算法竞赛小学期培训

初等数论

张晓昊

Sheauhaw Jang

少年班 73　数试 92

2020 年 7 月 21 日　火曜日

张晓昊 Sheauhaw Jang

~~少年班 73~~ 留级两年 数试 92

QQ: 1368287280

鸣谢: 计试 71 朱泽荧

本节要点:

本节的前置知识只有小学数学知识. 大家请放心!

本节理论知识较多, 定义和符号很重要, 结论的重要程度顺序为定理、命题、性质, 请大家注意.

受时间限制, 本节课的部分结论的证明可能没有或比较粗糙, 敬请各位数学大佬见谅. 感兴趣的同学可以课下自行补全证明.

2020年ICPC小学期期末考试报名

考 试 须 知

1. 报名成功的同学方可报名参加参加期末考试, 可以报名参加任意一期期末考试, 不受选课报名表的限制.

2. 报名当期期末考试后, 方有资格参加当期期末考试. 否则不能参加当期期末考试.

3. 报名当期期末考试后, 当期成绩有效. 不报名当期期末考试, 当期考勤成绩、作业成绩均作废, 当期不参与校队选拔和成绩代替.

4. 每名同学至多只能报名和参加一次期末考试, **考试信息不能修改, 请慎重考虑!**

5. 期末考试使用 XJTUOJ, 并且只能在指定考场参加期末考试, 届时 XJTUOJ 的外网的访问将会关闭.

6. 报名期末考试后, 期末考试可以不参加, 期末考试成绩记 0 分, 考勤成绩和作业成绩均有效. 期末考试分值较高, 建议慎重考虑.

7. 期末考试前, 请各位同学将 XJTUOJ 的 ID 修改成合法的 ID, 格式为 班级-姓名 (包括横杠). 班级名称为正规名称, 例如 少年班73 计试91 金禾91 等是合法班级名称, 少82 数试-91 计算机试验班91 气功71 等不属于正规班级名称, 可能不会被正确统计成绩. 若有多个常用的名称, 可以任选其一. 本报名表的班级填写正规名称, 并与XJTUOJ上的ID中的班级一致. 违反本条规定者, 可能不会被正确统计成绩.

8. 第一期期末考试时间为 2020年7月12日 星期日 13:00-18:00. 第二期期末考试时间为 **2020年7月26日 星期日 13:00-18:00.**

9. 期末考试可以携带不限量的纸质资料, 不允许携带任何电子设备.

10. 凭校园卡参加考试, 对号入座. 任何形式作弊一经发现取消考试资格, 所有成绩清零.

11. 期末考试不允许迟到, **可以提前交卷**, 提前交卷后不得返回考场.

12. 考试地点**西一楼A103.** 期末考试前一天（星期六）下午 14:00-20:00 开放试机, 可以测试编译环境和网络环境.

13. 期末考试有 5 道基础题和 6 道提高题. 细则见群 526350936 中的群文件及考试公告.

14. 每场期末考试的第一名（按ICPC赛制排名）直接获得入队资格, 成绩记满分.

15. ICPC小学期一切事项的最终解释权归西安交通大学ICPC校队所有.

定义 1 (整除)

对于 $a,b \in \mathbb{Z}, b \neq 0$, 若 $\exists c \in \mathbb{Z}$ 使得 $a = bc$ 成立, 则称 b 整除 a, 记做 $b \mid a$, 此时 b 叫做 a 的因数, a 叫做 b 的倍数.

命题 1 (偏序关系)

$\forall a, b, c \in \mathbb{Z}$

1. 反身性: $a \mid \pm a$.
2. 反对称性: 若 $a \mid b, b \mid a$, 则 $a = \pm b$.
3. 传递性: 若 $a \mid b, b \mid c$, 则 $a \mid c$.
4. 线性性: 若 $a \mid b, a \mid c$, 则 $\forall x, y \in \mathbb{Z}, a \mid xb + yc$.

例 1

求 n 的所有因数. $n \leq 10^{12}$.

暴力方法: $i \in \mathbb{Z}[1 \to n]$, 检验是否有 $i \mid n$. 时间复杂度为 $O(n)$.

由整除定义: $\forall i \mid n$, 有 $n/i \mid n$.

优化方法: $i \in \mathbb{Z}[1 \to \sqrt{n}]$, 若 $i \mid n$, 则 i 和 n/i 都是 n 的因数. 时间复杂度为 $O(\sqrt{n})$.

代码 1 (查找因数)

```
vector<ll> fcts;
void fndf(ll x) {
    for (ll i = 1; i * i <= x; ++i)
        if (x % i == 0) {
            fcts.push_back(i);
            if (i != x / i)
                fcts.push_back(x / i);
        }
}
```

定义 2 (素数合数)

对于 $a \in \mathbb{Z}, a \neq \pm 1$, 若 a 的正因数只有 1 和 $|a|$, 那么称 a 是素数 (质数), 否则称 a 是合数.

