POJ 1006 详细推导过程

张帅

2010 年 7 月 12 日

目录

1 题目描述

求解同余方程组：

$$x \equiv p \mod 23 \tag{1}$$

$$x \equiv e \mod 28 \tag{2}$$

$$x \equiv i \mod 33 \tag{3}$$

其中 p、 e 和 i 均为常数

求解最小的正整数 x。(所有的整数解 x 均关于 21252 同余)

2 推导过程

解 由(1)和同余的定义可以得到

$$x = p + 23 \cdot r_1 \quad (\text{其中 } r_1 \text{ 是常数}) \tag{4}$$

将(4)代入(2)中，得到：

$$p + 23 \cdot r_1 \equiv e \mod 28$$

经过变换可以得到：

$$23 \cdot r_1 \equiv e - p \mod 28$$

由同于的定义得到：

$$23 \cdot r_1 + 28 \cdot s_1 = e - p \tag{5}$$

由扩展欧几里得算法[1]可知，存在这样的 $r_1^{'}$ 和 $s_1^{'}$ 使得

$$23 \cdot r_1^{'} + 28 \cdot s_1^{'} = \gcd(23, 28) = 1 \tag{6}$$

成立。

(6)的一组特解为：

$$\begin{cases} r_1^{'} = -17 \\ s_1^{'} = 14 \end{cases}$$

由贝祖定理[2]可知，(6)的通解为：

$$\begin{cases} r_1^{'} = -17 + \dfrac{28}{\gcd(23, 28)} \cdot t_1 = -17 + 28 \cdot t_1 & (7) \\ s_1^{'} = 14 - \dfrac{23}{\gcd(23, 28)} \cdot t_1 = 14 - 23 \cdot t_1 & (8) \end{cases}$$

将(6)左右两边同时乘以 $(e - p)$ 得到：

$$23 \cdot (e - p) \cdot r_1^{'} + 28 \cdot (e - p) \cdot s_1^{'} = e - p \tag{9}$$

使用

$$\begin{cases} r_1 = (e - p) \cdot r_1^{'} & (10) \\ s_1 = (e - p) \cdot s_1^{'} & (11) \end{cases}$$

[1] http://en.wikipedia.org/wiki/Extended_Euclidean_algorithm

[2] http://en.wikipedia.org/wiki/B%C3%A9zout's_identity

可以将(9)变换为同(5)相同的形式。

将方程(6)的通解(7)代入方程(10)后再取模 *28*:

$$r_1 = (e-p)\cdot(-17) + (e-p)\cdot 28\cdot t_1 \equiv -17\cdot(e-p) \mod 28 \tag{12}$$

根据同余定义可以从方程(12)得到:

$$r_1 = 28\cdot r_2 + 17\cdot(p-e) \tag{13}$$

将方程(13)代入到方程(4)中:

$$\begin{aligned} x &= p + 23\cdot[28\cdot r_2 + 17\cdot(p-e)] \\ &= 644\cdot r_2 + 392\cdot p - 391\cdot e \end{aligned} \tag{14}$$

将方程(14)代入到(3)中，并将常数项移到右边，得到:

$$644\cdot r_2 \equiv -392\cdot p + 391\cdot e + i \mod 33 \tag{15}$$

在这里已经将三个方程的线性同余方程组转换为了两个方程的线性同余方程组，继续重复上面的过程。

根据同余的定义，从(15)可以得到:

$$r_2 = 33\cdot r_3 - 784\cdot p + 782\cdot e + 2\cdot i \tag{16}$$

将(16)代入(14)中，可以得到:

$$\begin{aligned} x &= 644\cdot(33\cdot r_3 - 784\cdot p + 782\cdot e + 2\cdot i) + 392\cdot p - 391\cdot e \\ &= 21252\cdot r_3 - 504504\cdot p + 503217\cdot e + 1288\cdot i \end{aligned} \tag{17}$$

将(17)模 *21252*:

$$\begin{aligned} x &\equiv (-504504)\cdot p + 503217\cdot e + 1288\cdot i && \mod 21252 \\ &\equiv ((-504504)\cdot p + 24\times 21252p) \\ &\quad + (503217e - 23\times 21252e) + 1288i && \mod 21252 \\ &\equiv 5544p + 14421e + 1288i && \mod 21252 \end{aligned} \tag{18}$$

由(18)和同余的定义可知:

$$x = \{21252r_0 + 5544p + 14421e + 1288i \mid r_0 \in \mathbb{Z}\} \tag{19}$$

3 参考资料

- 维基百科 Linear congruence theorem(大概译作线性同余理论)
- 维基百科 Chinese remainder theorem(中国剩余定理)
- 维基百科 Extended Euclidean algorithm(扩展欧几里德定理)
- 维基百科 Bézout's identity(贝祖定理)
- Jianing Yang 关于 POJ1006 的分析
- 我对于 POJ1006 的分析
- 我的博客:)