第3章 信息安全数学基础

东南大学 网络空间安全学科
胡爱群 教授/博导
二O一九年十月八日

主要内容

- 素数、素数性质 、大素数生成方法;
- 同余、中国剩余定理;
- 群、环、域、有限域的概念。

素数

定义：设正整数$n \neq 0$, 1。如果除了1和n外，n没有其它因数（因子），则n是素数（或质数、不可约数）。否则，n叫合数。

- 素数总是指正整数，通常写成 p.

例子：

2，3，5，7都是素数，而4，6，10，15，21都是合数。

互素的概念

- 设$a_1,\cdots,a_n$是$n(n\geq2)$个整数，若整数d是它们中每一个数的因数，那么，d叫做$a_1,\cdots,a_n$的公因数。
- 如果$a_1,\cdots,a_n$不全为零，则$a_1,\cdots,a_n$的所有公因数中最大的一个叫做最大公因数，记作$gcd(a_1,\cdots,a_n)$，或$(a_1,\cdots,a_n)$。
- 特别地，当$(a_1,\cdots,a_n)=1$时，称$a_1,\cdots,a_n$互素或互质。（也就是说$a_1,\cdots,a_n$没有公因数。）

整除

a,b是整数，p是素数

✓ $(a,b)=(b,a)$;
✓ 如果 $b|a$，则（a,b）$=b$;
✓ 如果 $p\nmid a$，则（p,a）$=1$,即互素。

素数的判定和生成

定理：

设n是一个正整数，如果对所有的素数$p \le \sqrt{n}$，都有$p \nmid n$，则n一定是素数。

该定理提供了一个寻找素数的方法（平凡除法）：

✓ 从1到n的整数中，删除$p \le \sqrt{n}$的所有素数$p_1, p_2, \ldots, p_k$的倍数（不含自己），余下来的数就是不大于n素数。

例子：求所有不超过100的素数。

解：

$\sqrt{100} = 10$，不超过10的素数有：2，3，5，7

从1-100中，依次删除所有2，3，5，7的倍数的数，余下的数就是不超过100的素数。

例子： 证明N=137为素数。

证明：

$\sqrt{137} < 12$ 的素数有2，3，5，7，11，依次用此数去除137，发现都不能整除。

根据前述的素数判定定理，可以判定137为素数。

练习：判断139为素数还是合数？

同余的概念

定义：

给定一个正整数m和两个整数a、b，如果a-b被m整除，则a和b同余，记为$a \equiv b \ mod(m)$。

定理：

设m是一个正整数，a、b是两个整数，则$a \equiv b \ mod(m)$的充要条件是：存在一个整数k，使得a=b+km。

练习：39=4 mod(7)；61=5 mod(7).

Euler函数

定义：

设m是一个正整数，把1,...,m-1中与m互素的数的个数记作$\varphi(m)$，$\varphi(m)$就叫做Euler函数。

- 对正整数m，欧拉函数是小于或等于m的正整数中与m互质的数的数目.
- 如果m是一个素数，则$\varphi(m)=m-1$。

例：$\varphi(1)=1$； $\varphi(8)=4$，因为1,3,5,7均和8互质

定理：

设m、n是两个互素的正整数，则$\varphi(mn)=\varphi(m)\varphi(n)$.

练习： 求$\varphi(10)$=？ $\varphi(77)$=?

Euler函数的推论

设p、q是不同的素数，

则　　　　　　（1）$\varphi(pq)=pq-p-q+1$.

设$n=pq$，则（2）如果知道n和$\varphi(n)$，就可求出p和q.

提示：

$$\begin{cases} p+q=n+1-\varphi(n) \\ p\cdot q=n \end{cases}$$

可求解该二元方程组得到p和q.

