§3.4 整数与整除

一．整除 (Division)

1. 整除

定义：设a和b是整数且a, 我们说 (a divides b)，是说，存在整数c使得b=ac。当a整除b, 我们说a是b的因子(factor)并且b是a的倍数(multiple of a)，记作。若a不能整除b, 记作。

2. 例子：

例1：判定是否有。

解：因为7不是整数，所以，而故。

例2：设n和d是正整数。问有多少个不超过n的正整数可以被d整除？

解：能被d整除的正整数具有形式dk，其中k是正整数，不超过n可以被d整除的正整数的个数，就是满足的k的个数, 也就是满足的k的个数，即。

3. 整除的性质

定理1：设a, b, c是整数，那么

(i)如果，那么；

(ii)如果，那么a|bc对所有整数c成立；

(iii)如果且，那么。

证明：(i) 假设且，那么由定义知，存在整数s和t，使得b=as，c=at，故b+c=as+at=a(s+t)。从而。

(ii)和(iii)的证明类似。

推理1：如果a, b, c是整数且和，那么，其中m, n是任意整数。

二．除算法 (The Division Algorithm)

定理2：（除算法）设a是整数，d是一个正整数，那么存在唯一的整数q和r且，有。

定义：在除算法中，d称为除数(divisor)，a称为被除数(dividend), q称为商(quotient), r称为余数(remainder)。商和余数记为：。

例3：101除以11，商和余数是多少？

解：101 = 商是9，余数是2。

例4：除以3，商和余数是多少？

解：故商是，余数是1.

注意：余数必须是非负数，不能写成。

三．模算术 (Modular Arithmetic)

1. 模和余数

设a和b是整数，m是正整数，那么a和b模m同余 (a is congruent to b modulo m)，是说m整除，记为。若a和b模m不同余，记为。

2. 模m同余的充要条件

定理3：设a和b是整数，m是正整数。那么当且仅当a。

例5：判定17和5是否模6同余？24和14是否模6同余？

解：因为 17 故。

又因为不能被6整除，故。

定理4：设m是正整数。整数a和b模m同余当且仅当存在整数k使得。

证明：设。那么。故存在整数k，使得，从而有。

反过来，假设，对某个整数k成立，那么，从而有。故。

3. 模运算的性质

定理5：设m是正整数。如果且，那么且。

证明：因为和，因而存在整数s和t，使得且。因此

且

因此且。

例6：因为且，由定理知

且

推论2：设m是正整数，且a和b是整数。那么

且

证明：因为

由定理5知，

且。

四．同余的应用

1. 凯撒密码 (密码学(Cryptology))

将英文字母表中所有字母向前移3个位置，最前面的3个字母移到最后面3个位置。用字母表

D,E,F,G,H, I, J,K,L,M,N,O,P, Q,R,S,T,U,V,W,X,Y,Z,A,B,C对应

A,B,C,D,E,F,G,H,I, J, K, L,M,N,O,P,Q,R,S,T, U,V,W,X,Y,Z,

进行编码。

例如： MEET YOU IN THE PARK 编码为

PHHW BRX LQ WKH SDUN

假设用0, 1, 2,, 25给26个字母编号，凯撒密码用公式表示为： f(p)= (p+3)mod 26 , .

f(p)为加密函数(encryption function).

解密函数(decryption function)为：(p3)mod 26。

凯撒密码可以推广到更一般的形式：

其中a,b为整数，经过选取a,b，使得f(p)为{0,1,

{0,1,的双射函数。

§3.5 素数和最大公因子

一．素数 (primes)

1. 定义：一个大于1的正整数p被称为素数，是说，p只有正因子p和1。一个大于1的正整数q如果不是素数，则q被称为合数(composite)。

例1：整数7是素数，因为它只有因子7和1，而整数9是合数，因为它有因子3且3.