例 2

判断给定的 n 是否为素数. 将 n 表示为若干素数的乘积. $1 < n \leq 10^{12}$.

问题 1

判断给定的 n 是否为素数. 将 n 表示为若干素数的乘积. $1 < n \leq 10^{18}$.

自行阅读 Miller-Rabin 算法和 Pollard-Rho 算法. 考试不作要求.

例 3

给定一个 $n \in \mathbb{N}_+$, 求区间 $[1, n]$ 的所有素数. $n \leq 10^7$.

定理 1 (算术基本定理)

$\forall n \in \mathbb{Z} \cap [2, +\infty)$, n 都可以唯一地表示为:

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s}$$

其中: $p_1, p_2, ..., p_s$ 是两两不同的素数, $\alpha_1, \alpha_2, ..., \alpha_s \in \mathbb{N}_+$.

上式称为 n 的标准分解式.

定理 2

$\forall n \in \mathbb{N}_+$, 有:

$$n! = \prod_p p^{\alpha(p,n)}$$

$$\alpha(p, n) = \sum_i \left\lfloor \frac{n}{p^i} \right\rfloor$$

例 2: 本质是求 n 的标准分解式.

枚举找出 n 最小的素因子 $p(n)$, 然后将 $n/p(n)$ 作为新的 n 重复操作.

设 $n>1$, n 是合数 $\iff p_0 \neq n \iff p_0 \leq \sqrt{n}$. 若 $p_0 > \sqrt{n}$, 则 n 是素数, $p_0 = n$. 故只需要枚举到 $\sqrt{n}$.

思考: 为什么新的枚举不从 2 开始? 为什么不判断 i 是否为质数?

代码 2 (素因数分解)

```
vector<ll> pfcts;
void fndpf(ll x)
{
    for (ll i = 2; i * i <= x; ++i)
        if (x % i == 0)
            fcts.push_back(i), x /= i, --i;
    if (x != 1) pfcts.push_back(x);
}
```

例 3:

埃氏筛:

维护一个 $[2 \to n]$ 的标记数组, 初始全部标记为素数. $i \in \mathbb{Z}[2 \to \sqrt{n}]$, 如果 i 是素数, 将 i 的倍数全部标记为合数.

埃氏筛的时间复杂度为 $O(n \log \log n)$.

线性筛: (难点)

埃氏筛中有的合数被标记多次, 我们希望 $\forall k \in \mathbb{Z}[2, n]$ 只被标记一次: 规定 k 被 k 的最小的质因子 $p(k)$ 标记. 记 $i(k) := k/p(k)$. 先枚举 i, 再枚举可能的 $p(k)$, $k = i(k)p(k)$ 就被 $p(k)$ 标记. 容易证明 $p(k)$ 的限制是 $p(k) \leq p(i)$.

线性筛的时间复杂度为 $O(n)$.

代码 3 (线性筛)

```
vector<int> ps; // 所有素数
bool chk[maxn]; // 合数为 true
void fillPrime(int rge)
{
    for (int i = 2; i <= rge; i++)
    {
        if (!chk[i])
            ps.push_back(i);
        for (int j = 0; j < ps.size() &&
                        ps[j] <= rge / i; j++)
        {
            chk[i * ps[j]] = true;
            if (i % ps[j] == 0) break;
        }
    }
}
```

性质 1

设 $n \in \mathbb{Z}, n > 1$ 的标准分解式为 $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_s}^{\alpha_s}$, 则

n 的因子个数

$$d(n) = \sum_{d|n} 1 = \prod_{i=1}^{s}(\alpha_i + 1)$$

n 的所有因子之和

$$\sigma(n) = \sum_{d|n} d = \prod_{i=1}^{s} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

感兴趣的同学自行阅读:

数论函数, Möbius 变换, Möbius 反转, Dirichlet 卷积.

考试不作要求.

定义 3 (最大公因数)

对于 $a_1, a_2, \ldots, a_n, d \in \mathbb{Z}$, 若 $\forall i \in \mathbb{Z}[1, n]$, $d \mid a_i$, 则称 d 是 $a_1, a_2, \ldots, a_n$ 的公因数. $a_1, a_2, \ldots, a_n$ 的公因数中的最大者称为 $a_1, a_2, \ldots, a_n$ 的最大公因数, 记做 $\gcd(a_1, a_2, \ldots, a_n)$, 或记做 $(a_1, a_2, \ldots, a_n)$. 若 $\gcd(a_1, a_2, \ldots, a_n) = 1$, 则称 $a_1, a_2, \ldots, a_n$ 互素.

命题 2

1. $\forall a \in \mathbb{N}_+$, $\gcd(a, 0) = a$.
2. $\forall a, b \in \mathbb{N}_+$, 若 $a \mid b$, 则 $\gcd(a, b) = a$.
3. $\forall a, b, k \in \mathbb{Z}$, $\gcd(a, b) = \gcd(a \pm kb, b)$.