练习：证明素数的性质（1）和（2）。

Euler定理

- 设m是大于1的整数，$\varphi(m)$是m的Euler函数。如果a是满足（a,m）=1的整数，则
$$a^{\varphi(m)} \equiv 1\ mod(m)$$

练习：验证 2^{10}=1 mod(11)。

解：m=11, a=2, $\varphi(m)$=10, (2,11)=1，根据Euler定理，上式成立。

也可以这样做：2^{10}=1024=1023+1=93*11+1=1 mod(11)

Fermat定理

设p是一个素数，则对任意一个整数a，有$a^p \equiv a\ mod(p)$.

证明：

1）如果a被p整除， 则a=0 mod(p), a^p=0 mod(p) $\Rightarrow a^p \equiv a\ mod(p)$.

2）如果a不能被p整除，则（a, p）=1. 又p为素数，有$\varphi(p)=p-1$.

根据Euler定理，$a^{\varphi(p)}$=1 mod(p) $\Rightarrow a^p=a^{p-1}a\equiv a$ mod(p).

练习：p=17, a=4, 4^{17}=4 mod (17)

大素数的生成

- 逐个查找太费时间，可以利用Euler定理进行检验，称为Fermat素性检验。
- Euler定理：设n是大于1的整数，$\varphi(n)$是n的Euler函数。如果a是满足（a,n）=1的整数，则 $a^{\varphi(n)} \equiv 1\ mod(n)$

✓ 如果n是一个素数，则$\varphi(n)=n-1$, 有$a^{n-1}=1 \bmod(n)$.

✓ 反过来说，如果有一个整数a, 且（a, n）=1, 使得$a^{n-1}\neq 1 \bmod(n)$, 那么n是一个合数，不是素数。

例子：n=63. 假定a=2, $2^{62}=2^{60}\bullet 2^2=(2^6)^{10} \bullet 2^2=\underbrace{64^{10}}_{=1 \bmod(63)} \bullet 2^2\neq 1 \bmod(63)$

因此63不是素数。

素性检验

给定奇数$n \geq 3$，

- 随机选取整数b, $2 \leq b \leq n-2$;
- 计算$r = b^{n-1} \pmod{n}$;
- 如果$r \neq 1$, 则n是合数;
- 重复上述过程t次。

注意：上述方法可以检验出来是合数，但若满足$r=1$的n未必是素数。但如果满足欧拉定理，则必然是素数。

练习：$n=561$是合数，但依然满足$r=1$.
提示：$561=3 \cdot 11 \cdot 17$

中国剩余定理

“韩信点兵”问题：有兵一队，若列成五行纵队，则末行1人；列成六行纵队，则末行五人；列成七行纵队，则末行4人；列成十一行纵队，则末行十人。求兵数。

解：设有x人，则上述问题可用同余式组表示：

$$\begin{cases} x \equiv 1\ mod(5) \\ x = 5\ mod(6) \\ x = 4\ mod(7) \\ x = 10\ mod(11) \end{cases}$$

如何求解上述同余式组？

中国剩余定理：

设 $m_1,m_2,\ldots,m_k$ 是 k 个两两互素的正整数，则对任意的整数 $b_1,b_2,\ldots,b_k$,

同余式组 $\begin{cases} x = b_1 \, mod(m_1) \\ x = b_2 \, mod(m_2) \\ \quad\quad \cdots \\ x = b_k \, mod(m_k) \end{cases}$ 一定有解,

且其解为:$x = M_1'M_1b_1+\cdots+M_k'M_kb_k \, mod(m)$ 。

其中 $m=m_1m_2\ldots m_k$, $m=m_iM_i$, $M_i'M_i = 1 \, mod(m_i)$, $i=1,2,\ldots,k$.

求解韩信点兵问题：

$$\begin{cases} x \equiv 1\ mod(5) \\ x = 5\ mod(6) \\ x = 4\ mod(7) \\ x = 10\ mod(11) \end{cases} \Rightarrow$$

$m_1=5, m_2=6, m_3=7, m_4=11.\ b_1=1, b_2=5, b_3=4, b_4=10.$

m=5 · 6 · 7 · 11=2310

M_1=6 · 7 · 11=462, M_2=5 · 7 · 11=385,

M_3=5 · 6 · 11=330, M_4=5 · 6 · 7=210.