定理1（算术基本定理）：每一个大于1的正整数可以表示成一个素数，或可以表示成两个或更多的素数的乘积，其中这些素因子可以写成非递减的顺序。

例2：给出100，641，999和1024的素因子分解。

解：

。

定理2：如果n是一个合数，那么n有一个小于或等于的素因子。

证明：假设n是合数，那么n有一个因子a，，并且n可以写成n=ab，其中b是大于1的正整数。这时，有或。假若不然，有且，那么n=ab = n，矛盾。故有或。因为a和b都是n的因子，故n有一个不大于的因子a（或b）。而a（或b）要么是一个素数，要么由算术基本定理，a（或b）有一个小于a（或b）的素因子，在两种情况下，n都有一个小于或等于的素因子。

例3：证明101是素数。

证明：只要证101没有小于或等于的素因子即可。因为小于或等于的素数只有2,3,5,7，而2,3,5,7都不是101的因子，故101是素数。

2. 求整数n的素数因子分解

对于任一整数n，从最小的素数2开始，用从小到大不超过的素数去除n，若求得一个素因子p，那么再对，从p开始从小到大求不超过的素因子。如果又求得素因子q，再对，从q开始，从小到大求不超过的素因子，如此进行下去。最后可求出n的所有素因子。

例4：求7007的素因子分解。

解：从2开始，用从小到大的素数去除7007. 2,3,5都不能整除7007. 而7可以整除7007. 7是第一个素因子。再从7开始用素数去除, 这时有。故7是第2个素因子。再从7开始用素数去除, 这时找到, 故11是第3个素因子。再从11开始用素数去除 求出13是最后一个素因子。故7007的素因子分解为：

7007=。

3. 素数的无穷性 (The infinitude of primes)

定理3：存在无穷多个素数。

证明：反证法。假设只有有穷多个素数，设是所有的素数，那么令。由算术基本定理，Q应能表示成中某些素数的因子分解。但对任意，。这因为，假若，又有，故有。即，矛盾。故Q是一个素数且，i=。这与是所有素数的假设矛盾。

\*因为素数有无穷多个，人们试图列出尽可能大的素数（在密码学中有用）。已知的最大素数具有这样的表达式：, 其中p是一个素数，这种素数称为梅森数(Mersenn primes)。但并不是所有具有表达式的数都是素数。

例5：都是梅森数，但不是梅森数，因为2047=.

\*目前已知的最大的梅森数是这是一个9百万位10进位的数字。

定理4（素数定理）：不超过x的素数个数的频率是（当x趋于无穷）。

\*其中ln x是x的自然对数。

二．关于素数的公开问题与猜想

1. 哥德巴赫猜想：

任何一个大于5的奇数可以表示成3个素数的和。

等价命题：任何一个大于2的偶数可以表示成2个素数的和。

目前已知的最好结果：

（Ramare1995）: 任何一个大于2的偶数可以表示成至多6个素数的和。

（陈景润1966）：任何一个大于2的偶数可以表示成两个素数之和或一个素数和两个素数的乘积之和。

2. 孪生素数猜想：

有无穷多个孪生素数p和p+2。

例如：3和5， 5和7，11和13，17和19，4967和4969等。

三．最大公因子和最小公倍数

1. 最大公因子 (greatest common divisors)

定义：设a和b都是非零整数。最大整数d满足且，称为a和b的最大公因子，记作d=gcd(a, b)。

例10：24和36的最大公因子是什么？

解：24和36的正的公因子有1,2,3,4,6和12。因此gcd(24,36)= 12。

例11：17和22的最大公因子是什么？

解：17和22的公因子只有1. 故gcd(17,22)=1。

2. 两个整数互素

定义：如果两个整数a, b，满足gcd(a, b)=1，那么称a和b互素(relatively prime)。

例如：例11中，17和22互素。

定义：整数两两互素是说。

例13：10, 17, 21两两互素。

3. 求最大公因子的方法

已知两个整数a和b，由算术基本定理，a, b可表示成

其中可能为0.

那么

\*首先，上式右边的数可以整除a和b，其次，更大的数不能整除a或b。

例14：求120和500的最大公因子。

解：120=

4. 最小公倍数(least common multiple)

定义：正整数a和b的最小公倍数是能够被a和b整除的最小正整数。记作：lcm(a, b).

假设

那么

例15：求

解：

lcm(

。

定理5：设a, b是正整数，那么。

作业：

1. 证明：如果a, b是整数，并且且，那么a=b或a=。
2. 证明：如果且，其中a,b,c是整数，m是正整数，那么。
3. 找出以下数字的素因子分解：

（1）126 （2）729 （3）143

4. 求以下数对的最大公因子：

（1）

（2）66； 126

5. 证明：对每一个正整数n，存在n个连续的合数。