第3章 一次同余方程

3.1 一次同余方程

【定义3.1.1】 记多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

$$n\in N, i\in[0,n], a_i\in Z.$$

设$m\in N, m\nmid a_n$, 则同余方程$f(x)\equiv 0 \pmod m$称为模m的同余方程, n称为$f(x)$的次数, 记为$\deg f(x)$或$\deg(f)$（deg为degree的前三个字母）.

同余方程的解

若a满足$f(x) \equiv 0 \pmod m$, 则满足$x \equiv a \pmod m$的所有整数都是方程的解. 即剩余类

$$C_a = \{x \mid x \in Z, x \equiv a \pmod m\}$$

中的每个剩余都是解, 并说剩余类C_a是同余方程$f(x) \equiv 0 \pmod m$的一个解. 这个解通常记为$x \equiv a \pmod m$.

当a_i, a_j均为同余方程$f(x) \equiv 0 \pmod m$的解, $a_i \not\equiv a_j \pmod m$, 就称它们是不同的解. 所有对模m的两两不同余的解的个数, 称为是同余方程的解数.

同余方程-求解

由同余方程的解的定义可知, 若同余方程有解, 则遍历模 的一个完全剩余系, 就能找到其所有的解. 通常选择遍历模 的最小非负完全剩余系.这种方法适合模数较小的情形.

一次同余方程-举例

【例3.1.1】 求解同余方程$5x \equiv 3 \pmod 7$.

解: 将模7的一个完全剩余系中的剩余代入方程中, 这里选择最小非负完全剩余系{0, 1, 2, 3, 4, 5, 6}. 因 $5\times 2\equiv 10\equiv 3 \pmod 7$, 故 $x \equiv 2 \pmod 7$ 为同余方程的所有解.

【例3.1.2】 求解同余方程$4x \equiv 2 \pmod 6$.

解: 将模6的一个完全剩余系中的剩余代入方程中, 这里选择最小非负完全剩余系{0, 1, 2, 3, 4, 5}. 因

$4\times 2\equiv 8\equiv 2 \pmod 6$, $4\times 5\equiv 20\equiv 2 \pmod 6$,

故$x \equiv 2 \pmod 6, x \equiv 5 \pmod 6$为同余方程的所有解.

一次同余方程-举例

【例3.1.3】 求解同余方程$3x \equiv 2 (\mathrm{mod}\ 6)$.

解: 将模6的一个完全剩余系中的剩余代入方程中, 这里选择最小非负完全剩余系{0,1,2,3,4,5}. 因都不满足方程, 故同余方程的无解.

【例3.1.4】 求同余方程$4x^2+27x-12$≡0(mod 15)的解.

解: 取模15的绝对值最小完全剩余系: -7, -6, ..., -1, 0, 1, 2, ..., 7, 直接计算知x＝-6, 3是解. 所以, 该同余方程的解是

x≡-6, 3(mod 15).

一次同余方程-性质

【定理3.1.1】 设$a \in Z, m \in N$, 若$(a, m) = 1$, 则同余方程$ax \equiv 1(mod\ m)$有唯一解.

证明: 由于0, 1, 2, 3, …, $m-1$为模m的一个完全剩余系, $(a, m) = 1$, 故$0, a, 2a, \dots, (m-1)a$也组成模m的一个完全剩余系, 故其中必有且仅有一个数
$s \times a, s \in (0, m-1]$, 且$n$为整数, 使得等式
$s \times a \equiv 1(\mathrm{mod}\, m)$成立.

实际上, 运用欧几里德算法, 可求得$s, t \in Z$, 使得
$sa + tm = 1$. 等式两端模m, 得到$as \equiv 1(\mathrm{mod} m)$. 则
$x \equiv s(\mathrm{mod} m)$即为同余方程的解.

一次同余方程-举例

【例3.1.5】 解同余方程$15x \equiv 1(\mathrm{mod}28)$.

解: 由于(15,28)=1,方程有唯一解.

由欧几里德算法

28=15+13　15=13+2　13=6×2+1

1=13-6×2

=13-6×(15-13)=13×7-6×15

=(28-15)×7-6×15=28×7-13×15

即: 1=28×7-13×15

等式两端模28得15×(-13)≡1(mod 28).

故 x≡-13≡15(mod 28)

一次同余方程-性质

【定理3.1.2】 设$a \in Z, m \in N, (a, m) = 1$, 则同余方程$ax \equiv b(\bmod m)$有唯一解.

证明: 唯一性证明. 由于0, 1, 2, 3, ..., $m-1$为模m的一个完全剩余系, $(a, m) = 1$, 故$0, a, 2a, \dots, (m-1)a$也组成模m的一个完全剩余系, 故其中必有且仅有一个数$i \times a, i \in (0, m-1]$, 且$i$为整数, 使得$i \times a \equiv b(\bmod m)$成立.