例 4

$a, b \in \mathbb{N}$, 求 $\gcd(a, b)$. $0 < a, b \leq 10^{18}$.

不妨设 $a \geq b$.

暴力方法：$i \in \mathbb{Z}[b \to 1]$, 检验是否有 $i \mid a, i \mid b$. 时间复杂度 $O(b)$.

辗转相除法：

$$\gcd(a, b) = \gcd\left(b, a - \left\lfloor \frac{a}{b} \right\rfloor b\right) = \gcd(b, a\%b)$$

将 $b, a\%b$ 作为新的 a, b 重复以上步骤，直到 $b = 0$ 时得到 $\gcd(a, 0) = a$.

辗转相除法时间复杂度为 $O(\log b)$.

代码 4 (辗转相除法)

```
ll gcd(ll a, ll b)
{
    return b ? gcd(b, a % b) : a;
}
```

命题 3

$\forall a, b \in \mathbb{Z}; a, b \neq 0$:

1. $\forall m \in \mathbb{N}_+$, $\gcd(am, bm) = \gcd(a, b)m$.
2. $\forall$ a, b 的公因数 d, $\gcd(a/d, b/d) = \gcd(a, b)/d$.

   特别地:

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$$

命题 4

$\forall a, b, c \in \mathbb{Z}$, 都有

$$\gcd(a, c)\gcd(b, c) \geq \gcd(ab, c) \geq \gcd(a, c)$$

思考 $\gcd(a, c) = \gcd(b, c) = 1$ 的特殊情况.

定义 4 (最小公倍数)

对于 $a_1, a_2, \dots, a_n, d \in \mathbb{Z}$, 若 $\forall i \in \mathbb{Z}[1, n]$, $a_i \mid d$, 则称 d 是 $a_1, a_2, \dots, a_n$ 的公倍数. $a_1, a_2, \dots, a_n$ 的公倍数中的最小者称为 $a_1, a_2, \dots, a_n$ 的最小公倍数, 记做 $\operatorname{lcm}(a_1, a_2, \dots, a_n)$, 或记做 $[a_1, a_2, \dots, a_n]$.

定理 3

$$\forall a, b \in \mathbb{N}_+, \gcd(a, b)\operatorname{lcm}(a, b) = ab$$

命题 5

$\forall a, b \in \mathbb{Z}; a, b \neq 0$:

1. $\forall m \in \mathbb{N}_+, \operatorname{lcm}(am, bm) = \operatorname{lcm}(a, b)m$.
2. $\forall$ a, b 的公倍数 D, $\operatorname{lcm}(D/a, D/b) = D/\gcd(a, b)$.
3. $\forall$ a, b 的公倍数 D, $\gcd(D/a, D/b) = D/\operatorname{lcm}(a, b)$.

代码 5 (最小公倍数)

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

命题 6

$\forall a_1, a_2, a_3, ..., a_n \in \mathbb{N}_+$, 有:

$$\gcd(a_1, a_2, a_3, ..., a_n) = \gcd(\gcd(a_1, a_2), a_3, ..., a_n)$$

$$\operatorname{lcm}(a_1, a_2, a_3, ..., a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, a_2), a_3, ..., a_n)$$

例题: XJTUOJ 1124.

练习 1

给定 $x, y \in \mathbb{N}_+$, $x, y \le 10^{12}$. 求满足下列条件的 $a, b \in \mathbb{N}_+$ 的数量:

$$\gcd(a, b) = x, \operatorname{lcm}(a, b) = y$$

记 $a_0 := a/x, b_0 := b/x$. 于是

$$\gcd(a_0, b_0) = 1$$
$$\operatorname{lcm}(a_0, b_0) = \frac{y}{x}$$

枚举 a_0, b_0 即可.

总时间复杂度为 $O(\sqrt{y}\log y)$.

练习 2

给定一个 $x \in \mathbb{N}_+$. 求 $a, b \in \mathbb{N}^+$, s.t. $\operatorname{lcm}(a,b) = x$, $\max(a,b)$ 最小. $x \le 10^{12}$.

设 $a, b \in \mathbb{N}_+; \operatorname{lcm}(a,b) = x$, 有标准分解式.

$$a = \prod_{i=1}^{s} {p_i}^{\alpha_i}, b = \prod_{i=1}^{s} {p_i}^{\beta_i}$$

取:

$$a' = \prod_{\alpha_i > \beta_i} {p_i}^{\alpha_i}, b' = \prod_{\alpha_i \le \beta_i} {p_i}^{\beta_i}$$

有: $a' \le a, b' \le b$, $\gcd(a', b') = 1$, $a'b' = \operatorname{lcm}(a', b') = \operatorname{lcm}(a, b) = x$.

这说明任给一种结果 a, b, 总能找到等效或者更优的 $\gcd(a,b) = 1$ 的结果. 于是我们忽略掉 $\gcd(a,b) > 1$ 的情况, 把 $\operatorname{lcm}(a,b) = x$ 转化成了 $\gcd(a,b) = 1, ab = x$, 时间复杂度 $O(\sqrt{x} \log x)$.

