一次同余式解法的特点及其分析

李婷

（巴蜀中学，重庆 400013）

摘 要：主要对一次同余式的解法进行了初步的探讨，特别是对一次同余式的欧拉定理算法，欧几里德算法等七种解法进行了比较与分析。

关键词：同余式；一次同余式；模；解法

1 一次同余式

定义 1.1：同余式 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0 \pmod m$ 叫做一元 n 次同余式，其中 $m\nmid a_n, a_i\in Z, i=0,\cdots,n$，n 称为模 m 的次数。

注意 1：只有当 $m\nmid a_n$ 的时候，才称 n 为模 m 的次数。

如 $10x^7-25x^6+15x^4+2x^2-4\equiv 0 \pmod 5$ 是二次同余式。

定义 1.2：$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是一整系数多项式。若有一整数 c 可使 $f(c)\equiv 0 \pmod m$，则 c 叫做同余式 $f(x)\equiv 0 \pmod m$ 的根或解。若 a 能使 $f(a)\equiv 0 \pmod m$，而 $a\equiv b \pmod m$，则显然有 $f(b)\equiv 0 \pmod m$，两个关于模 m 不同余的解叫做不相同的解。

注意 2：若 a 为 $f(x)\equiv 0 \pmod m$ 的解，则 km+a 也是 $f(x)\equiv 0 \pmod m$ 的解。即 $f(km+a)\equiv 0 \pmod m$ 故称为 $f(x)\equiv 0 \pmod m$ 的一个解。

2 一次同余式 $ax\equiv b \pmod m$ 的解法

代数学中的一个主要问题是研究代数方程的解，而在数论中提供的问题是研究同余式的解。我们注意到同余方程 $ax\equiv b \pmod m$ 解的特征有两个，首先是只需数 m 的完全剩余系 0,1…m-1 中寻求方程的解；其次，与代数线性方程 ax=b 不同，同余方程 $ax\equiv b \pmod m$ 可以无解，有一个解或者多个解。如 $2x\equiv 1 \pmod 4$ 无解，而 $2x\equiv 1 \pmod 3$ 有一个解，而 $2x\equiv 4 \pmod 6$ 有两个解 $x\equiv 2, x\equiv 5$。

那么，究竟同余方程 $ax\equiv b \pmod m$ 何时有解？有几个同余类适合此方程？

定理 1.1.1：若 $(a,m)=1$，则 $ax\equiv b \pmod m$ 有唯一解。

定理 1.1.2：若 $(a,m)=d, d\nmid b$，则 $ax\equiv b \pmod m$ 没有解。

定理 1.1.3：若 $(a,m)=d, d\mid b$，则 $ax\equiv b \pmod m$ 有 d 个解。

有以上三个定理我们可以容易的判断出一次同余式解的存在性及不同解的个数，以下将分 $(a,m)=1$ 和 $(a,m)=d>1$ 两种情形探讨一次同余式的解法及其比较。

首先，当 $(a,m)=1$ 时，同余式 $ax\equiv b \pmod m$ 有以下七种解法：

2.1 观察法解一次同余式

在模 m 的完全剩余系 0,1,…m-1 中考虑同余式的解。易知，当模 m 较小时，可以利用观察法或方程具有特殊形式时，可以用观察法直接快速的得出方程的解。如前面举的例子 $2x\equiv 1 \pmod 3$ 等等。

在系数较大的情况下，可利用同余性质，将同余式系数减小而且有带余除法定理，可保证系数在一个固定范围内作为模 m 的余数，进而用观察法可快速得出方程的解。

2.2 欧拉定理算法

由欧拉定理有 $a^{\phi(m)}=1 \pmod m$，而 $ax=b \pmod m$，可得 $a^{\phi(m)}\equiv b\cdot a^{\phi(m)-1} \pmod m$ 即得：$x\equiv b\cdot a^{\phi(m)-1} \pmod m$ 为所求之解。

例：解 $8x\equiv 9 \pmod{11}$

解 $\phi(11)=10, 8^{10}x\equiv 8^9\cdot 9\equiv(-2)\cdot(-3)^9\equiv 6\cdot 9^4\equiv 6\cdot(-2)^4\equiv 6\cdot 2^4\equiv 6\cdot 5\equiv 8 \pmod{11}$

此方法给出了一次同余式的一个公式解。这种解法在理论上较易分析，但当模 m 较大时，求 $\phi(m)$ 便要涉及到 m 的标准分解，较复杂，不宜进行计算机编程计算。所以这种解法更适合 m 较小时，或 $\phi(m)$ 较易求解时用。

2.3 化为不定方程的解法

$ax\equiv b \pmod m$ 有解⇔存在整数 x,y，使得 $ax-b=my$。即不定方程 $ax-my=b$ 有解。于是同余式可转化为不定方程求解。

