$3^{644} \mod 645$

$$2\,|\,644 \qquad 2\,|\,322$$

$(644)_{10} = (1010000100)_2$

644: 512 256 128 64 32 16 8 4 2 1

$644 = 512 + 132$, $132 = 128 + 4$

$a_0=0$, $x=1$, $power=3^2 \mod 645 = 9$

$a_1=0$ $x=1$ $power=9^2 \mod 645 = 81$

$a_2=1$ $x=1\cdot 81 \mod 645 = 81$ $power=81^2 \mod 645 = 111$

$a_3=0$ $x=81$ $power=111^2 \mod 645 = 66$

$a_4=0$ $x=81$ $power=66^2 \mod 645 = 486$

$a_5=0$ $x=81$ $power=486^2 \mod 645 = 126$

$a_6=0$ $x=81$ $power=126^2 \mod 645 = 396$

$a_7=1$ $x=(81\cdot 396) \mod 645 = 471$ $power=396^2 \mod 645 = 81$

$a_8=0$ $x=471$ $power=81^2 \mod 645 = 111$

$a_9=0$ $x=(471\cdot 111) \mod 645 = 36$

Chapter 5 Induction and recursion

拉梅定理：设a、b是满足a≥b的正整数，则欧几里得算法为了求出$\gcd(a,b)$而使用的除法的次数小于或等于b的十进制位数的五倍

Chapter 6 Counting

$$P(n,r) = \frac{n!}{(n-r)!}$$

$$C(n,r) = \frac{n!}{r!(n-r)!}$$

$$(a+b)^n = \sum_{j=0}^{n} C(n,j)\cdot a^{n-j} b^j$$

Vandermonde

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k} \qquad C_{m+n}^{r} = \sum_{k=0}^{r} C_m^{r-k}\cdot C_n^k$$

$$\binom{2n}{n} = \sum_{k=0}^{n}\binom{n}{k}^2 \qquad C_{2n}^{n} = \sum_{k=0}^{n}(C_n^k)^2$$

General

$$\sum_{1\le i\le n}|A_i| - \sum_{1\le i<j\le n}|A_i\cap A_j| + \sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k| - \cdots + (-1)^{n+1}|A_1\cap A_2\cap\cdots A_n|$$

有重复的组合

n个元素的集合中允许重复的r组合有 $C_{n+r-1}^{r} = C_{n+r-1}^{n-1}$ 个

隔板

5.54. 具有不可区别物体的集合的排列

类型1 n_1个 类型2 n_2个 ...

$$\frac{n!}{n_1!n_2!n_3!\cdots n_k!}$$

把n个不同的物体分配到k个不同的盒子使n_i个物体放入盒子i的方式

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

把物体放入盒子

可区别的物体与可区别的盒子

n个不同物体放入k个不同盒子 使得n_i个物体放入盒子i的方式数.

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

不可区别的物体与可区别的盒子

C_{n+r-1}^{n-1} 种方式 将r个不可区别的球放入n个可区别的盒子里

可区别的物体与不可区别的盒子

n个 放入k

$$\sum_{j=1}^{k} S(n,j) = \sum_{j=1}^{k}\sum_{i=0}^{j-1}(-1)^i\binom{j}{i}(j-n)^n$$

$$= \sum_{j=1}^{k}\sum_{i=0}^{j-1}(-1)^i C_j^i (j-n)^n$$

$S(n,j)$ n个可区别物体放入j个不可区别的盒子

$$\sum_{j=1}^{k} S(n,j) = \sum_{j=1}^{k}\frac{1}{j!}\sum_{i=0}^{j-1}(-1)^i C_j^i (j-i)^n$$