ,利用中国剩余定理求x mod 35

$$5\times 3=1(mod\,7)$$

$$7\times 3=1(mod\,5)$$

所以

$$x=2\times 5\times 3+3\times 7\times 3=93(mod\,m)$$

---

13. 求解同余方程33x=22 (mod 77)

原方程等价于

3x=2 (mod 7)

3x=1(mod 7)的一个特解为 x=5

3x=2 (mod 7)的一个特解为 x=10

通解为 x=10+$\frac{77}{(33,77)}t$=10+7t;

t=0,1,2,3,4,....

九、二次同余式和平方剩余

Part I二次同余式与平方剩余

1. 二次同余式的一般形式

$$ax^2+bx+c=0(mod\, m)$$

其中a≠0(mod m)

2. 平方剩余

设m是正整数，若同余式

$$x^2=a(mod\, m)\ (a,m)=1$$

有解，则a叫做模m的平方剩余(或二次剩余)；否则，a叫做模m的平方非剩余（或二次非剩余）

3.欧拉判别条件

设p是奇素数，(a,p)=1,则a是模p的平方剩余的充分必要条件是

$$a^{\frac{p-1}{2}} = 1(mod\, p)$$

4. 勒让德符号

$(\frac{a}{p})$=1 若a是模p的平方剩余

=-1，若a是模p的平方非剩余

0，p|a

周期性:

$$(\frac{a+p}{p}) = (\frac{a}{p})$$

完全可乘性:

$$(\frac{a \cdot b}{p}) = (\frac{a}{p})(\frac{b}{p})$$

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$$

5. 二次互反律

若p,q为互素奇素数

$$(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(\frac{p}{q})$$

Part II 练习题

14. 计算 60mod 137 是否为平方剩余

$$(\frac{60}{137})=(\frac{2}{137})(\frac{2}{137})(\frac{3}{137})(\frac{5}{137})$$

$$(\frac{2}{137})=(-1)^{(\frac{137^2-1}{8})}=1$$

$$(\frac{3}{137})=(-1)^{(\frac{3-1}{2})(\frac{137-1}{2})}(\frac{137}{3})=(\frac{2}{3})=(-1)^{(\frac{3^2-1}{8})}=-1$$

$$(\frac{5}{137})=(-1)^{(\frac{5-1}{2})(\frac{137-1}{2})}(\frac{137}{5})=(\frac{2}{5})=(-1)^{(\frac{5^2-1}{8})}=-1$$

$$\text{所以}(\frac{60}{137})=1$$

60是模137的平方剩余

十、原根与指数的基本定理与性质

Part I 原根与指数

1. 指数

设m>1是整数，a是与m互素的正整数，则使得

$$a^e=1\ (mod\ m)$$

成立的最小正整数e叫做a对模m的**指数**，记作$ord_m(a)$

当且仅当e=φ(m)时，a叫做模m的**原根**

2. 指数的基本性质

设m>1是整数，a是与m互诉的整数，则整数d使得

$$a^d = 1(mod\, m)$$

的充要条件是

$$ord_m(a)|d$$

特别地，有

$$ord_m(a)|\varphi(m)$$

即a模m的指数一定整除φ(m)，通过这个性质可以更方便地求出指数

若b=a(mod m),则ordm(b)=ordm(a)

$a^0, a^1, ..., a^{ordm(a)-1}$模$m$两两不同余，

特别的，当ordm(a)=φ(m)时，构成模m的简化剩余系

$$a^d = a^k(mod\, m)$$

的充分必要条件是 d=k(mod m)

$$ord_m(a^d) = \frac{ord_m(a)}{(d, ord_m(a))}$$

如果模m存在一个原根g，则模m有φ(φ(m))个不同的原根

3. 大指数的构造

如果(ordm(a),ordm(b))=1,则

$$ord_m(ab) = ord_m(a)ord_m(b)$$

设m,n都是大于1的整数，a是与m互素的整数，则

若n|m,则ordn(a)|ordm(a)

若(m,n)=1,则

$$ord_{mn}(a) = [ord_m(a)ord_n(a)]$$

Part II 练习题

10. 写出模 11 的简化剩余系，并列举每个简化剩余的阶（ord11）

x	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$ord_m(x)$	1	10	5	5	5	10	10	10	5	5

φ(11)=10=2x5

15. p 是奇素数，证明在模 p 的简化剩余系中，平方剩余与平方非剩余的个数 都是**p−1/2** 个

平方剩余个数等于同余式

$$x^{\frac{p-1}{2}} = 1(mod\, p)$$

的解数，且

$$x^{\frac{p-1}{2}} - 1|x^{p-1} - 1$$

此同余式的解数为p-1/2,故平方剩余的个数为p-1/2,所以平方非剩余的个数为p-1/2

十一、素数的确定性判别算法

厄氏筛法

十二、素数的概率性判别算法

1. 伪素数

设n是一个奇合数，如果整数b，(b,n)=1使得同余式

$$b^{n-1} = 1(mod\ n)$$

成立，则n叫做基于b的伪素数

2. 伪素数的性质

n是对于基b的伪素数当且仅当b模n的阶整除n-1

n是基于b1,b2的伪素数，则n是基于b1xb2的伪素数

如果n是基于b的伪素数，则n也是基于b^{-1}的伪素数

如果有一个整数b使得上式不成立，则模n的简化剩余系中至少有一半数使得上式不成立

3. **Fermat**素性检验

给定奇整数n>=3和安全参数t

(1)随机选取整数b，(n,b)=1，2<=b<=n-2

(2)计算r=b^{n-1}(mod n)

(3)如果 r!=1,则n是合数

(4)上述过程重复t次

若通过t次的费马素性检验，n是素数的可能性大于1-$\frac{1}{2^t}$

4.Miller-Rabin素性检验

设n是奇素数，且有n-1=2^st

则有下列因数分解式

$$b^{n-1}-1=(b^{2^{s-1}t}+1)(b^{2^{s-2}t}+1)\dots(b^t+1)(b^t-1)$$

如果有同余式

$$b^{n-1}=1(mod\,n)$$

则下列同余式至少有一个成立

$$b^t=1(mod\,n)$$

$$b^t=-1(mod\,n)$$

$$b^{2t}=-1(mod\,n)$$

$$\dots$$

$$b^{st}=-1(mod\,n)$$

如果有一个数能使这些式子全部不成立，则n是合数

Miller-Rabin素性检验

给定奇整数n>=3和安全参数k

写n-1=2^st,其中t是奇整数

(1)随机选取整数b,2<=b<=n-2

(2)计算r0=b^t(mod n)

(3) a.如果r0=1或r0=n-1，则通过检验，可能为素数，回到(1),继续选取另一个随机整数b

b.否则，计算r1=r_0^2(mod n)

(4) a.如果r1=n-1，则通过检验，可能为素数，回到(1),继续选取另一个随机整数b

b.否则，计算r2=r_1^2(mod n)

如此继续下去

(r+2)a.如果r_{s-1}=n-1，则通过检验，可能为素数，回到(1),继续选取另一个随机整数b

b.否则，n为合数

两个素性检验的过程就为最后一道题的答案