根据$M_i' M_i = 1\ mod(m_i)$ =>$M_1' = 3, M_2' = 1, M_3' = 1, M_4' = 1$

代入： $x = M_1' M_1 b_1 + \cdots + M_k' M_k b_k\ mod(m)$ =2111 mod(2310)

即共有2111个士兵。

利用中国剩余定理求解大的幂次数

求 x=$2^{1000000}$ mod(77)

解: 77=7·11, 求x等价于求$\begin{cases} x = b_1 \, mod(7) \\ x = b_2 \, mod(11) \end{cases}$

由Euler定理，$2^{\varphi(7)} = 2^6 = 1 \, mod(7); 2^{\varphi(11)} = 2^{10} = 1 \, mod(11);$

因此 $b_1 = 2^{1000000} = (2^6)^{166666} \cdot 2^4 = 2 \, mod(7)$

$b_2 = 2^{1000000} = (2^{10})^{100000} = 1 \, \mathrm{mod}(11)$

运用中国余数定理，可以求得x=23 (mod 77)

Euclid除法及广义Euclid除法

- 任意两个整数a、$b(b>0)$，则对于任意的整数c， 存在唯一的整数q、r， 使得 $a=qb+r$，$c\le r\le b+c$. r为余数。

例子： 121=2·48+25；

例子：设a=169, b=121, 求a和b的最大公因子，即（a,b）=?

利用广义Euclid除法：

169=1·121+48

121=2 ·48+25

48=1 · 25+23

25=1 · 23+2

23=11 · 2+1

因此 （169， 121）=1.

RSA算法中私钥的计算

设有两个素数p=719, q=1283.

$n=p \cdot q=719 \cdot 1283=922477$

$\varphi(n)=\varphi(p)\ \varphi(q)=(p-1)(q-1)=920476$

随机选取整数$e=7$, $1<e<\varphi(n)$, 使得（e, $\varphi(n)$）=1.

公钥是$K_p=\{n,e\}$, 私钥为d, $1<d<\varphi(n)$，满足$e \cdot d=1 \bmod(\varphi(n))$，$d$=?

需要把上式写成：1=？$\cdot\varphi(n)+e\cdot d$

$\varphi(n)=920476=131496\cdot 7+4$

$7=2\cdot 4+(-1)$

在不知道p和q的情况下，求不出私钥d .

$1=-7+2\cdot 4$

$=(-1)\cdot 7+2\cdot$（$920476-131496\cdot 7$）

$=2\cdot 920476+$（-262993）$\cdot 7$

$=$（$2-7$）$\cdot 920476+$（$920476-262993$）$\cdot 7$

$=$（-5）$\cdot \underbrace{920476}_{\varphi(n)}+\underbrace{657483\cdot 7}_{d\bullet e}$ => $d=657483$

群的概念

定义：设G是一个具有结合法的非空集合，如果：

（1）满足结合律：

$$\forall a,b,c\in G,\ \text{都有}\ (ab)c=a(bc);$$

（2）G中存在单位元：

$$\exists e\in G,\ \text{对任意}a\in G\text{，都有}\ ae=ea=a;$$

（3）G中的元素具有可逆元：

$$\text{对任意}a\in G\text{，}\exists a^{-1}\in G,\ \text{使得}aa^{-1}=a^{-1}a=e.$$

G的结合法写作乘法时，G称为乘群；G的结合法写作加法时，G称为加群。

同态的概念

设G、G'是两个群，f是G到G'的一个映射，如果对任意的a、$b\in G$，都有

$$f(ab)=f(a)\mathrm{f}(b)$$

则f叫做G到G'的一个同态。

✓如果f是一个加密过程，即 $E(ab)=E(a)\mathrm{E}(b)$, 称为乘同态。
$E(a+b)=E(a)+E(b)$, 称为加同态。

环的概念

定义：

设R具有两种结合法（通常表示为加法和乘法）的非空集合，如果下列条件成立：

（1）R对于加法构成一个交换群；

（2）（结合律） $\forall a,b,c\in R$, 都有 $(ab)c=a(bc)$;

