

# Chapter 1 导言、算法分析与STL

---

## 1.1 OJ

---

- [Codeforces](#)
- [Virtual Judge](#)
- [牛客网 - 找工作神器 | 笔试题库 | 面试经验 | 实习招聘内推, 求职就业一站解决 牛客网](#)
- [AtCoder](#)
- [首页 - 洛谷 | 计算机科学教育新生态](#)
- [Welcome To PKU JudgeOnline](#)
- [Welcome to Hangzhou Dianzi University Online Judge](#)
- [力扣\(LeetCode\) 全球极客挚爱的技术成长平台](#)

## 1.2 Resources

---

- [OI Wiki - OI Wiki](#)

## 1.3 算法分析

---

- [复杂度简介 - OI Wiki](#)

### 1.3.1 渐进分析

1. 渐进记号在数学上实际是集合，**等于**实际上是**属于**或**包含**
2.  $\Theta$ 符号：

若存在正常量  $c_1$  和  $c_2$ ，使得对于足够大的  $n$ ，函数  $f(n)$  能“夹入”  $c_1 g(n)$  与  $c_2 g(n)$  之间，则  $f(n)$  属于集合  $\Theta(g(n))$ 。因为  $\Theta(g(n))$  是一个集合，所以可以记“ $f(n) \in \Theta(g(n))$ ”，以指出  $f(n)$  是  $\Theta(g(n))$  的成员。作为替代，我们通常记“ $f(n) = \Theta(g(n))$ ”以表达相同的概念。因为我们按这种方式活用了等式，所以你可能感到困惑，但是在本节的后面我们将看到这样做有其好处。

3.  $O$ 符号：表示函数的一个在常量因子内的上界
4.  $\Omega$ 符号：表示函数的一个在常量因子内的下界

### 1.3.2 求解递归式

1. 递归式的编写
2. 主方法解递归式：[主定理\(Master Theorem\) - 知乎](#)

## 1.4 STL

---

参考[C++ 参考手册 - cppreference.com](#)

## 1.5 Question

---

- 我们学习了三种渐进符号：渐进紧确界、渐进上界与渐进下界。那么使用这些渐进分析算法有什么意义呢？
- 为什么其中渐进上界是较为常用的渐进符号呢？
- 还有哪些算法分析方法？适用于哪些情况？

# Chapter 2 模拟、枚举与贪心

---

## 2. 1 模拟

---

- [P1138 第k小整数 - 洛谷 | 计算机科学教育新生态](#)
- [Problem - A - Codeforces](#)
- [Problem - B - Codeforces](#)
- [T539827 202411H Enemy - 洛谷 | 计算机科学教育新生态](#)

## 2.2 枚举

- 试除法: [【算法拾遗】试除法 - Trial Division - 知乎](#)
- [P2241 统计方形 \(数据加强版\) - 洛谷 | 计算机科学教育新生态](#)

## 2.3 贪心

- 部分背包: [算法设计与分析\\_中国大学MOOC\(慕课\)](#)
- [Problem - A - Codeforces](#)

# Chapter 3 双指针、滑动窗口

## 3.1 双指针

1. 快慢指针 [27. 移除元素 - 力扣 \(LeetCode\)](#)
2. 左右指针 [977. 有序数组的平方 - 力扣 \(LeetCode\)](#)

## 3.2 滑动窗口

1. [209. 长度最小的子数组 - 力扣 \(LeetCode\)](#)

# Chapter 4 高精度

见板子

# Chapter 5 二分、前缀和与差分

略

# Chapter 6 分治与搜索

## 6.1 分治

- 归并排序

## 6.2 搜索

- dfs本质上是n叉树前序遍历, bfs本质上是n叉树层序遍历
- 回溯时, 相关量的改变在递归返回是需要撤销
- dfs可以用stack实现 (或者说递归本来就是运行在栈上), bfs可以用queue实现
- 特别的, lambda表达式可用于实现递归, 相对来说较方便

# Chapter 7 数论

## 模运算

模运算是大数运算中常见的操作, 在算法竞赛中面对数据过大的时候, 题目往往需要给出需要取模的要求, 取模数一般为 $1e9 + 7$ 、 $1e9 + 9$ 、998244353。

这三个数比较大, 但小于int32位最大值, 并且三个数都是质数, 至于为什么要质数, 后面学习到其他算法会讲到。

定义取模运算为求 $a$ 除以 $m$ 的余数, 记作:

$$a \bmod m = a \% m$$

一般的取余都是正整数的操作, 对于负数求余数, 不同的编译语言结果可能不同。

取模的性质:

加:  $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

减:  $(a - b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$

乘:  $(a * b) \bmod m = ((a \bmod m) * (b \bmod m)) \bmod m$

对于除法取模是错误的, 除法取模需要使用“逆”, 在后续会讲到。

在运算过程中, 对于大数相乘取模, 会出现溢出的情况, 即 $a * b$ 或 $(a \bmod m) * (b \bmod m)$ 可能会发生溢出。

此时我们可以不直接计算 $a * b$ , 改为计算 $(a * 2 * 2 \dots 2 * 2) * (b / 2 / 2 \dots / 2 / 2)$ 直到 $b$ 减少为0为止。对于这种/2的操作我们可以采用二进制来处理。

但是如果 $b$ 是奇数的话,  $b / 2$ 会取整, 丢弃余数1, 所以要判断 $b$ 的奇偶性。

如果 $b$ 是偶数就是 $(a * 2) * (b / 2)$ 。

如果 $b$ 是奇数就是 $(a * 2) * (b / 2 + 1) = (a * 2) * (b / 2) + (a * 2)$ 。

```
1 long long mul (long long a, long long b, long long m)
2 {
3     a = a % m;
4     b = b % m;
5     long long res = 0;
6     while(b > 0)
7     {
8         if(b & 1) //判断奇偶
9             res = (res + a) % m;
10        a = (a + a) % m; //a*2
11        b >>= 1; //b向右边移动一位, 即去掉已经处理过的最后一位。
12    }
13    return res;
14 }
15 int main()
16 {
17     long long a = 0x7877665544332211;
18     long long b = 0x7988776655443322;
19     long long m = 0x998776655443322;
20     cout << a * b % m << '\n'; //318333883276991760
21     cout << mul(a, b, m); //411509877096934416
22 }
```

## 快速幂

对于幂运算求 $a^n$ , 如果我们直接一个一个的乘, 时间复杂度为 $O(n)$ 。如果使用快速幂, 时间复杂度为 $O(\log_2 n)$ 。

快速幂标准做法采用位运算实现, 下面介绍快速幂如何实现。

例如要计算 $a^{11}$ 。我们可以分成 $a^{11} = a^8 * a^2 * a^1$ 。其中8、2、1都是2的几次方, 得出二进制为1101。

那么如何把11分解成 $8 + 2 + 1$ ? 把 $n$ 按二进制处理即可。

遇到没有的幂次, 我们进行判断一下跳过就可以了, 比如 $a^{11}$ 中没有 $a^4$ , 检测到位为0, 即可跳过。

[P1226【模板】快速幂 - 洛谷 | 计算机科学教育新生态](#)

```
1 long long fastpow(long long a, long long b, long long mod)
2 {
3     long long ans = 1;
4     a = a % mod;
5     while(b)
6     {
7         if(b & 1) //检测最后一位是0还是1。
8             ans = (ans * a) % mod; //如果是1, 就乘以当前位数。
9         a = (a * a) % mod; //递推a的次方。
10        b >>= 1; //n向右边移动一位, 即去掉已经处理过的最后一位。
11    }
12    return ans;
13 }
```

# GCD和LCM

最大公约数(GCD)和最小公倍数(LCM)是比赛中的高频考点。

## 整除

定义： $a$ 能整除 $b$ ，记为 $a|b$ 。其中， $a$ 、 $b$ 为整数，且 $a \neq b$ ， $b$ 是 $a$ 的倍数。

性质：

- 1.若 $a$ 、 $b$ 、 $c$ 为整数，且 $a|b$ 、 $b|c$ ，则 $a|c$ 。
- 2.若 $a$ 、 $b$ 、 $m$ 、 $n$ 为整数，且 $c|a$ 、 $c|b$ ，则 $c|(ma + nb)$ ；

## GCD

GCD的定义：整数 $a$ 和整数 $b$ 的最大公约数能同时整除 $a$ 和 $b$ 的最大整数，记为 $\gcd(a, b)$ 。

例如： $\gcd(15, 81) = 3$ ， $\gcd(0, 0) = 0$ ， $\gcd(0, 3) = 3$ ， $\gcd(-6, -15) = 3$ 。 $-a$ 和 $a$ 的因子相同， $\gcd(a, b) = \gcd(|a|, |b|)$ 所以我们在比赛中只考虑正整数的GCD。