一次同余方程-性质

【定理3.1.2】 设$a \in Z, m \in N, (a,m) = 1$,则同余方程$ax \equiv b \pmod m$有唯一解.

求解过程: 由【定理3.1.1】, $(a,m) = 1$, $ax \equiv 1 \pmod m$有解, 设解为$x \equiv x_0 \pmod m$, 即$ax_0 \equiv 1 \pmod m$.又$b \equiv b \pmod m$, 故$(ax_0)b \equiv b \pmod m$. 也即$a(bx_0) \equiv b \pmod m$, 对比同余方程$ax \equiv b \pmod m$可知同余方程的解为$x \equiv bx_0 \pmod m$.

一次同余方程-举例

【例3.1.6】 求解同余方程$15x \equiv 3 \pmod{28}$.

解: 由【例3.1.5】知, $15x \equiv 1 \pmod{28}$的解为

$$x \equiv 15 \pmod{28}.$$

故同余方程$15x \equiv 3 \pmod{28}$的解为

$$x \equiv 3 \times 15 \equiv 45 \equiv 17 \pmod{28}.$$

一次同余方程-性质

【定理3.1.3】 设$a \in Z, m \in N, (a,m)=d$,则同余方程$ax \equiv b \pmod m$有解的充要条件是$d|b$. 并且有解时, 解数为$d=(a,m)$.

证明: 必要性 即已知同余方程$ax \equiv b \pmod m$有解, 去证明$(a,m)|b$.

设方程的解为$x \equiv s \pmod m$, 则存在整数t, 使得

$$as - mt = b.$$

因为$(a,m)|a, (a,m)|m$,故$(a,m)|\ as - mt = b$.必要性成立.

一次同余方程-性质

下面证明充分性, 即已知$(a,m)|b$,证明方程$ax \equiv b \pmod m$有解.

（1）先考虑同余方程 $\frac{a}{(a,m)}x\equiv 1 \left(\bmod \frac{m}{(a,m)}\right)$的解.

因为$\left(\frac{a}{(a,m)},\frac{m}{(a,m)}\right)=1$,由【定理3.1.1】, 方程有唯一解. 记方程的解为$x \equiv x_0 \left(\bmod \frac{m}{(a,m)}\right)$.

一次同余方程-性质

（2）现考虑同余方程$\frac{a}{(a,m)}x\equiv\frac{b}{(a,m)}(\text{mod }\frac{m}{(a,m)})$的解.

由【定理3.1.2】, 方程$\frac{a}{(a,m)}x\equiv\frac{b}{(a,m)}(\text{mod }\frac{m}{(a,m)})$的解为

$$x\equiv\frac{b}{(a,m)}x_0\left(\text{mod}\,\frac{m}{(a,m)}\right).$$

由同余性质, 若$\frac{a}{(a,m)}x\equiv\frac{b}{(a,m)}\left(\text{mod}\,\frac{m}{(a,m)}\right)$, 则$ax\equiv b(\text{mod}\,m)$. 即$x\equiv\frac{b}{(a,m)}x_0(\text{mod}\,m)$是方程$ax\equiv b(\text{mod}\,m)$的一个特解.

一次同余方程-性质

（3）写出同余方程$ax \equiv b \pmod m$的全部解为
$x \equiv \frac{b}{(a,m)} x_0 + \frac{m}{(a,m)} t \pmod m, t = 0,1,2,\ldots,(a,m) - 1.$

一次同余方程-性质

为什么说上述形式包含了方程的所有解？

事实上，若有$ax' \equiv ax \equiv b \pmod{m}$,则

$$a(x - x') \equiv 0 \pmod{m}.$$

故$\frac{a}{(a,m)}(x - x') \equiv 0 \left(\bmod \frac{m}{(a,m)}\right)$.

因$\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right)$=1, 故$(x - x')$≡0$\left(\bmod \frac{m}{(a,m)}\right)$. 即

$$x \equiv x' \left(\bmod \frac{m}{(a,m)}\right).$$

也即$x \equiv x' + \frac{m}{(a,m)} t, t \in Z$.

一次同余方程-性质

虽然t的取值为任意整数, 但对于原方程

$$ax \equiv b \pmod{m},$$

在给定特解x'时, 不同的解应该为模m的不同剩余类. 上述全部解的表达式中, 当$t = 0,1,2, \dots, (a,m) - 1$时, x为模m的(a,m)个不同的剩余类. 例如, $t = 0$和$t = (a,m)$时是属于模m的同一个剩余类.

一次同余方程-求解步骤

故解同余方程$ax \equiv b \pmod{m}$的步骤如下:

(1) 判断方程是否有解. 即判断(a,m)是否整除b.

(2) 计算$\frac{\mathrm{a}}{(\mathrm{a,m})}x \equiv 1 \left(\mathrm{mod}\, \frac{\mathrm{m}}{(\mathrm{a,m})}\right)$的解. 运用欧几里德算法求解. 设求得的解为$x \equiv x_0 \left(\mathrm{mod}\, \frac{m}{(a,m)}\right)$.

