数论基础

陈劭源

Feb 12, 2019

自我介绍

- 陈劭源
- 南京大学匡亚明学院
- QQ：1977009005
- Codeforces: `sy_chen`
- 获奖记录
  - NOIP2014 提高组江苏省一等奖
  - 第四届中国大学生程序设计竞赛（吉林站）金奖
  - 2018 ACM-ICPC 徐州站金奖
  - 2018 ACM-ICPC EC-Final 金奖（第四名）

课堂练习和作业

- 洛谷（https://www.luogu.org/）
- 请进入以下链接，加入 nfls_wc 团队：
  https://www.luogu.org/team/show?teamid=15021
- 课堂练习和作业将在团队作业中发布。

基本概念

取模运算： $a \bmod b$ 表示 a 除以 b 的余数，即最小的**非负整数** c，使得 $a - c$ 是 b 的倍数。

例如：$12 \bmod 5 = 2,\ -3 \bmod 7 = 4$

注意：这里定义的取模运算和 C++ 等编程语言中的取模运算 (a % b) 不完全一致。C++ 的取模运算在操作的时候，如果操作数有负数，那么结果也有可能是负数（通常是和被除数的符号相同），但这里定义的取模运算结果总是非负整数。如果涉及到负数的取模，在 C++ 中一般会写成这样：

```
(a % b + b) % b
```

基本概念

取模运算的基本性质：

1. $0 \leq a \bmod c < c$。我们把所有不超过 c 的非负整数全体记为 $\mathbb{Z}_c$。

基本概念

取模运算的基本性质：

1. $0 \leq a \bmod c < c$。我们把所有不超过 c 的非负整数全体记为 $\mathbb{Z}_c$。
2. $(a+b) \bmod c = ((a \bmod c) + (b \bmod c)) \bmod c$

基本概念

取模运算的基本性质：

1. $0 \leq a \bmod c < c$。我们把所有不超过 c 的非负整数全体记为 $\mathbb{Z}_c$。
2. $(a+b) \bmod c = ((a \bmod c)+(b \bmod c)) \bmod c$
3. $(a-b) \bmod c = ((a \bmod c)-(b \bmod c)) \bmod c$

基本概念

取模运算的基本性质：

1. $0 \leq a \bmod c < c$。我们把所有不超过 c 的非负整数全体记为 $\mathbb{Z}_c$。
2. $(a+b) \bmod c = ((a \bmod c)+(b \bmod c)) \bmod c$
3. $(a-b) \bmod c = ((a \bmod c)-(b \bmod c)) \bmod c$
4. $ab \bmod c = (a \bmod c)(b \bmod c) \bmod c$

基本概念

同余：记号 $a \equiv b \pmod{c}$ 表示 a 和 b 模 c 同余，即

$$a \bmod c = b \bmod c$$

例如：$3 \equiv 5 \pmod{2}$, $10 \equiv 3 \pmod{7}$, $-4 \equiv 8 \pmod{6}$。

基本概念

同余：记号 $a \equiv b \pmod{c}$ 表示 a 和 b 模 c 同余，即

$$a \bmod c = b \bmod c$$

例如：$3 \equiv 5 \pmod{2}$, $10 \equiv 3 \pmod{7}$, $-4 \equiv 8 \pmod{6}$。

线性同余方程：形如

$$ax \equiv b \pmod{n}$$

$(n > 0)$ 的方程称为线性同余方程，其中 x 为未知数。

例：$3x \equiv 4 \pmod{5}$ 是线性同余方程。你能找出它的解吗？

基本概念

同余：记号 $a \equiv b \pmod{c}$ 表示 a 和 b 模 c 同余，即

$$a \bmod c = b \bmod c$$

例如：$3 \equiv 5 \pmod{2}$, $10 \equiv 3 \pmod{7}$, $-4 \equiv 8 \pmod{6}$。

线性同余方程：形如

$$ax \equiv b \pmod{n}$$

$(n > 0)$ 的方程称为线性同余方程，其中 x 为未知数。

例：$3x \equiv 4 \pmod{5}$ 是线性同余方程。你能找出它的解吗？

$3, 8, 13, 18, -2, -7, -12, -17$ 等都是这个线性同余方程的解。

线性同余方程

例：$3x \equiv 4 \pmod 5$ 是线性同余方程。你能找出它的解吗？
$3, 8, 13, 18, -2, -7, -12, -17$ 等都是这个线性同余方程的解。