## GCD的性质

1.  $\gcd(a, b) = \gcd(a, a + b) = \gcd(a, k * a + b)$
2.  $\gcd(ka, kb) = k * \gcd(a, b)$
3. 定义多个整数的GCD:  $\gcd(a, b, c) = \gcd[\gcd(a, b), c]$
4. 若 $\gcd(a, b) = d$ ，则 $\gcd(a/d, b/d) = 1$ ，即 $a/d$ 与 $b/d$ 互素
5.  $\gcd(a + cb, b) = \gcd(a, b)$

## 求GCD

求GCD常用方法有很多种，这里我只介绍两种较为重要的。

### 1) 欧几里得

即辗转相除法， $\gcd(a, b) = \gcd(b, a \bmod b)$ 。

下面给出证明：

设整数 $a$ 和 $b(a > b)$ ，则有 $a = k * b + q$ ，其中 $a$ 、 $b$ 、 $k$ 、 $q$ 分别为被除数，除数，商和余数。

当 $q$ 为0，显然 $\gcd(a, b) = k$ 为 $k$ 。

当 $q$ 不为0，设 $a$ 和 $b$ 最大公约数为 $d$ 。则有 $a = d * k_1$ ， $b = d * k_2$ 。

由 $a = k * b + q$ 可以得到， $q = a - k * b = d * k_1 - k * k_2 * d = d(k_1 - k * k_2)$ 。

可以看出 $d$ 能整除 $q$ ，所以 $a$ 与 $b$ 最大公约数等于 $b$ 与 $q$ 最大公约数。

反之我们也需要证明，即 $a$ 和 $b$ 的最大公约数就是 $b$ 和 $q$ 的最大公约数。上面证明，我们得出 $d$ 是 $q$ 的一个因子。

已知 $q$ 是 $b$ 和 $d$ 的因子，那么 $q$ 就可以整除 $k * b + d$ 。此时 $a = k * d + b$ 就可以得到 $q$ 整除 $a$ 。

所以 $a$ 、 $b$ 中任意一个公因数也必定是 $b$ 、 $q$ 的任意一个公因数，即 $a$ 、 $b$ 的公因数集等于 $b$ 、 $q$ 的公因数集。那么两个集合里的最大值也相等。

[B4025 最大公约数 - 洛谷 | 计算机科学教育新生态](#)

```
1 int mygcd(int a, int b) //一直递归找gcd，回溯条件是b为0，此时可以得知gcd为a，因为gcd(a, 0)=a。
2 {
3     return b ? mygcd(b, a % b) : a;
4 }
```

另外，对于 C++17，我们可以使用 `<numeric>` 头中的 `std::gcd` 与 `std::lcm` 来求最大公约数和最小公倍数。

## 2) 更相减损术

即辗转相减法，由GCD的性质： $\gcd(a, b) = \gcd(b, a - b) = \gcd(a, a - b)$ 。用大数减去小数，把所得的差与较小的数比较，继续减法，直到减数与差相等。

```
1  int mygcd(int a,int b)
2  {
3      while(a != b)
4      {
5          if(a > b)
6              a = a - b;
7          else
8              b = b - a;
9      }
10     return a;
11 }
```

更相减损术避免了欧几里得取模计算，但是计算次数更多。由于避免了取模操作，所以常用于高精度计算GCD问题。

## LCM

$a$ 和 $b$ 的最小公倍数表示为 $\text{lcm}(a, b)$ 。

设 $a = p_1^{c_1} p_2^{c_2} \dots p_m^{c_m}$ ,  $b = p_1^{f_1} p_2^{f_2} \dots p_m^{f_m}$ , 则 $\gcd(a, b) = p_1^{\min\{c_1, f_1\}} p_2^{\min\{c_2, f_2\}} \dots p_m^{\min\{c_m, f_m\}}$ ,  
 $\text{lcm}(a, b) = p_1^{\max\{c_1, f_1\}} p_2^{\max\{c_2, f_2\}} \dots p_m^{\max\{c_m, f_m\}}$ 。于是可以得出 $\gcd(a, b) \text{lcm}(a, b) = ab$ 。

注意要先除法后乘法，防止溢出。

```
1  int lcm(int a,int b)
2  {
3      return a / gcd(a,b) * b;
4  }
```