例：解 $8x\equiv 9 \pmod{11}$

解：原方程对应的不定方程为 $8u-11v=9$，其通解为（对任意整数 t）

$u=8+11tv=5+8t$

所以 $x\equiv 8 \pmod{11}$

这种解法对模 m 的要求较低而且易于利用计算机编程来求解一次同余式。

2.4 减少模数的解法

对于 $ax+b\equiv 0 \pmod m$ （1）$0<a, b<m\Rightarrow ax+b=my\Rightarrow my\equiv b \pmod a$ （2）

此时 a<m，然后去掉 m=ka+c，b=pa+d 中 a 的倍数。

$\Rightarrow cy\equiv d \pmod a$ 不断将模变小，此时，若（2）有解 y_0，则 $x_0=\frac{my_0-b}{a}$ 为（1）的解。而（2）中模数显然比 m 小，经过几次转换后一般可以用观察法求解，再递推出原方程的解。

例：求解同余式 $325x\equiv 20 \pmod{161}$

解 原同余式既是：$3x\equiv 20 \pmod{161}$，

解同余式：$161x\equiv -20 \pmod 3$，

$2y\equiv 1 \pmod 3$ 得：$y\equiv \pmod 3$，

所以原同余式的解是：$x\equiv\frac{20+2\times 161}{3}\equiv 114 \pmod{161}$。

这种解法的优点在于将大模化为小模，从而减少计算量。所以此方法适合于模数较大时。

2.5 欧几里德算法

$(a,m)=1$ 时，可借用辗转相除法求整数的最大公因数的方法，结合同余式的性质，可转化为一个形如 $x\equiv r \pmod m$ 的同解方程，达到求解目的。即当 m>a 时，利用恒等变形将 a 变小，直至将 x 的系数变为 1。

例：解 $103x\equiv 57 \pmod{211}$

解 因为 $(103,211)=1$，故方程有唯一解，而 211=2×103+5，于是

$2\times 103x\equiv 114x \pmod{211}$ ①

且 $211x\equiv 0 \pmod{211}$ ②

由 $x\equiv 0 \pmod{211}$ ②-①可得：$5x\equiv -114\equiv 97 \pmod{211}$ ③

又 211=42 5+1

而 $42\times 5x\equiv 42\times 97\equiv 65 \pmod{211}$ ④

由②-④得：$x\equiv -65\equiv 46 \pmod{211}$

2.6 分式法

先把 $ax\equiv b \pmod m$ 写成 $x\equiv\frac{b}{a} \pmod m$ 的形式，（这里 $\frac{b}{a}$ 只是一种形式上的写法）然后用与 m 互素的数陆续的乘右端的分子和分母，目的在于把分母的绝对值变小，直到变成 1 为止。

例：解同余式 $37x\equiv 25 \pmod{107}$

解 因为 $(37,107)=1$，则方程有唯一解为：

$$x\equiv\frac{25}{37}\equiv\frac{25\times 3}{37\times 3}\equiv\frac{75}{111}\equiv\frac{75-107}{111-107}\equiv\frac{-32}{4}\equiv -8\equiv 99 \pmod{107}$$

这种方法给出了一次同余式的一种形式解，较直观。但这种解法只适合于模 m 不太大，如三位数或三位以内的时候较方便。这种解法其实与解法 1.1.5 形异实同。

但这里特别应注意的是：

2.6.1 此处的“分数”$\frac{b}{a}$ 仅仅是一个形式符号，不能当一般的分数一样进行运算。

2.6.2 对 $\frac{b}{a}$ 的“分子”，“分母”乘以不为零的整数或约去一个与模 m 互素的数，否则所得出的结果可能不是原同余式的解。

2.7 威尔逊定理解法

$ax\equiv b \pmod p$，$(a,p)=1, 0<a<p$，p 为素数。由威尔逊定理有：$ax\equiv -b(p-1)! \pmod p\Rightarrow x\equiv -\frac{(p-1)!}{a}\cdot b \pmod p$ 和欧拉定理解法一样，此种解法也是给出了一次同余式的一组公式解，但此时要求模为素数且模不能太大，否则计算阶乘将较麻烦。

其次：当 $(a,m)=d>1$ 时，利用定理 1.1.2，1.1.3 及以上几种解法易求同余式的解。

对于多元一次同余式，可将其转化为一元一次同余式来求解。

参考文献

[1]李复中.初等数论选讲[M].长春：东北师范大学出版社，1984，12：93-112.

[2]华罗庚.数论导引[M].北京：科学出版社，1979：32-39.

[3]柯召，孙琦.数论讲义[M].北京：高等教育出版社，1986，4：115-122.

[4]熊全淹.初等整数论[M].武汉：湖北人民出版社，1982，6：88-138.

责任编辑：程鹏