数论: 整数问题、素数问题、整除问题、同余问题

组合数学: 计数问题、置换群问题

1. 数论基础
2. 模方程：余数
3. **欧几里得算法：(最大公约数)**

int gcd(int a, int b) return b==0 ? a : gcd(b, a%b);

1. **扩展欧几里得算法：(二元一次不定方程)**

int extend\_euclid(int a, int b, int &x, int &y){

if(b==0) { x=1; y=0; return a; }

int d=extend\_euclid(b,a%b,x,y);

int t=x; x=y; y=t-a/b\*y; return **d**; }

其他解:(x0+kb’, y0-ka’) a’=a/gcd(a,b) b’=b/gcd(a,b)

1. **大整数取模：(1234567891011121314%2）**

scanf(“%s%d”, n, &m); int len = strlen(n); int ans=0;

for(i=0~len-1) **ans**=(int)(((long)ans\*10+n[i]-‘0’)%m);

1. **乘方取模/幂取模： （ ）**

int multimod (int a, int n, int m){

int tmp = a, res = 1;

while(n) {

if(n & 1) { res \*= tmp; res %= m; }

tmp \*= tmp; tmp %= m; n >>= 1; }

return **res**; }

1. **矩阵快速幂**

struct mat { int v[MAXN][MAXN]; };

mat e, ans;

mat matrix\_mul(mat p1, mat p2){

mat t; int i, j, k; memset(t.v, 0, sizeof(t.v));

for(i=0~N) for(j=0~N) if(p1.v[i][j]) for(k=0~N)

t.v[i][k] += (p1.v[i][j] \* p2.v[j][k]);

return t; } 结束

mat matrix\_mi(mat p, int k) {

mat t; memset(t.v, 0, sizeof(t.v));

for(int i=0; i<=N; i++) t.v[i][i] = 1;

while(k) {

if(k&1) t = matrix\_mul(t, p);

k >>= 1; p = matrix\_mul(p, p);

}

return t;}

1. 素数
2. 因数分解
3. 1