1. 这些解之间有什么规律？

线性同余方程

例：$3x \equiv 4 \pmod 5$ 是线性同余方程。你能找出它的解吗？
$3, 8, 13, 18, -2, -7, -12, -17$ 等都是这个线性同余方程的解。

1. 这些解之间有什么规律？

一般来说，对于方程 $ax \equiv b \pmod c$，如果 x_0 是一个解，那么 $x_0 + kc$ 也是这个方程的解。

2. 是否所有线性同余方程都有解？

线性同余方程

例：$3x \equiv 4 \pmod 5$ 是线性同余方程。你能找出它的解吗？
$3, 8, 13, 18, -2, -7, -12, -17$ 等都是这个线性同余方程的解。

1. 这些解之间有什么规律？

一般来说，对于方程 $ax \equiv b \pmod c$，如果 x_0 是一个解，那么 $x_0 + kc$ 也是这个方程的解。

2. 是否所有线性同余方程都有解？

并不是。$2x \equiv 3 \bmod 4$ 就没有解。（为什么？）

那么，什么情况下

线性同余方程

例：$3x \equiv 4 \pmod 5$ 是线性同余方程。你能找出它的解吗？
$3, 8, 13, 18, -2, -7, -12, -17$ 等都是这个线性同余方程的解。

1. 这些解之间有什么规律？

线性同余方程

例：$3x \equiv 4 \pmod 5$ 是线性同余方程。你能找出它的解吗？
$3, 8, 13, 18, -2, -7, -12, -17$ 等都是这个线性同余方程的解。

1. 这些解之间有什么规律？

一般来说，对于方程 $ax \equiv b \pmod c$，如果 x_0 是一个解，那么 $x_0 + kc$ 也是这个方程的解。

2. 是否所有线性同余方程都有解？

线性同余方程

例：$3x \equiv 4 \pmod 5$ 是线性同余方程。你能找出它的解吗？
$3, 8, 13, 18, -2, -7, -12, -17$ 等都是这个线性同余方程的解。

1. 这些解之间有什么规律？

一般来说，对于方程 $ax \equiv b \pmod c$，如果 x_0 是一个解，那么 $x_0 + kc$ 也是这个方程的解。

2. 是否所有线性同余方程都有解？

并不是。$2x \equiv 3 \bmod 4$ 就没有解。（为什么？）

线性同余方程

如果引入未知数 y，那么方程 $ax \equiv d \pmod{b}$ 就可以改写成 $ax - by = d$。令 $b' = -b$，方程又可以写为 $ax + b'y = d$。因此只要讨论形如 $ax + by = d$ 的方程的解法就行了。这样的方程称为**裴蜀方程**。

线性同余方程

如果引入未知数 y，那么方程 $ax \equiv d \pmod{b}$ 就可以改写成 $ax - by = d$。令 $b' = -b$，方程又可以写为 $ax + b'y = d$。因此只要讨论形如 $ax + by = d$ 的方程的解法就行了。这样的方程称为**裴蜀方程**。

裴蜀定理：$ax + by = d$ 有解的充分必要条件是 $d \mid \gcd(a, b)$。

推论：$ax + by = 1$ 有解当且仅当 a, b 互质。

线性同余方程

如果引入未知数 y，那么方程 $ax \equiv d \pmod{b}$ 就可以改写成 $ax - by = d$。令 $b' = -b$，方程又可以写为 $ax + b'y = d$。因此只要讨论形如 $ax + by = d$ 的方程的解法就行了。这样的方程称为**裴蜀方程**。

裴蜀定理：$ax + by = d$ 有解的充分必要条件是 $d | \gcd(a, b)$。

推论：$ax + by = 1$ 有解当且仅当 a, b 互质。

例如：$3x - 2y = 5$ 一定有解，例如 $x = 3, y = 2$。$4x + 2y = 1$ 肯定无解，因为 $4x + 2y$ 一定是 2 的倍数。

线性同余方程

如果引入未知数 y，那么方程 $ax \equiv d \pmod{b}$ 就可以改写成 $ax - by = d$。令 $b' = -b$，方程又可以写为 $ax + b'y = d$。因此只要讨论形如 $ax + by = d$ 的方程的解法就行了。这样的方程称为**裴蜀方程**。

