基础数论 Day2

2023 SDUTACM 寒假集训

凌乱之风

山东理工大学

2023 年 2 月 3 日

目录

快速幂

定义

快速幂可以 $O(\log n)$ 计算 $a^n \bmod p$

算法

考虑将指数用二进制来表示。最多有 $\lfloor \log n \rfloor + 1$ 个二进制位。所以只需要用 $O(\log n)$ 次乘法就可以算出答案。

参考代码 (时间复杂度 $O(\log n)$):

```
int power(int a, int n, int p) {
    int res = 1;
    while (n) {
        if (n & 1) {
            res = 1LL * res * a % p;
        }
        a = 1LL * a * a % p;
        n >>= 1;
    }
    return res;
}
```

同余

定义

若整数 a, b 除以正整数 m 所得的余数相等，则称 a, b 模 m 同余。记作 $a \equiv b \pmod m$

例

$26 \equiv 14 \pmod{12}$

性质

- 整除性：$m \mid (a-b)$，即 $a - b = k \times m, k \in \mathbb{Z}$
- 传递性：$a \equiv b \pmod m, b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$
- 基本运算：
  $a \equiv b \pmod m, c \equiv d \pmod m \Rightarrow a \pm c \equiv b \pm d \pmod m$
  $a \equiv b \pmod m, c \equiv d \pmod m \Rightarrow a \times c \equiv b \times d \pmod m$
  $a \equiv b \pmod m \Rightarrow a \times n \equiv b \times n \pmod m, n \in \mathbb{Z}$
- 除法原理：若 $k \times a \equiv k \times b \pmod m$，且 k, m 互质，则 $a \equiv b \pmod m$

欧拉定理

定义

若正整数 a, m 满足 $\gcd(a, m) = 1$，则 $a^{\varphi(m)} \equiv 1 \pmod{m}$

证明

设 $1 \sim m$ 中与 m 互质的数的序列为 $x_1, x_2, \cdots, x_{\varphi(m)}$
再设另一个序列 $ax_1, ax_2, \cdots, ax_{\varphi(m)}$，其中 $\gcd(a, m) = 1$

引理 1：$ax_1, ax_2, \cdots, ax_{\varphi(m)}$ 模 m 后两两互不相同

反证：假设 $\exists i, j \in [1, \varphi(m)]$ 满足 $ax_i \equiv ax_j \pmod{m}$，那么 $m \mid a(x_j - x_i)$，由于 $\gcd(a, m) = 1$，所以 $m \mid (x_j - x_i)$，与 $0 < x_j - x_i < m$ 矛盾。

引理 2：$ax_1, ax_2, \cdots, ax_{\varphi(m)}$ 模 m 后与 m 互质

反证：假设 $\exists i \in [1, \varphi(m)]$ 满足 $ax_i \equiv t \pmod{m}$ 且 $\gcd(t, m) \neq 1$，那么设 $d = \gcd(t, m)$，所以 $d \mid t, d \mid m$，根据 $ax_i = k \times m + t$ 得出 $d \mid ax_i$，与 $\gcd(ax_i, m) = 1$ 矛盾。

欧拉定理

证明 (续)

由引理 1 和引理 2 可知，$ax_1, ax_2, \cdots, ax_{\varphi(m)}$ 是 $x_1, x_2, \cdots, x_{\varphi(m)}$ 的一个排列，所以有

$$ax_1 ax_2 \cdots ax_{\varphi(m)} \equiv x_1 x_2 \cdots x_{\varphi(m)} \pmod{m}$$

即

$$a^{\varphi(m)} x_1 x_2 \cdots x_{\varphi(m)} \equiv x_1 x_2 \cdots x_{\varphi(m)} \pmod{m}$$

根据除法原理得

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

1. 快速幂
2. 同余
3. 欧拉定理与费马小定理
   - 欧拉定理
   - 费马小定理
4. 乘法逆元
5. 扩展欧几里得
6. 习题

费马小定理

定义

若质数 p 和正整数 a 满足 $\gcd(a,p)=1$，则 $a^{p-1}\equiv 1 \pmod p$

证明

由于 $\varphi(p)=p-1$ 其中 p 为质数，所以根据欧拉定理得 $a^{p-1}\equiv 1 \pmod p$

乘法逆元

定义

若 $ax \equiv 1 \pmod{p}$，则称 x 是 a 模 p 意义下的乘法逆元。记作 a^{-1}

费马小定理求逆元

设质数 p，那么正整数 a 满足

$$a \times a^{-1} \equiv 1 \pmod{p}$$

根据费马小定理 $a^{p-1} \equiv 1 \pmod{p}$

$$a \times a^{-1} \equiv a^{p-1} \pmod{p}$$

得出逆元

$$a^{-1} \equiv a^{p-2} \pmod{p}$$

可以使用快速幂求解。

参考代码 (时间复杂度 $O(\log n)$):

```
int inv(int a, int p) {
    return power(a, p - 2, p);
}
```

扩展欧几里得

引理 1：裴蜀定理

设 a, b 是不全为 0 的整数，则 $\exists x, y$ 满足 $ax + by = \gcd(a, b)$

算法

由裴蜀定理得

$$
\begin{aligned}
ax + by = \gcd(a, b) &= \gcd(b, a \bmod b) && (1)\\
&= bx' + (a \bmod b)y' && (2)\\
&= bx' + (a - \lfloor \frac{a}{b} \rfloor \times b)y' && (3)\\
&= ay' + b(x' - \lfloor \frac{a}{b} \rfloor \times y') && (4)
\end{aligned}
$$

所以 $x = y', y = x' - \lfloor \frac{a}{b} \rfloor \times y'$，递归边界当 $b = 0$ 时，$x = 1, y = 0$

参考代码 (时间复杂度 $O(\log n)$):

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

扩展欧几里得求线性同余方程

线性同余方程定义

形如 $ax \equiv t \pmod{b}$ 的方程称为线性同余方程，其中 a, b, t 为给定整数，x 为未知数。

求解

即求解 $ax + by \equiv t$
根据裴蜀定理，有解的条件为 $\gcd(a, b) \mid t$
首先求解 $ax + by \equiv \gcd(a, b)$，得到一组解 x_0, y_0 满足 $ax_0 + by_0 \equiv \gcd(a, b)$
两边除以 $\gcd(a, b)$ 再乘 t

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

所以解为 $x = \dfrac{t}{\gcd(a, b)}x_0, y = \dfrac{t}{\gcd(a, b)}y_0$

习题 1.【模板】快速幂 || 取余运算

题目链接：https://www.luogu.com.cn/problem/P1226

习题 2.【模板】乘法逆元

题目链接：https://www.luogu.com.cn/problem/P3811

习题 3.[NOIP2012 提高组] 同余方程

题目链接：https://www.luogu.com.cn/problem/P1082

习题 4. 青蛙的约会

题目链接：https://www.luogu.com.cn/problem/P1516

习题 5.[2022ICPC 杭州 A] Modulo Ruins the Legend

题目链接：https://codeforces.com/gym/104090/problem/A

习题 6.[2022CCPC 桂林 E] Draw a triangle

题目链接：https://codeforces.com/gym/104008/problem/E

习题 7.Ginger 的数

题目链接：https://ac.nowcoder.com/acm/contest/49030/F

Thanks!