## 裴蜀定理

定义：如果 $a$ 与 $b$ 都为整数，则有整数 $x$ 和 $y$ 使 $ax + by = \gcd(a, b)$ 。

推论：整数 $a$ 与整数 $b$ 互素当且仅当存在整数 $x$ 和 $y$ ，使 $ax + by = 1$ 。

证明：使得 $ax + by = d$ ， $d$ 一定是 $\gcd(a, b)$ 的整数倍。因为

$a = \gcd(a, b) * k_1$ ,  $b = \gcd(a, b) * k_2$ ,  $ax + by = \gcd(a, b) * k_1 * x + \gcd(a, b) * k_2 * y = \gcd(a, b) * (k_1 * x + k_2 * y) = d$ 。

所以最小的 $d$ 是 $\gcd(a, b)$ 。

[P4549 【模板】裴蜀定理 - 洛谷 | 计算机科学教育新生态](#)

```
1  #include <iostream>
2  using namespace std;
3  int a[100003];
4  long long gcd(int a,int b)
5  {
6      return b ? gcd(b,a%b):a;
7  }
8  int main ()
9  {
10     int n;
11     int i;
12     cin>>n;
13     for(i = 0;i < n;i++)
14     {
15         cin>>a[i];
16     }
17     long long sum = 0;
18     sum = gcd(abs(a[0]),abs(a[1]));
19     for(i = 1;i < n;i++)
20     {
```

```

21     sum = gcd(abs(a[i]),sum);
22 }
23 cout<<sum;
24 }

```

## 二元线性丢番图方程

方程 $ax + by = c$ 成为二元性丢番图方程， $x$ 和 $y$ 是变量，其他是已知整数，问是否有整数解。

该方程是二维平面上的一条直线，如果直线上有整数坐标点，就有解，没有则无解，如果存在一个解就有无数个解。

**定理：**设 $a, b$ 为整数且 $\gcd(a, b) = d$ 。如果 $d$ 不能整除 $c$ ，那么方程 $ax + by = c$ 没有整数解，否则存在无穷多个解。如果 $(x_0, y_0)$ 是方程的一个特解，那么所有解可以表示为

$$x = x_0 + \frac{b}{d} * n,$$

$$y = y_0 - \frac{a}{d} * n,$$

$n$ 为任意整数。

例如：

(1) 方程 $18x + 3y = 7$ 没有整数解，因为 $\gcd(18, 3) = 3$ ，3不能整除7；

(2) 方程 $25x + 15y = 70$ 存在无穷个解，因为 $\gcd(25, 15) = 5$ 且5整除70，一个特解是 $x_0 = 4, y_0 = -2$ ，通解是 $x = 4 + 3n, y = -2 - 5n$ 。

**证明：**令 $a = da', b = db'$ ，有 $ax + by = d(a'x + b'y) = c$ 。如果 $x, y, a', b'$ 是整数，那么 $c$ 必须是 $d$ 的整数倍数，才有整数解。

对于通解的形式， $x$ 值按 $b/d$ 递增， $y$ 值按 $-a/d$ 递增。我们可以设 $(x_0, y_0)$ 是这条直线上的一个整数点，那么它移动到另一个点后的坐标为 $(x_0 + \Delta x, y_0 + \Delta y)$ 。此时 $\Delta x, \Delta y$ 必须是整数， $(x_0 + \Delta x, y_0 + \Delta y)$ 才是另一个整数点，我们知道这个直线必定通过原点，那么可以得到 $a\Delta x + b\Delta y = 0$ 。

那么 $\Delta x$ 最小值是多少？因为 $a/d$ 与 $b/d$ 互素，只有 $\Delta x = b/d, \Delta y = -a/d$ 时候，才为整数，并且满足 $a\Delta x + b\Delta y = 0$

## 扩展欧几里得

方程 $ax + by = \gcd(a, b)$ ，根据前一节的定理，它有整数解。扩展欧几里得算法求一个特解 $(x_0, y_0)$ 。

下面证明为什么可以得到特解。

已知 $ax + by = \gcd(a, b), bx' + (a\%b)y' = \gcd(b, a\%b)$ 。

那么 $ax + by = bx' + (a\%b)y' = bx' + (a - b(a/b))y' = ay' + b(x' - (a/b)y')$

所以可以得到 $x = y', y = x' - (a/b)y'$ 。

递归终止条件 $\gcd(a, 0) = a$ ，此时易知 $x=1, y=0$ 。

```

1  long long exgcd(long long a, long long b, long long &x, long long &y)
2  {
3      if(b == 0)
4      {
5          x = 1;
6          y = 0;
7          return a;
8      }
9      long long d = exgcd(b, a%b, y, x);
10     y -= a/b*x;
11     return d;
12 }