（3）（分配律） $\forall a,b,c\in R$, 都有$a(b+c)=ab+ac$;

则R叫做环。

有限域的概念

- ✓ 集合F={a，b，…}，对F的元素定义了两种运算：“+”和“*”，并满足以下3个条件：

（1）F的元素关于运算“+”构成交换群，设其单位元素为0；

（2）$F\backslash\{0\}$的元素关于运算“*”构成交换群。即F中元素排除元素0后，关于“*”法构成交换群。

（3）分配律成立，即对于任意元素a，b，$c \in F$，恒有

$a*(b+c)=(b+c)*a=a*b+a*c$。

- ✓ p是素数时，F\{0，1，2，…，p-1}，在mod p意义下，关于求和运算“+”及乘积“*”，构成了域。F域的元素数目有限时称为有限域, 记为GF(p)。
- ✓ 有限域元素的数目称为有限域的阶。

GF(p)有限域中的运算

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(a) 模5的加法

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(b) 模5的乘法

$p=5$

三大难解数学问题

1、大整数的因数分解问题

- 给定两个大的素数p、q, 计算乘积$p \cdot q=n$很容易；
- 给定大整数n，求n的素因数p、q，使得$n=p \cdot q$非常困难。

如：p=20000000000000002559, q=80000000000000001239是两个大素数，它们的乘积

n=1600000000000000229500000000000003170601

但要分解这个数很困难。

2、离散对数问题

已知有限循环群$G=<g>=\{g^k|k=0,1,2,\ldots\}$及其生成元$g$和阶$n=|G|$.

- 给定整数a, 计算元素$g^a=h$很容易；
- 给定元素h, 计算整数x, $0\le x\le n$, 使得$g^x=h$非常困难。

例如：给定p=200000000000000002559, g=11,a=20030428, 可以计算出g^a=1134889584997235257 (mod p)

但要求整数x, 使得g^x=1134889584997235257 (mod p) 非常困难。

3、椭圆曲线离散对数问题

已知有限域F_p上的椭圆曲线点群

$E(F_p)=\{(x,y)\in F_p\times Fp|y^2=x^3+ax+b,\ a,b\in F_p\}\cup\{O\}$

点$P=(x,y)$的阶为一个大的素数。

- 给定整数a, 计算点$Q=aP=(x_a, y_a)$很容易；
- 给定点Q，计算整数x, 使得 xP=Q非常困难。

将 n 写成二进制:

$$n = n_0 + n_1 2 + n_2 2^2 + \cdots + n_{k-2} 2^{k-2} + n_{k-1} 2^{k-1},$$

其中 $n_i \in \{0,1\}$, $i=0,1,\cdots,k-1$.

$$nP = n_0 P + n_1 2P + n_2 2^2 P + \cdots + n_{k-2} 2^{k-2} P + n_{k-1} 2^{k-1} P$$

$$nP = \underbrace{\underbrace{\cdots\underbrace{\underbrace{\underbrace{n_0 P_0}_{Q_0} + n_1 P_1}_{Q_1} + n_2 P_2}_{Q_2} + \cdots + n_{k-2} P_{k-2}}_{Q_{k-2}} + n_{k-1} P_{k-1}}_{Q_{k-1}}.$$

习题

1. 利用素数判定定理，求所有不超过110的素数.

2. 证明N=131为素数.

3. 求m=91的Euler函数$\varphi(91)$=?

4. 用Euler定理，验证 $2^{12}=1 \ mod(13)$.

5. 用中国剩余定理，求 $x=2^{100000} \bmod(55)$.