定义 5 (同余)

$\forall m, a, b \in \mathbb{Z}; m \neq 0$. 若 $m \mid a-b$, 则称 a 和 b 模 m 同余, 记作

$$a \equiv b \pmod{m}$$

命题 7 (等价关系)

$\forall a, b, c, m \in \mathbb{Z}; m \neq 0$

1. 自反性: $a \equiv a \pmod{m}$.
2. 对称性: $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$.
3. 传递性: 若 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 则 $a \equiv c \pmod{m}$.

% 运算的再认识: $a \equiv a\%b \pmod{b}$. $a\%b$ 是满足 $a \equiv x \pmod{m}$ 的绝对值最小的非负 (非正) 整数 x. 推论: $a \geq 0$ 时有 $0 \leq a\%b < b$.

命题 8

$\forall a,b,c,d,m \in \mathbb{Z}, m \neq 0$, 若 $a \equiv c \pmod m, b \equiv d \pmod m$, 则:

1. $a \pm b \equiv c \pm d \pmod m$.
2. $a \cdot b \equiv c \cdot d \pmod m$.

思考: 复杂的表达式中, 哪些% 运算可以省略?

命题 9

$\forall a,b,k,m \in \mathbb{Z}; m \neq 0$, 若 $ak \equiv bk \pmod m$, 则

$$a \equiv b \pmod{\frac{m}{\gcd(k,m)}}$$

命题 9 表明, 同余式两端不能直接做除法.

若 $a \equiv b \pmod m$, 则 $k^a \equiv k^b \pmod m$ 不一定成立. 试举出反例.

练习 3

给定 $a_1, a_2, ..., a_n, k \in \mathbb{N}_+$, 求 $i, j \in \mathbb{Z}$ 满足 $1 \le i < j \le n$ 且 $\exists x \in \mathbb{Z}$, s.t. $a_i \cdot a_j = x^k$ 的数量. $1 < n \le 10^5, 1 < k \le 100, a_i \le 10^5 (i \in \mathbb{Z}[1, n])$.

考虑 a, b 的标准分解式:

$$a = \prod_{p_i=1}^{s} {p_i}^{\alpha_i}, b = \prod_{p_i=1}^{s} {p_i}^{\beta_i}$$

那么 $a \cdot b = x^k$ 的充分必要条件是 $\forall i \in [1, s] \cap \mathbb{Z}$, $k \mid \alpha_i + \beta_i$, 即 $\alpha_i + \beta_i \equiv 0 \pmod k$. 那么我们只关心 $\alpha \mod k$, 将各项指数对 k 取模后全部相等的 a 归为一类, 这样能与 a 配对的类型是确定的一个.

用 `std::map<int,int>` 表示一类数字, 并用 `std::map` 统计每一类的数量, 然后进行统计.

总时间复杂度为 $O(n \log n)$.

练习 4

给定正整数 n 和 k，计算 $\sum_{i=1}^{n} k\%i$ 的值，$1 \le n, k \le 10^9$.

模数不同，用乘法和加法表示.

$$\sum_{i=1}^{n} k\%i = \sum_{i=1}^{n} \left(k - \left\lfloor \frac{k}{i} \right\rfloor i\right) = nk - \sum_{i=1}^{n} \left\lfloor \frac{k}{i} \right\rfloor i$$

发现 $f(i) = \lfloor k/i \rfloor$ 是单调减的，且 $f(\lfloor k/\lfloor k/x \rfloor \rfloor) = f(x)$，$f$ 在区间 $[x, \lfloor k/\lfloor k/x \rfloor \rfloor]$ 上是常值函数，可以进行等差数列的求和.

f 至多有 $2\sqrt{k}$ 个取值，总时间复杂度为 $O(\sqrt{k})$.

同余方程 $ax \equiv c \pmod{b}$ 和不定方程 $ax + by = c$ 等价.

命题 10 (通解)

若 a, b 不全为 0, 且 $ax + by = c$ 有特解 x_0, y_0, 则其一切解可以表示为

$$x = x_0 + t\frac{b}{\gcd(a,b)} \qquad y = y_0 - t\frac{a}{\gcd(a,b)}$$

其中 $t \in \mathbb{Z}$.

定理 4 (Bézout)

若 a, b 不全为 0, 则 $ax + by = c$ 有解当且仅当 $\gcd(a,b) \mid c$.

推论 1

$\forall a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$ 当且仅当 $ax + by = 1$ 有解.

例 5

求解不定方程 $ax + by = c$. $0 < a, b, c \le 10^9$.

求解 $ax + by = c$ 可转化为求解 $ax_0 + by_0 = \gcd(a, b)$,

$$x = x_0 \cdot \frac{c}{\gcd(a, b)} \qquad y = y_0 \cdot \frac{c}{\gcd(a, b)}$$

如何求解 x_0, y_0? 扩展欧几里得算法:

若 $b = 0$, 则 $x_0 = 1, y_0 = 0$ 是一组解.