(3) 写出方程$\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \left(\mathrm{mod}\, \frac{m}{(a,m)}\right)$的解为

$$x \equiv \frac{b}{(a,m)}x_0 \left(\mathrm{mod}\, \frac{m}{(a,m)}\right).$$

(4) 写出方程$ax \equiv b \pmod{m}$的全部解为

$$x \equiv \frac{b}{(a,m)}x_0 + \frac{m}{(a,m)}t (mod\, m), t = 0,1,2,\ldots,(a,m)-1.$$

一次同余方程-求解

可以看出, 先判断方程是否有解. 若有解, 就用欧几里德算法求得方程$\frac{\mathrm{a}}{(\mathrm{a},\mathrm{m})}x \equiv 1(\mathrm{mod}\,\frac{\mathrm{m}}{(\mathrm{a},\mathrm{m})})$的解. 然后可以先写出$\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)}(\mathrm{mod}\,\frac{m}{(a,m)})$的解再写出方程的全部解, 也可以直接写出方程的全部解.

一次同余方程-举例

【例3.1.7】 求解同余方程$45x \equiv 9 \pmod{84}$.

解: (1) 判断方程是否有解. (45, 84)=3|9, 同余方程有解.

(2) 计算$\frac{a}{(a,m)}x \equiv 1 (\bmod \frac{m}{(a,m)})$的解. 由【例3.1.5】知,

$15x \equiv 1 \pmod{28}$的解为$x \equiv 15 \pmod{28}$.

(3) 写出方程$\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} (\bmod \frac{m}{(a,m)})$的解, 同余方程

$15x \equiv 3 \pmod{28}$的解为$x \equiv 3 \times 15 \equiv 45 \equiv 17 \pmod{28}$.

(4) 写出方程$ax \equiv b \pmod{m}$的全部解.

$$x \equiv 17 + 28t \pmod{84}, t = 0, 1, 2.$$

一次同余方程-举例

【例3.1.8】 求解同余方程$69x \equiv 12 \pmod{111}$.

解: (1) 判断方程是否有解. (69, 111)=3|12, 同余方程有解.

(2) 计算$\frac{a}{(a,m)}x \equiv 1 \left(\bmod \frac{m}{(a,m)}\right)$的解. 代入相关参数得:

$$\frac{69}{(69,111)}x \equiv 1\left(\bmod \frac{111}{(69,111)}\right).$$

即$23x \equiv 1 \pmod{37}$.

用欧几里德算法求解过程如下:

一次同余方程-举例

$37 = 23 + 14,\qquad 23 = 14 + 9,\qquad 14 = 9 + 5,$
$9 = 5 + 4,\ \ 5 = 4 + 1.$

$$
\begin{aligned}
1 &= 5 - 4 = 5 - (9 - 5) = 5 \times 2 - 9 \\
&= (14 - 9)\ \times 2 - 9 = 14 \times 2 - 9 \times 3 \\
&= 14 \times 2 - (23 - 14) \times 3 = 14 \times 5 - 23 \times 3 \\
&= (37 - 23)\ \times 5 - 23 \times 3 = 37 \times 5 - 23 \times 8
\end{aligned}
$$

等式两端模37得 $1 \equiv 37 \times 5 - 23 \times 8 \pmod{37}.$
故$23x \equiv 1 \pmod{37}$ 的解为

$$x_0 \equiv x \equiv -8 \equiv 29 \pmod{37}.$$

一次同余方程-举例

(3)写出方程$ax \equiv b \pmod{m}$的全部解.

$x \equiv \frac{b}{(a,m)} x_0 + \frac{m}{(a,m)} t(mod\, m), t = 0,1,2, \dots, (a,m) - 1.$

代入相关参数得:

$$x \equiv \frac{12}{(69,111)} \times (-8) + \frac{111}{(69,111)} \mathrm{t} \pmod{111},$$
$$t = 0,1,2, \dots, (69,111) - 1.$$

即方程$69x \equiv 12 \pmod{111}$的全部解为

$$x \equiv 79 + 37t \pmod{111}, t = 0, 1, 2.$$

逆元

【定义3.1.2】 设$a \in Z, m \in N, (a,m)=1$, 则存在唯一的一个模$m$的剩余类, 类中任意元素$a'$,都使得$aa' \equiv 1 \pmod{m}$成立.

a'称为a的模m的逆元, 记为$a^{-1}\ (mod m)$,即

$$a \times a^{-1} \equiv 1 \pmod{m}.$$

由解一次同余方程的学习可知, 当m较小的时候, 可以用穷举的方式求a模m的逆元, 如【例3.1.1】-【例3.1.4】所示；当m较大时, 常采用欧几里德算法求解, 如【例3.1.7】所示.

作业-3