```

## 二元丢番图方程 $ax + by = c$ 的解

用扩展欧几里德算法得到 $ax + by = \gcd(a, b)$ 的一个特解后，再利用它求方程 $ax + by = c$ 的一个特解。步骤如下：

(1) 判断方程 $ax + by = c$ 是否有整数解，即 $\gcd(a, b)$ 能整除 $c$ 。记 $d = \gcd(a, b)$ 。

(2) 用扩展欧几里得算法求 $ax + by = d$ 的一个特解 $x_0, y_0$ 。

(3) 在 $ax_0 + by_0 = d$ 两边同时乘以 $c/d$ ，得： $ax_0c/d + by_0c/d = c$ 。

(4) 对照 $ax + by = c$ ，得到它的一个解 $(x'_0, y'_0)$ 为： $x'_0 = x_0c/d, y'_0 = y_0c/d$ 。

(5) 方程 $ax + by = c$ 的通解:  $x = x'_0 + (b/d)n$ ,  $y = y'_0 - (a/d)n$ 。

已知通解为 $x = x_0 + (b/d)n$ 要使 $x$ 最小, 则需要 $x_0$ 不断的减 $b/d$ 。那么此过程相当于取模, 可以简单化为

$((x_0 \% (b/d) + b/d) \% (b/d))$ , 多加一次再去模防止负数。

[P1516 青蛙的约会 - 洛谷 | 计算机科学教育新生态](#)

```
1  #include <iostream>
2
3  using namespace std;
4  long long exgcd(long long a, long long b, long long &x, long long &y)
5  {
6      if(b == 0)
7      {
8          x = 1;
9          y = 0;
10         return a;
11     }
12     long long d = exgcd(b, a%b, y, x);
13     y -= a/b*x;
14     return d;
15 }
16 int main () {
17     long long x, y, m, n, l;
18     cin >> x >> y >> m >> n>>1;
19     long long c = x - y;
20     long long a = n - m;
21     if (a < 0) {
22         a = -a;
23         c = -c;
24     }
25     long long d = exgcd(a, 1, x, y);
26     if (c % d != 0) //判断方程有无整数解
27         cout << "Impossible";
28     else
29         cout << ((x*c/d) % (1 / d) + (1 / d)) % (1 / d);
30 }
```

## 同余

设 $m$ 是正整数, 若 $a$ 和 $b$ 是整数, 且 $m|(a - b)$ , 则称 $a$ 和 $b$ 模 $m$ 同余。即 $a$ 除以 $m$ 得到的余数和 $b$ 除以 $m$ 的余数相同, 或者说 $a - b$ 除以 $m$ , 余数为0。

把 $a$ 和 $b$ 模 $m$ 同余记为 $a \equiv b \pmod{m}$ ,  $m$ 称为同余的模。

## 一元线性同余方程

设 $x$ 是未知数, 给定 $a$ 、 $b$ 、 $m$ , 求整数 $x$ , 满足 $ax \equiv b \pmod{m}$ 。

$ax \equiv b \pmod{m}$ 表示 $ax - b$ 是 $m$ 的倍数, 设为 $-y$ 倍, 则有 $ax + my = b$ , 这就是二元线性丢番图方程。所以求解一元线性同余方程等价于求解二元线性丢番图方程。

**定理:** 设 $a$ 、 $b$ 和 $m$ 是整数,  $m > 0$ ,  $\gcd(a, m) = d$ 。若 $d$ 不能整除 $b$ , 则 $ax \equiv b \pmod{m}$ 无解; 若 $d$ 能整除 $b$ , 则 $ax \equiv b \pmod{m}$ 有 $d$ 个模 $m$ 不同余的解。

此定理可以参考前面的线性丢番图方程来理解, 如果有一个特解是 $x_0$ , 那么通解是 $x = x_0 + (m/d)n$ , 当 $n = 0, 1, 2, \dots, d - 1$ 时, 有 $d$ 个模 $m$ 不同余的解。

**推论:**  $a$ 和 $m$ 互素时, 因为 $d = \gcd(a, m) = 1$ , 所以线性同余方程 $ax \equiv b \pmod{m}$ 有唯一的模 $m$ 不同余的解。

## 逆

给定整数 $a$ , 且满足 $\gcd(a, m) = 1$ , 称 $ax \equiv 1 \pmod{m}$ 的一个解为 $a$ 模 $m$ 的逆。记为 $a^{-1}$ 。