否则 $\gcd(a, b) = \gcd(b, a\%b)$, 设 $bx_1 + (a\%b)y_1 = \gcd(b, a\%b)$, 则:

$$bx_1 + (a\%b)y_1 = bx_1 + \left(a - \left\lfloor \frac{a}{b} \right\rfloor b\right) y_1 = ay_1 + b\left(x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1\right)$$

$$x_0 = y_1 \qquad y_0 = x_1 - \left\lfloor \frac{a}{b} \right\rfloor y_1$$

求解 x_1, y_1 只需要将 $b, a\%b$ 作为新的 a, b 重复以上步骤即可.

在进行扩展欧几里得算法的同时, 我们可以得到返回值 $\gcd(a, b)$.

扩展欧几里得算法的时间复杂度为 $O(\log b)$.

代码 6 (扩展欧几里得)

```
ll exgcd(ll a, ll b, ll &x, ll &y)
{
    if (!b) { x = 1; y = 0; return a; }
    ll d = exgcd(b, a % b, y, x);
    y = y - a / b * x;
    return d;
}
```

性质 2

扩展欧几里得算法求得的 x_0, y_0 满足 $|x_0| \le |b|, |y_0| \le |a|$.

证明提示: 使用数学归纳法.

练习 5

判断 $ax+by+cz = n$ 有无非负整数解? $0 \le a, b, c < 2 \cdot 10^5, 1 \le n \le 10^{18}$.

若有解, 一定有 $|x| \le b$ 的解. 枚举 x 解 y, z 即可.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \cdots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{1}$$

一次同余方程组 (1) 的一个解应表示为 $x \equiv C \pmod{m}$,
其中 $m := \operatorname{lcm}(m_1, m_2, \cdots, m_n)$.

定理 5 (中国剩余定理)

方程组 (1) 中, 若 $m_1, m_2, \cdots, m_n$ 两两互素, 则方程组有且仅有一个解:

$$x \equiv \sum_{j=1}^{n} M_j M_j' a_j \pmod{m}$$

其中 $M_j = m/m_j, M_j M_j' \equiv 1 \pmod{m_j}$ $(1 \le j \le n)$

M_j' 的存在性: $\gcd(M_j, m_j) = 1$. 总时间复杂度 $O(\log m)$.

方程组 (1) 中, 若 $m_1, m_2, \cdots, m_n$ 并非两两互素, 则方程组不一定有解.

记前 k 个方程组成的方程组为 $(1)_k$. 通过 $(1)_k$ 的解求 $(1)_{k+1}$.

基础: $x \equiv a_1 \pmod{m_1}$ 的解为其本身.

归纳: 记 $M_k = \operatorname{lcm}(m_1, m_2, \cdots, m_k)$, 设方程组 $(1)_k$ 有解 $x \equiv A \pmod{M_k}$. 则有通解 $x = A + tM_k$, $t \in \mathbb{Z}$. 解关于 t 的同余方程

$$A + tM_k \equiv a_{k+1} \pmod{m_{k+1}} \tag{2}$$

可以使用扩展欧几里得算法. 如果 t 有解, 那么 $x \equiv A+tM_k \pmod{M_{k+1}}$ 就是前 $k+1$ 个方程的一个解.

思考: $(1)_k$ 的一个解能通过 (2) 式求出多少 $(1)_{k+1}$ 的解? 是唯一解吗?

于是如果 (2) 式中 t 无解, 则方程组无解.

总时间复杂度 $O\left(\log \prod m_i\right)$.

定义 6 (Euler 函数)

Euler 函数 $\varphi(n)$ 是定义在 $\mathbb{N}_+$ 上的函数, 在正整数 n 处的值为 $1, 2, \cdots, n$ 中与 n 互素的数的个数.

引理 1

φ 是积性函数. 即 $\forall m, n \in \mathbb{N}_+ : \gcd(m, n) = 1$, 有 $\varphi(mn) = \varphi(m)\varphi(n)$.

提示: 使用中国剩余定理.[3]

定理 6

设 $n > 1$ 的标准分解式为 $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_s}^{\alpha_s}$, 则

$$\varphi(n) = n\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right)$$

提示: 使用引理 1 和标准分解式将 $\varphi(n)$ 分解为 $\varphi(p^k)$ 形式的项的乘积.

练习 6

求第 k 小的 $\varphi(n)$ 为合数的数 n. $k \le 10^{100}$.

考虑 $\varphi(n)$ 何时是合数?

引理 2

若 $n > 2$, 则 $2 \mid \varphi(n)$.