裴蜀定理：$ax + by = d$ 有解的充分必要条件是 $d | \gcd(a, b)$。

推论：$ax + by = 1$ 有解当且仅当 a, b 互质。

例如：$3x - 2y = 5$ 一定有解，例如 $x = 3, y = 2$。$4x + 2y = 1$ 肯定无解，因为 $4x + 2y$ 一定是 2 的倍数。

另外，如果找到了 $ax + by = d$ 的一组解 (x_0, y_0)，那么 $(x_0 + kb/g, y_0 - ka/g)$，其中 $g = \gcd(a, b)$ 都是这个方程的解。

线性同余方程

那么，如何求 $ax+by=d$（其中 $d=\gcd(a,b)$）的一个解呢？考虑欧几里得算法

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

这个算法实际上是利用了 $\gcd(a,b)=\gcd(b,a \bmod b)=d$ 这个性质。

扩展欧几里得算法

$$\gcd(a, b) = \gcd(b, a \bmod b) = d$$

根据裴蜀定理，$ax + by = d$ 和 $bx + (a \bmod b)y = d$ 都有解。那么，我们可不可以根据 $bx + (a \bmod b)y = d$ 的解得到 $ax + by = d$ 的解呢？

扩展欧几里得算法

$$\gcd(a,b)=\gcd(b,a \bmod b)=d$$

根据裴蜀定理，$ax+by=d$ 和 $bx+(a \bmod b)y=d$ 都有解。那么，我们可不可以根据 $bx+(a \bmod b)y=d$ 的解得到 $ax+by=d$ 的解呢？

可以！假设 $by_0+(a \bmod b)x_0=d$，那么注意到 $a=a \bmod b+b\lfloor a/b \rfloor$，从而

$$by_0+(a \bmod b+b\lfloor a/b \rfloor)x_0-b\lfloor a/b \rfloor x_0=d$$
$$(a \bmod b+b\lfloor a/b \rfloor)x_0+b(y_0-\lfloor a/b \rfloor x_0)=d$$
$$ax_0+b(y_0-\lfloor a/b \rfloor x_0)=d$$

也就是说，$(x_0, y_0-\lfloor a/b \rfloor x_0)$ 是 $ax+by=d$ 的一组解！

扩展欧几里得算法

$$by_0 + (a \bmod b)x_0 = d$$
$$ax_0 + b(y_0 - \lfloor a/b \rfloor x_0) = d$$

利用这一性质，我们可以修改欧几里得算法，在求出 $\gcd(a, b)$ 的同时，还可以求出方程 $ax + by = \gcd(a, b)$ 的一对整数解。新得到的这个算法就称为**扩展欧几里得算法**。

扩展欧几里得算法

$$by_0 + (a \bmod b)x_0 = d$$
$$ax_0 + b(y_0 - \lfloor a/b \rfloor x_0) = d$$

利用这一性质，我们可以修改欧几里得算法，在求出 $\gcd(a, b)$ 的同时，还可以求出方程 $ax + by = \gcd(a, b)$ 的一对整数解。新得到的这个算法就称为**扩展欧几里得算法**。

练习：求 $\gcd(14, 39)$ 以及方程 $14x + 39y = 1$ 的一对整数解。

扩展欧几里得算法

练习：求 $\gcd(14, 39)$ 以及方程 $14x + 39y = 1$ 的一对整数解。

扩展欧几里得算法

练习：求 $\gcd(14,39)$ 以及方程 $14x+39y=1$ 的一对整数解。

$$
\begin{aligned}
39 &= 14\cdot 2+11\\
14 &= 11\cdot 1+3\\
11 &= 3\cdot 3+2\\
3 &= 2\cdot 1+1\\
2 &= 1\cdot 2+0
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3+(-1)\cdot 2\\
&= 3+(-1)\cdot(11-3\cdot 3)\\
&= 4\cdot(14-1\cdot 11)+(-1)\cdot 11\\
&= 4\cdot 14+(-5)\cdot(39+(-2)\cdot 14)\\
&= 14\cdot 14+(-5)\cdot 39
\end{aligned}
$$

扩展欧几里得算法

扩展欧几里得算法的代码实现

```
void exgcd(LL a, LL b, LL &g, LL &x, LL &y) {
    if (b == 0) { g = a; x = 1; y = 0;}
    else {
        exgcd(b, a % b, g, y, x);
        y -= x * (a / b);
    }
}
```

