Centro Federal de Educação Tecnológica de Minas Gerais

Engenharia de Computação

- AED -

Algoritmos e estruturas de dados

André Neves

Leonam

Novembro de 2018

Sumário

1 Apresentação do problema

O problema apresenta um contexto onde um empregado, por exigência de seu senhor, passa a apresentar relatórios sobre realização de suas tarefas. Cada relatório indica a hora em que ele começou e parou de trabalhar, e a quantidade de vezes que realizou cada tarefa. O Senhor anda desconfiado da autenticidade do relatório apresentado.

O empregado sempre trabalha apenas nas P primeiras horas do dia, que significa período de trabalho, citado no início do caso de teste. Isso significa que se por exemplo, $P = 10$, ele trabalhará de 0 às 9 horas.

Cada caso de teste refere-se à entrega de n relatórios, que reportam sobre a execução de n tarefas. O empregado não informou a data de inicio e fim dos relatórios, mas apenas a hora. Isso significa que ele pode ter começado e terminado em qualquer dia.

Suponha que as horas de início e fim sejam respectivamente 0 e 3, e mantenha o valor de período P igual a 10. Com isso ele pode ter trabalhado apenas entre 0 e 3 horas no primeiro dia, ou entre 0 e 9 horas no primeiro dia e entre 0 e 3 horas no segundo dia, com a possibilidade de extender a qualquer quantidade de dias.

Ou seja, em cada dia ele trabalha entre 0 e P - 1 horas, com exceção no primeiro e último dia, os quais os limites são as horas de início e fim reportadas no relatório, respectivamente.

2 Modelagem das equações de congruência

Ao tomar o exemplo anterior, o empregado teria infinitas possibilidades de cronogramas de trabalho, já que não informou as datas de início e fim. De acordo com o exemplo citado acima, seriam algumas possibilidades:

Dia trabalhado	**Período de trabalho**	**Total**
1º	de 0h às 3h	4h

Tabela 1: 1ª possibilidade

Dia trabalhado	**Período de trabalho**	**Total**
1º	de 0h às 9h	10h
2º	de 0h às 3h	4h

Tabela 2: 2ª possibilidade

Dia trabalhado	Período de trabalho	Total
1º	de 0h às 9h	10h
2º	de 0h às 9h	10h
3º	de 0h às 3h	4h

Tabela 3: 3ª possibilidade

Dia trabalhado	Período de trabalho	Total
1º	de 0h às 9h	10h
2º	de 0h às 9h	10h
3º	de 0h às 9h	10h
4º	de 0h às 3h	4h

Tabela 4: 4ª possibilidade

É possível perceber o padrão onde a quantidade total de horas trabalhadas, independente da possibilidade, é igual a:

$$t \cdot 10 + 4$$

Para qualquer $t \in \mathbb{N}$, onde $t + 1$ representa a quantidade de dias trabalhados.

3 Modelagem do sistema de congruências lineares

Segundo a descrição do problema, são informados n relatórios de n tarefas. Cada i-ésimo relatório possui as informações S_i, T_i, $A_{i,1}$, $A_{i,2}$, ..., $A_{i,n}$, que referem-se respectivamente à hora de início, fim, e a quantidade de vezes que foram realizadas as tarefas 1, 2, 3, ..., n.

Seja C_i a contabilidade do tempo total gasto para realizar as tarefas referentes ao i-ésimo relatório. Baseado nos valores de S_i e T_i, conforme a seção 2, temos:

$$C_i = t \cdot P + (T_i - S_i + 1) \tag{1}$$

Para qualquer $t \in \mathbb{N}$.

Seja D_1, D_2, ..., D_n o tempo de duração de cada tarefa. Baseado nisso e no relatório, C_i possui também a seguinte definição:

$$C_i = A_{i,1} \cdot D_1 + A_{i,2} \cdot D_2 + \cdots + A_{i,n} \cdot D_n \tag{2}$$

E baseado nas equações 1 e 2, temos que:

$$A_{i,1} \cdot D_1 + A_{i,2} \cdot D_2 + \cdots + A_{i,n} \cdot D_n = t \cdot P + (T_i - S_i + 1) \tag{3}$$

Para qualquer $t \in \mathbb{N}$.

Isso remete à definição de congruência modular. Dois números a e b são congruêntes com módulo P se a diferença entre eles for múltiplo de P. Ou seja, se para qualquer $t \in \mathbb{R}$, $a - b = t \cdot P$. Ou seja:

$$a \equiv b \pmod{P} \quad \Leftrightarrow \quad a - b = t \cdot P \tag{4}$$

Para qualquer $t \in \mathbb{N}$.