$\varphi(1) = \varphi(2) = 1$. 讨论何时 $\varphi(n) = 2$ 即可.

$$p^\alpha - p^{\alpha-1} = 1 \iff p = 2, \alpha = 1$$

$$p^\alpha - p^{\alpha-1} = 2 \iff \begin{cases} p = 2, \alpha = 2 \\ p = 3, \alpha = 1 \end{cases}$$

于是满足 $\varphi(n) = 2$ 的 n 只有 $3, 4, 6$. $\forall n > 6$, $\varphi(n)$ 是合数.

答案: $k = 1$ 时 $n = 5$, 否则 $n = k + 5$.

命题 11

设 p 是素数, 则:

1. $\varphi(p) = p - 1$.
2. 若 $p \mid n$, 则 $\varphi(pn) = p\varphi(n)$.

例 6

分别求 $\varphi(i)$ $(i = 1, 2, \cdots, n)$. $n \leq 10^7$.

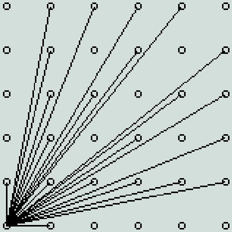
由引理 1 和命题 11 可以利用类似线性筛的方法线性求得.

代码 7 (Euler 函数线性筛)

```
int phi[mxn];
vector<int> ps;
void Euler(int rge) {
    phi[1] = 1;
    for (int i = 2; i <= rge; i++) {
        if (phi[i] == 0)
            phi[i] = i - 1, ps.push_back(i);
        for (int j = 0; j < ps.size()
                    && ps[j] <= rge / i; j++)
            if (i % ps[j])
                phi[i * ps[j]] = phi[i] * (ps[j] - 1);
            else {
                phi[i * ps[j]] = phi[i] * ps[j]; break;
            }
    }
}
```

练习 7

作为体育委员，C 君负责这次运动会仪仗队的训练。仪仗队是由学生组成的 $N \times N$ 的方阵，为了保证队伍在行进中整齐划一，C 君会跟在仪仗队的左后方，根据其视线所及的学生人数来判断队伍是否整齐 (如下图)。现在，C 君希望你告诉他队伍整齐时能看到的学生人数。



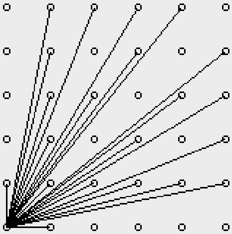
能看见的点关于 $y=x$ 对称. 先考虑该边界下方的点.

观察者位置 $(0,0)$ 能看见的点 (x,y) 一定满足 $\gcd(x,y)=1$.

第 k 列能看见 $\varphi(k)$ 个点.

该区域内的答案 $A=\sum_{k=1}^{n-1}\varphi(k)$.

总答案 $1+2\sum_{k=1}^{n-1}\varphi(k)$.



定理 7 (Euler 定理)

若 $\gcd(a, n) = 1$, 则

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

提示: 用简化剩余系的想法证明.

推论 2 (Fermat 小定理)

设 p 是素数, $p \nmid a$, 则

$$a^p \equiv a \pmod{p}$$

定理 8 (Euler 降幂公式)

$\forall a, x, m \in \mathbb{N}_+$, 若 $x \geq \varphi(m)$, 则

$$a^x \equiv a^{x \% \varphi(m) + \varphi(m)} \pmod{m}$$

Euler 降幂公式的证明请自行阅读相关资料.

练习 8

计算

$$\underbrace{a^{a^{a^{\cdots}}}}_{k个a} \mod m$$

$1 \le k \le 200, 1 \le a \le 10^{18}, 0 < m \le 10^{12}$

使用 Euler 降幂公式递归计算即可.

预处理 $m, \varphi(m), \varphi \circ \varphi(m), \cdots, \varphi_k(m)$, 时间复杂度为 $O(k\sqrt{m})$.

每步递归计算使用快速幂, 递归总复杂度为 $O(k \log m)$.

可能导致爆 `ll`, 考虑手写分治乘法或者使用 `__int128_t`.

总时间复杂度 $O(k\sqrt{m})$.

思考: 多组数据如何优化时间复杂度?

定义 7 (逆元)

对于 $a, m \in \mathbb{Z} : m \neq 0$, 若 $\exists c \in \mathbb{Z}$ s.t.

$$ac \equiv 1 \pmod{m}$$

则称 c 是 a 对模 m 的逆元, 记做 $a^{-1} \pmod{m}$ 或 $\bar{a} \pmod{m}$.

定理 9

a 对模 m 的逆元存在, 当且仅当 $\gcd(a, m) = 1$, 此时逆元唯一.

提示: 用 Bézout 定理.

问题 2

求证:

同余方程 $ax \equiv b \pmod{m}$ 有解当且仅当 $\gcd(a, m) \mid b$, 且在区间 $0 \leq x < m / \gcd(a, m)$ 上有唯一解, 在区间 $0 \leq x < m$ 上有 $\gcd(a, m)$ 个解.