其中，g 存放求出的 $\gcd(a,b)$，x,y 则存放方程 $ax+by=g$ 的一组整数解。求出了 $ax+by=g$ 的一组整数解 (x,y) 后，这个方程的全部整数解都可以写成 $(x+kb/g, y-ka/g)$ 的形式。

注意：上述代码求出的解是 $|x|+|y|$ 最小的一个解，因此使用扩展欧几里得算法时通常不需要担心整数溢出的问题。

扩展欧几里得算法

这样我们可以用扩展欧几里得算法求出 $ax+by=d$（其中 $d=\gcd(a,b)$ 的一组整数解。

如果 d 是 $\gcd(a,b)$ 的倍数，如何求 $ax+by=d$ 的解？

扩展欧几里得算法

这样我们可以用扩展欧几里得算法求出 $ax+by=d$（其中 $d=\gcd(a,b)$ 的一组整数解。

如果 d 是 $\gcd(a,b)$ 的倍数，如何求 $ax+by=d$ 的解？

解：求出 $ax+by=\gcd(a,b)$ 的解 (x_0,y_0)，然后 $(x_0 d/\gcd(a,b), y_0 d/\gcd(a,b))$ 就是方程 $ax+by=d$ 的解。

乘法逆元

线性同余方程 $ax \equiv 1 \pmod{p}$ 的解称为 a 关于 p 的**乘法逆元**（简称**逆元**）或者**数论倒数**，记为 $x = a_p^{-1}$。当省略模数也不会引起混淆时，通常直接写成 a^{-1}。

例如：3 关于 5 的乘法逆元是 2，7 关于 8 的乘法逆元是 7。

$6 \times 3 \times 2 \bmod 5 = 6$，这里，3 的乘法逆元 2 把“乘 3”的效果抵消掉了。乘法逆元的名称就是这么来的。

乘法逆元

线性同余方程 $ax \equiv 1 \pmod{p}$ 的解称为 a 关于 p 的**乘法逆元**（简称**逆元**）或者**数论倒数**，记为 $x = a_p^{-1}$。当省略模数也不会引起混淆时，通常直接写成 a^{-1}。

例如：3 关于 5 的乘法逆元是 2，7 关于 8 的乘法逆元是 7。

$6 \times 3 \times 2 \bmod 5 = 6$，这里，3 的乘法逆元 2 把“乘 3”的效果抵消掉了。乘法逆元的名称就是这么来的。

根据裴蜀定理的推论，a 关于 p 的乘法逆元存在的充分必要条件是 a 与 p 互质。可以利用扩展欧几里得算法直接解线性同余方程 $ax \equiv 1 \pmod{p}$，从而得到乘法逆元。

乘法逆元

有了乘法逆元，我们就可以定义模运算下的除法：

模意义下除以一个数，等于乘以这个数的乘法逆元。

乘法逆元

有了乘法逆元，我们就可以定义模运算下的除法：

模意义下除以一个数，等于乘以这个数的乘法逆元。

这样，四种四则运算都有了模意义下的对应运算

名称	四则运算	模运算
加法	$a+b$	$(a+b) \bmod p$
减法	$a-b$	$(a-b) \bmod p$
乘法	$a \times b$	$(ab) \bmod p$
除法	$a \div b$	$(ab^{-1}) \bmod p$

当除数和模数互质时，模运算除法才有意义。

乘法逆元

有了乘法逆元，我们就可以定义模运算下的除法：

模意义下除以一个数，等于乘以这个数的乘法逆元。

这样，四种四则运算都有了模意义下的对应运算

名称	四则运算	模运算
加法	$a+b$	$(a+b) \bmod p$
减法	$a-b$	$(a-b) \bmod p$
乘法	$a \times b$	$(ab) \bmod p$
除法	$a \div b$	$(ab^{-1}) \bmod p$