例如:  $8x \equiv 1 \pmod{31}$ , 有一个解是 $x = 4$ , 4是8模31的逆。所有的解, 例如35、66等, 都是8模31的逆。

所以从逆的要求来看,  $\gcd(a, m) = 1$ 可以看出, 模 $m$ 最好是一个大于 $a$ 的素数, 才能保证 $\gcd(a, m) = 1$ 。

## 求逆

### 1) 扩展欧几里得求逆

$ax \equiv 1 \pmod{m}$ , 即丢番图方程  $ax + my = 1$ , 先用扩展欧几里得求  $ax + my = 1$  的一个特解  $x_0$ , 通解  $x = x_0 + mn$ 。然后通过取模计算最小整数解  $((x_0 \bmod m) + m) \bmod m$ 。

```
1  #include <iostream>
2  using namespace std;
3  long long exgcd(long long a, long long b, long long &x, long long &y)
4  {
5      if(b == 0)
6      {
7          x = 1;
8          y = 0;
9          return a;
10     }
11     long long d = exgcd(b, a%b, y, x);
12     y -= a/b*x;
13     return d;
14 }
15 int main ()
16 {
17     long long a, b;
18     long long y, x;
19     cin >> a >> b;
20     long long d = exgcd(a, b, x, y);
21
22     cout << (x % b + b) % b;
23 }
```

### 2) 费马小定理求逆

设  $n$  是素数,  $a$  是正整数且与  $n$  互素, 有  $a^{n-1} \equiv 1 \pmod{n}$ 。

$a * a^{n-2} \equiv 1 \pmod{n}$ , 那么  $a^{n-2} \bmod n$ , 就是  $a$  模  $n$  的逆。

计算时候采用快速幂取模。

```
1  long long mod_inverse(long long a, long long mod)
2  {
3      return fast_pow(a, mod - 2, mod);
4  }
```

## 逆与除法取模

求  $(a/b) \bmod m$ , 即使  $a$  除以  $b$ , 然后对  $m$  取模。这里  $a$ 、 $b$  都是很大的数, 会溢出导致取模出错。用逆可以避免除法计算。

设  $b$  的逆元是  $b^{-1}$ , 有  $(a/b) \bmod m = ((a/b) \bmod m)((bb^{-1}) \bmod m) = (a/b * bb^{-1}) \bmod m = (ab^{-1}) \bmod m$

除法的模运算转换为乘法模运算, 即

$$(a/b) \bmod m = (ab^{-1}) \bmod m = (a \bmod m)(b^{-1} \bmod m) \bmod m$$

2024 ICPC 湖北省赛 [Problem - J - Codeforces](#)

```
1  #include <bits/stdc++.h>
2
3  using namespace std;
4  long long m = 998244353;
5  long long fastpow(long long a, long long b, long long mod)
6  {
7      long long ans = 1;
8      a = a % mod;
9      while(b)
10     {
11         if(b & 1)
```



```

12         ans = ans * a % mod;
13         a = a * a % mod;
14         b = b >> 1;
15     }
16     return ans;
17 }
18 long long a[1000003];
19 int main ()
20 {
21     int n;
22     long long sum = 0;
23     int i;
24     cin>>n;
25     for(i = 0;i < n;i++)
26     {
27         cin>>a[i];
28         sum +=a[i];
29         sum = sum%m;
30     }
31     cout<<sum*fastpow(n,m - 2,m)%m;
32     return 0;
33 }

```

## 素数

定义：只能被1和自己整除的正整数。

## 素数判定

### 1) 试除法

时间复杂度 $O(\sqrt{n})$ ,  $n \leq 10^{12}$ 。

```

1 bool is_prime(long long n)
2 {
3     if(n <= 1)
4         return false;
5     for(long long i = 2;i<= sqrt(n);i++)//i*i<=n
6     {
7         if(n % i ==0)
8             return false;
9     }
10    return true;
11 }

```

### 2)Miller-Rabin素性测试

```

1 #include <bits/stdc++.h>
2
3 using namespace std;
4 long long fast_pow(long long x,long long y,int m)
5 {
6     long long res = 1;
7     x = x % m;
8     while(y)
9     {
10         if(y&1)
11             res = (res * x) % m;
12         x = (x * x) % m;
13         y >>= 1;
14     }
15     return res;