性质 3

$\forall a, b, p \in \mathbb{Z}$: p 是素数, $\gcd(b, p) = 1$. 我们可以扩展定义有理数 a/b 模 p 的同余关系:

$$\frac{a}{b} \equiv a \cdot b^{-1} \pmod p$$

例 7

求 a 对模 m 的逆元, $0 < a < m < 10^9$.

1. 利用 Euler 定理或 Fermat 小定理:

   若 m 是素数, 则 $m \nmid a$ 时逆元存在, $a^{-1} \equiv a^{p-2} \pmod m$.

   否则 $\gcd(a, m) = 1$ 时逆元存在, $a^{-1} \equiv a^{\varphi(m)-1} \pmod m$.

2. 利用 Bézout 定理: 解不定方程 $ax \equiv 1 \pmod m$, 解即 a 的逆元.

时间复杂度为 $O(\log m)$.

例 8

$n, p \in \mathbb{N}_+$: p 是素数. 分别求 $1!, 2!, \cdots, n!$ 和 $1, 2, \cdots, n$ 对模 p 的逆元.

$0 < n \leq 10^7, 1 < p \leq 10^9, n < p$.

先考虑阶乘的逆元.

暴力: 直接求逆元. 时间复杂度为 $O(n \log p)$.

优化: 注意到 $k! = (k-1)! \cdot n$. 于是就有

$$(k-1)!^{-1} \equiv k!^{-1} \cdot k \pmod p$$

于是只需要算出来 $n!$ 及其逆元, 每一个 $k!^{-1}$ 都可以递推得到. 时间复杂度为 $O(n)$.

求得阶乘逆元后立即得到 $k^{-1} \equiv k!^{-1} \cdot (k-1)! \pmod p$.

总时间复杂度为 $O(n)$.

例 9

p 是素数, 分别求 $a_1, a_2, \cdots, a_n$ 的逆元. $0 < n \leq 10^7$, $0 < a_i < p \leq 10^9$ $(i = 1, 2, \cdots, n)$.

参考例 8. $1!, 2!, \cdots, n!$ 是 $1, 2, \cdots, n$ 的前缀乘积.

记 $S(k) := a_1 a_2 \cdots a_k$. 于是有:

$$S(k-1)^{-1} \equiv S(k)^{-1} \cdot a_k \pmod p$$

直接算出 $S(n)^{-1}$, 每一个 $S(k)$ 可以递推得到.

求得前缀积逆元后, 立即得到

$$a_k^{-1} \equiv S(k)^{-1} \cdot S(k-1) \pmod p$$

总时间复杂度为 $O(n)$.

代码 8 (线性求逆元)

```
s[0] = 1;
for (int i = 0; i < n; ++i) s[i + 1] = s[i] * a[i] % p;
sv[n] = qpow(s[n], phi - 1);
for (int i = n; i > 0; --i) sv[i - 1] = sv[i] * a[i - 1] % p;
for (int i = 0; i < n; ++i) inv[i] = sv[i + 1] * s[i] % p;
```

二次剩余 *

思考: $\sqrt{n}$ 在模 m 意义下的值.

应用: 暴力预处理. 时间复杂度 $O(m)$.

阅读: 二次剩余及其性质.

思考: 一个数可以有多少个二次剩余? 使用时应该如何选择?

定义 8 (组合数)

$$C_n^m := \frac{n!}{m!(n-m)!}$$

叫做组合数.

下面讨论求模 p 意义下组合数的方法:

方法一:

若 p 是素数, 直接根据公式, 预处理 $1!, 2!, \cdots, n!$ 及其逆元, 调用时计算

$$C_n^m \equiv n! \cdot m!^{-1} \cdot (n-m)^{-1} \pmod p$$

由例 8, 预处理时空复杂度为 $O(n)$. 调用时间复杂度为 $O(1)$.

适用于 n 较小的情形.

命题 12

$$C_n^m = C_{n-1}^{m-1} + C_{n-1}^m$$

回想 Day4A 题. 数字三角形问题.

方法二:

可以用 dp 方法制作杨辉三角形, 计算组合数. 使用时直接读取即可.

预处理时空复杂度 $O(n^2)$, 调用时间复杂度为 $O(1)$.

适用于 n 较小的场景. 该做法的好处是不受模数限制.

定理 10 (Lucas 定理)

若 p 是素数, 则

$$C_n^m \equiv C_{n\%p}^{m\%p} \cdot C_{n/p}^{m/p} \pmod p$$

方法三:

若 p 是素数, 则可以使用 Lucas 定理.

对于 $C_{n\%p}^{m\%p}$, 直接用方法一计算, 时空复杂度为 $O(p)$.

对于 $C_{n/p}^{m/p}$, 进行递归计算, 计算 $\log_p n$ 次.

总时间复杂度 $O(p \log_p n)$. 适用于 p 较小的场景.

若 p 是合数，想办法转化成质数的情形.

方法四：扩展 Lucas (难点)

设 p 的标准分解式为 $p = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_s}^{\alpha_s}$. 分别解出 $x \equiv C_n^m \pmod{p_i^{\alpha_i}}$ $(i = 1, 2, \cdots, s)$，然后联立方程组，用中国剩余定理求解即可.

