

Contents

1.1 快速 \mathbb{F} 1

1 Math

1 1.2 擴展歐基里德 1

1 Math

1.1 快速 \mathbb{F}

```
//x^y % p
int func(int x, int y, int p){
    int res = 1;
    while(y != 0){
        if(y%2==1){
            res *= x;
            res %=p;
        }
        x *= x;
        y /= 2; // 5^8 => (5^2)^4
        x %= p; // ((5^2) % 7)^4
    }
    return res;
}
```

1.2 擴展歐基里德

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

int lcm(int a, int b)
{
    return a * b / gcd(a, b);
}

pair<int, int> ext_gcd
(int a, int b) //擴展歐幾里德  $ax+by = gcd(a,b)$ 
{
    if (b == 0)
        return {1, 0};
    if (a == 0)
        return {0, 1};
    int x, y;
    tie(x, y) = ext_gcd(b % a, a);
    return make_pair(y - b * x / a, x);
}
```