当除数和模数互质时，模运算除法才有意义。

模运算有和四则运算完全相同的运算律。

乘法逆元

求乘法逆元的方法：

- 扩展欧几里得算法

乘法逆元

求乘法逆元的方法：

- 扩展欧几里得算法
- 对于模数 p 是质数的情况，由费马小定理可知，对于与 p 互质的 a，有

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

从而 $a^{p-2} \bmod p$ 就是 a 关于 p 的乘法逆元。
这种方法也可以推广到当 p 不是质数的情况（参考欧拉定理）。

乘法逆元

求乘法逆元的方法：

- 扩展欧几里得算法
- 对于模数 p 是质数的情况，由费马小定理可知，对于与 p 互质的 a，有

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

从而 $a^{p-2} \bmod p$ 就是 a 关于 p 的乘法逆元。
这种方法也可以推广到当 p 不是质数的情况（参考欧拉定理）。

- 利用递推公式

$$i^{-1} = -\left\lfloor \frac{p}{i} \right\rfloor \cdot (p \bmod i)^{-1} \bmod p$$

可以在线性时间内求出前 n 个正整数的乘法逆元。

练习

洛谷 P1082：用欧几里得算法求逆元。

练习

洛谷 P1082：用欧几里得算法求逆元。

扩展：利用欧拉定理求逆元

> 如果 $\gcd(a,p)=1$，那么 $a^{\phi(p)} \equiv 1 \pmod{p}$。
> 其中，$\phi(p)$ 的定义如下：将 p 分解质因数
>
> $$p=\prod {p_i}^{a_i}$$
>
> 那么 $\phi(p)=\prod(p_i-1){p_i}^{a_i-1}$。

线性同余方程组

如下形式的方程组称为**线性同余方程组**

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases}$$

线性同余方程组

如下形式的方程组称为**线性同余方程组**

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases}$$

中国剩余定理：当 b_1 和 b_2 互质时，上述方程组的所有解可写成 $x_0 + kb_1b_2$ 的形式，即可以合并成

$$x \equiv x_0 \pmod{b_1b_2}$$

这一个方程。

线性同余方程组

如下形式的方程组称为**线性同余方程组**

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases}$$

中国剩余定理：当 b_1 和 b_2 互质时，上述方程组的所有解可写成 $x_0 + kb_1b_2$ 的形式，即可以合并成

$$x \equiv x_0 \pmod{b_1b_2}$$

这一个方程。

当 b_1 和 b_2 不互质呢？

线性同余方程组

如下形式的方程组称为**线性同余方程组**

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases}$$

中国剩余定理：当 b_1 和 b_2 互质时，上述方程组的所有解可写成 $x_0 + kb_1b_2$ 的形式，即可以合并成

$$x \equiv x_0 \pmod{b_1b_2}$$

这一个方程。

当 b_1 和 b_2 不互质呢？

仅当 $a_1 \equiv a_2 \pmod{\gcd(b_1, b_2)}$ 时有解。此时的解可以写成 $x_0 + k\operatorname{lcm}(b_1, b_2)$，即方程组可以合并成

$$x \equiv x_0 \pmod{\operatorname{lcm}(b_1, b_2)}$$

线性同余方程组

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases} \Rightarrow \quad x \equiv x_0 \pmod{\operatorname{lcm}(b_1, b_2)}$$

那么，如何确定 x_0 的值呢？

线性同余方程组

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \end{cases} \Rightarrow \quad x \equiv x_0 \pmod{\operatorname{lcm}(b_1, b_2)}$$

那么，如何确定 x_0 的值呢？

注意到

$$x_0 = k_1 b_1 + a_1 = k_2 b_2 + a_2$$

其中 k_1, k_2 是待定系数。改写一下等式，可以得到

$$k_1 b_1 - k_2 b_2 = a_2 - a_1$$

这是裴蜀方程，可以用扩展欧几里得算法求解。

练习

洛谷 P4777：解线性同余方程组。

注意事项

1. 如果方程组包含多于两个线性同余方程，逐个合并即可。
2. 两个**long long**相乘时可能会发生溢出。可以类比快速幂，实现两个**long long**相乘。
3. 题目中保证答案不超过 10^{18}，意思是所有模数的 lcm 不超过 10^{18}。

```
LL mulmod(LL a, LL b, LL p) {
    b = (b % p + p) % p;
    LL r = 0;
    while (b) {
        if (b & 1) r = (r + a) % p;
        a = (a + a) % p;
        b >>= 1;
    }
    return r % p;
}
```

练习题

- 洛谷 P3811：逐个求逆元可能过不了，需要使用线性求逆元的方法。
- 洛谷 P1313：可以利用模运算计算组合数，从而避免大数运算。
- 洛谷 P1516：裴蜀定理、扩展欧几里得算法的应用。
- 洛谷 P3951：可以先尝试着找规律。