```

```

16 }
17 bool witness(long long a,long long b)//素性测试，返回true表示n是合数
18 {
19     long long u = n - 1;//u是n-1的二进制去掉末尾0
20     int t = 0;//n-1的二进制，是奇数u的二进制后面加t个0
21     while(u&1 == 0)//整数n-1末尾0的个数就是t
22     {
23         u = u>>1;
24         t++;
25     }
26     long long x1,x2;
27     x1 = fast_pow(a,u,n);
28     for(int i = 1;i <= t;i++) //平方取模
29     {
30         x2 = fast_pow(x1,2,n);
31         if(x2 == 1&&x1 != 1&&x1 != n-1)
32         {
33             return true;
34         }
35         x1 = x2;
36     }
37     if(x1 != -1)
38         return true;//用费马测试判断是否为合数
39     return false;
40 }
41 int miller_rabin(long long n,int s)
42 {
43     if(n < 2)
44         return 0;
45     if(n == 2)
46         return 1;
47     if(n%2==0)
48         return 0;
49     for(int i = 0;i < s &&i < n;i++)//s次测试
50     {
51         long long a = rand()%(n-1) + 1; //a为随机数
52         if(witness(a,n))
53             return 0;
54     }
55     return 1;
56 }
57 int main()
58 {
59     int m;
60     cin>>m;
61     int cnt = 0;
62     for(int i = 0;i < m;i++)
63     {
64         long long n;
65         cin>>n;
66         int s = 50//50次测试
67         cnt += miller_rabin(n,s);
68     }
69     cout<<cnt;
70 }

```

## 素数筛

给定 $n$ ，求 $2$ 到 $n$ 内所有的素数。逐个判断时间复杂度非常高，我们可以筛法一起筛出所有整数，把非素数筛掉。

### 埃式筛

时间复杂度 $O(n\log_2\log_2^n)$

对于初始队列 $\{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \dots, n\}$ 。

(1)输出最小素数 $2$ ，然后筛掉 $2$ 的倍数，得 $\{3, 5, 7, 9, 11, 13, \dots\}$ 。

(2) 筛出最小素数3，然后筛掉3的倍数，得{5, 7, 11, 13, ...}。

(3) 输出最小素数5，然后筛掉5的倍数，得{7, 11, 13, ...}。

```
1  const int N=1e7;
2  int prime[N+1]; //储存素数
3  bool visit[N+1]; //true表示被筛掉，不是素数
4  int E_sieve(int n)
5  {
6      for(int i = 0; i <= n; i++)
7      {
8          visit[i] = false; //初始化为false
9      }
10     for(int i = 2; i * i <= n; i++) //遍历用来做筛除的数2、3、5
11     {
12         if(!visit[i])
13         {
14             for(int j = i*i; j <= n; j+=i)
15             {
16                 visit[j] = true; //标记为非素数
17             }
18         }
19     }
20     int k = 0; //记录素数个数
21     //上面筛完了，下面开始记录素数
22     for(int i = 2; i <= n; i++)
23     {
24         if(!visit[i])
25             prime[k++] = i; //把筛出来的素数存入数组中
26     }
27     return k;
28 }
```

埃式筛中做了一些无用功，某个数会被筛到好几次，比如12就被2和3筛了两次，所以我们可以使用更快的欧式筛来改进。

## 欧式筛

时间复杂度为 $O(n)$ 。

一个合数肯定有一个最小质因数；让每个合数只被它的最小质因数筛选一次，达到不重复的目的。

[P3383 【模板】线性筛素数 - 洛谷](#) | [计算机科学教育新生态](#)

```
1  int prime[N+1]; //保存素数
2  bool vis[N+1]; //记录是否被筛
3  int euler_sieve(int n)
4  {
5      int cnt = 0;
6      memset(vis, 0, sizeof(vis));
7      memset(prime, 0, sizeof(prime));
8      for(int i = 2; i <= n; i++) //检查每个数，筛去合数
9      {
10         if(!vis[i])
11             prime[cnt++] = i; //如果没有被筛过，是素数，记录下来。
12         for(int j = 0; j < cnt; j++) //用已经得到的素数去筛后面的数。
13         {
14             if(i * prime[j] > n) //只筛小于或等于n的数，大于直接退出
15                 break;
16             vis[i * prime[j]] = 1; //用最小质因数筛去x
17             if(i % prime[j] == 0) //如果i能整除它，表明i肯定不是x的最小质因数，
18                 break;
19         }
20     }
21     return cnt;
22 }
```