问题转化为了如何求解 $x \equiv C_n^m \pmod{p^\alpha}$，其中 p 是素数.

若 $\alpha = 1$，利用 Lucas 定理即可.

否则，利用公式:

$$C_m^n \equiv \frac{n!}{m!(n-m)!} = \frac{\dfrac{n!}{p^{a_1}}}{\dfrac{m!}{p^{a_2}} \cdot \dfrac{(n-m)!}{p^{a_3}}} \cdot p^{a_1 - a_2 - a_3} \pmod{p^\alpha}$$

其中 $a_1=\alpha(p,n),a_2=\alpha(p,m),a_3=\alpha(p,n-m)$. 于是就有

$$\gcd\left(\frac{n!}{p^{a_1}},p^\alpha\right)=\gcd\left(\frac{m!}{p^{a_2}},p^\alpha\right)=\gcd\left(\frac{(n-m)!}{p^{a_3}},p^\alpha\right)=1$$

于是 $\dfrac{n!}{p^{a_1}},\dfrac{m!}{p^{a_2}},\dfrac{(n-m)!}{p^{a_3}}$ 都有逆元.

问题转化为了如何求解 $\dfrac{n!}{p^a} \mod p^\alpha$.

$$n!=p^{\lfloor n/p\rfloor}\cdot\left\lfloor\frac{n}{p}\right\rfloor!\cdot\prod_{(i,p)=1}^{n}i$$

第 2 项进行递归计算, 计算 $\log_p n$ 次.

由于 i 取模后有周期 p^α, 故:

$$\prod_{(i,p)=1}^{n}i\equiv\left(\prod_{(i,p)=1}^{p^\alpha}i\right)^{\lfloor n/p^\alpha\rfloor}\cdot\prod_{(i,p)=1}^{n\%p^\alpha}i \pmod{p^\alpha} \tag{3}$$

(3) 式中第 1 项底数可以预处理, 使用快速幂. 第 2 项暴力计算.

总时间复杂度 $O(p\log n)$.

自行阅读同余类、剩余系定义, 尝试使用等价类和商集来理解.

自行阅读简化剩余系的定义, 思考与 Euler 函数的关系.

命题 13

若 $(a,m)=1$, x 通过模 m 的简化剩余系, 则 ax 也通过模 m 的简化剩余系.

试用命题 13 证明 Euler 定理.

命题 14

若 m_1,m_2 是两个互质的正整数, x_1,x_2 分别通过模 m_1,m_2 的简化剩余系, 则 $m_2x_1+m_1x_2$ 通过通过模 m_1,m_2 的简化剩余系.

试用中国剩余定理理解命题 14.

试用命题 14 证明 Euler 函数通项公式.

定义 9 (群)

若集合 S 装备了二元运算 $+$, 满足: s 有零元, s 有负元且 $+$ 有结合律, 则称 $(S,+)$ 是一个群. 如果群 $(S,+)$ 上的 $+$ 有交换律, 则称 $(S,+)$ 是一个 Abel 群.

$\mathbb{R}$ 关于加法运算是 Abel 群. $\mathbb{R}\backslash 0$ 关于乘法运算是 Abel 群.

$\mathbb{Z}_m$ 关于加法运算是 Abel 群. $\mathbb{Z}_p\backslash 0$ 关于乘法运算是 Abel 群.

扩展阅读: 原根, 循环群, 群的阶, 群表示论, 群同态, 群特征.

定义 10 (环)

若集合 S 装备了二元运算 $+, \times$, $+$ 叫做加法, $\times$ 叫做乘法, 满足: $+$ 有交换律, $+$ 有结合律, s 有零元, s 有负元, $\times$ 有交换律, $\times$ 关于 $+$ 有左交换律和右交换律, 则称 $(S, +, \times)$ 是一个环. 如果 $\times$ 满足交换律, 则称 S 是交换环.

$\mathbb{R}$ 是交换环. $M_n(\mathbb{R})$ 是环, 但不是交换环.

定义 11 (域)

若 S 是交换环, 且 $\times$ 有不是零元的幺元, S 中的任意非零元都有逆元, 则称 S 是一个域.

$\mathbb{Z}_p$ 是一个域.

- 闵嗣鹤, 严士健. 初等数论 (第三版). 北京: 高等教育出版社. 2003.
- 秋叶拓哉, 岩田阳一, 北川宜稔. 挑战程序设计竞赛 (第 2 版). 北京: 人民邮电出版社. 2013.
- Ronald L. Graham, Donald E. Knuth, Oren Patashnik. 具体数学：计算机科学基础 (第 2 版). 北京: 人民邮电出版社. 2013.
- B.A. 卓里奇. 数学分析 (第一卷)(第 4 版). 北京: 高等教育出版社, 2006.
- 丘维声. 高等代数. 北京: 科学出版社. 2013.