代码`vis[i*prime[j]] = 1`中，表示用最小的质因数筛去了它的倍数，其中`prime[j]`是最小质因数。

后面一行中发现能整除这个最小质因数，那么可以说明的最小是 $prime[j]$ ，那么后面的 $prime[j+1]$ 肯定不是最小质因数，于是可以退出循环了。比如当 $i = 4$ 时候，我们首先看 $prime[j] = 2$ ，筛去8，然后发现 $i$ ，那么 $prime[j+1] = 3$ 就不会执行，因为 $3 * 4 = 12$ ，而12的最小质因数是2，如果真的执行了，那么当 $i = 6$ 的时候， $prime[i] = 2$ ，就会又执行一次，重复计算了。

## 质因数分解

前面我们讲LCM的时候提到了算术基本定理，即任何大于1的正整数 $n$ 可以唯一分解为有限个素数的乘积： $n = p_1^{c_1} p_2^{c_2} \dots p_m^{c_m}$ ，其中 $c_i$ 都为正整数， $p_i$ 都为素数且从小到大。我们可以通过这个定理来分解质因数。

### 欧拉筛求最小质因数

我们知道欧拉筛是每次用最小质因数来操作，所以我们直接记录每次的最小质因数就可以了。

可以用来求 $1 \sim n$ 的每个数的最小质因数。

```
1  int prime[N+1]; //保存素数
2  int vis[N+1]; //记录最小质因数
3  int euler_sieve(int n)
4  {
5      int cnt = 0;
6      memset(vis, 0, sizeof(vis));
7      memset(prime, 0, sizeof(prime));
8      for(int i = 2; i <= n; i++) //检查每个数，筛去合数
9      {
10         if(!vis[i])
11         {
12             prime[cnt++] = i; //如果没有被筛过，是素数，记录下来。
13             vis[i] = i; //记录最小质因数
14         }
15         for(int j = 0; j < cnt; j++) //用已经得到的素数去筛后面的数。
16         {
17             if(i * prime[j] > n) //只筛小于或等于n的数，大于直接退出
18                 break;
19             vis[i * prime[j]] = prime[j]; //记录最小质因数
20             if(i % prime[j] == 0) //如果i能整除它，表明i肯定不是x的最小质因数，
21                 break;
22         }
23     }
24     return cnt;
25 }
```

### 试除法分解质因数

上面的欧拉筛是求最小质因数，分解质因数也可以采用试除法来求解。时间复杂度 $O(\sqrt{n})$

(1) 首先检查 $2 \sim \sqrt{n}$ 的所有素数，如果他能整除 $n$ ，就是最小质因数。然后连续的用 $p_1$ 去除 $n$ 。目的是为了去掉 $n$ 中的 $p_1$ ，从而得到 $n_1$

(2) 然后对于 $n_1$ ，可以从 $p_1 \sim \sqrt{n}$ 来检查所有素数，和步骤1一样。因为我们找到了最小质因数 $p_1$ ，所以 $p_1$ 前面的数就没有必要检查了。

最后做完之后，如果剩下一个大于1的数，那么它也是一个素数，是 $n$ 的最大质因数。

```
1  int p[20]; //记录因数，p[1]为最小因数
2  int c[40]; //记录第i个因数的个数，
3  int factor(int n)
4  {
5      int m = 0;
6      for(int i = 2; i <= sqrt(n); i++)
7      {
8          if(n % i == 0)
9          {
10             p[++m] = i; //记录最小因数
11             c[m] = 0; //初始化有0个此因数
12             while(n % i == 0) //把n中重复的去掉
13             {
14                 n = n / i;
```

```
15         c[m]++; //去一次个数加1
16     }
17 }
18 }
19 if(n > 1)
20 {
21     p[++m] = n;
22     c[m] = 1;
23 }
24 return m;
25 }
```

## Chapter 8 动态规划

---

### 8.1 dp基础

---

- dp问题具有最优子结构与重叠子问题
- 自上而下叫记忆化搜索，自下而上叫dp

### 8.2 线性dp

---

- [300. 最长递增子序列 - 力扣 \(LeetCode\)](#)
- [1143. 最长公共子序列 - 力扣 \(LeetCode\)](#)

### 8.3 背包dp

---

#### 8.3.1 01背包

- 模板题，网上随便找一道
- [416. 分割等和子集 - 力扣 \(LeetCode\)](#)

#### 8.3.2 完全背包

- 模板题，反转01背包容量遍历顺序即可重复

### 8.4 区间dp

---

- [P1880 [NOI1995](#)] [石子合并 - 洛谷](#) | [计算机科学教育新生态](#)