Com base na definição 4, a informação do i-ésimo relatório pode ser representada pela equação 5:

$$A_{i,1} \cdot D_1 + A_{i,2} \cdot D_2 + \cdots + A_{i,n} \cdot D_n \equiv (T_i - S_i + 1) \pmod{P} \tag{5}$$

Ao combinar as informações de todos os n relatórios, temos o sistema de congruências lineares 6:

$$\begin{cases} A_{1,1} \cdot D_1 + A_{1,2} \cdot D_2 + \cdots + A_{1,n} \cdot D_n \equiv (T_1 - S_1 + 1) \pmod{P} \\ A_{2,1} \cdot D_1 + A_{2,2} \cdot D_2 + \cdots + A_{2,n} \cdot D_n \equiv (T_2 - S_2 + 1) \pmod{P} \\ \vdots \\ A_{n,1} \cdot D_1 + A_{n,2} \cdot D_2 + \cdots + A_{n,n} \cdot D_n \equiv (T_n - S_n + 1) \pmod{P} \end{cases} \tag{6}$$

Que pode ser representado na forma matricial:

$$\begin{bmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,n} \\ A_{2,1} & A_{2,2} & \dots & A_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n,1} & A_{n,2} & \dots & A_{n,n} \end{bmatrix} \begin{bmatrix} D_1 \\ D_2 \\ \vdots \\ D_n \end{bmatrix} = \begin{bmatrix} T_1 - S_1 + 1 \\ T_2 - S_2 + 1 \\ \vdots \\ T_n - S_n + 1 \end{bmatrix} \pmod{P} \tag{7}$$

Segundo a teoria dos números e da aritmética modular, um sistema de congruências lineares relativas a um número primo pode ser resolvido com os métodos usuais da álgebra linear, como inversão de matriz, regra de Cramer ou redução de Gauss Jordan, também conhecido como

escalonamento.

Isso pode ser explicado pelo fato de que toda a álgebra linear pode ser aplicadas sobre corpos, ao invés de apenas sobre números reais. Um sistema de congruências lineares com módulo em um número primo mantém as propriedades de corpo se for respeitado os requisitos de utilização de adição e multiplicação acompanhados da operação mod P, além do inverso multiplicativo.

4 Resolução de sistemas de equações com Eliminação de Gauss-Jordan ou escalonamento

Um sistema linear pode ser substituído por outro que seja simplificado e ainda tenha o mesmo conjunto solução do primeiro, que é obtido pela aplicação de uma série de **operações elementares**, que são:

1. Trocar duas equações de posição.
2. Substituir uma equação pela mesma multiplicada por um escalar diferente de 0.
3. Substituir uma equação pela mesma somada a outra que tenha sido multiplicada por um escalar.

Seja o seguinte sistema linear:

$$\begin{cases} a_{1,1} \cdot x_1 + a_{1,2} \cdot x_2 + \cdots + a_{1,n} \cdot x_n = b_1 \\ a_{2,1} \cdot x_1 + a_{2,2} \cdot x_2 + \cdots + a_{2,n} \cdot x_n = b_2 \\ \vdots \\ a_{n,1} \cdot x_1 + a_{n,2} \cdot x_2 + \cdots + a_{n,n} \cdot x_n = b_n \end{cases} \tag{8}$$

O sistema linear 8 pode também ser representado pela forma matricial compacta:

$$\left[\begin{array}{cccc|c} a_{1,1} & a_{1,2} & \dots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} & b_n \end{array}\right] \tag{9}$$

As **operações elementares** citadas anteriormente podem ser aplicadas à matriz 9 do sistema 8. Nesse caso as orientações são: . Trocar duas linhas da matriz de posição. 2. Substituir uma linha da matriz pela mesma linha multiplicada por um escalar diferente de 0. 3. Substituir uma linha da matriz pela mesma linha somada a um multiplo escalar de outra linha

1. Trocar duas linhas de posição.

2. Substituir uma linha pela mesma multiplicada por um escalar diferente de 0.

3. Substituir uma linha pela mesma somada a outra que tenha sido multiplicada por um escalar.

O método de Gauss-Jordan consiste em aplicar operações elementares à matriz de um sistema, até que esteja na forma **escalonada reduzida**.

Definição: Pivô é o primeiro elemento não-nulo de cada linha.

Definição: Inverso multiplicativo de a é um número b tal que $a \cdot b = 1$.

4.1 Triangulação inferior da matriz do sistema

O algoritmo descrito aqui será focado em triangular inferiormente a matriz do sistema, de forma que todas as células abaixo da diagonal principal sejam iguais a zero. Será baseado nos seguintes passos:

1. Linha atual a é a primeira linha.

2. Para a linha atual a, encontrar o pivô e chamá-lo de p.

3. Para cada linha b seguinte:

   (a) Calcular o fator de multiplicação f, que é o inverso multiplicativo do pivô vezes o número da linha b pertencente à mesma coluna do pivô.

   (b) Substituir a linha b por $(f \cdot a - b)$, ou seja, a linha b será igual a f multiplicado pela linha a menos a linha b

4. Repetir o item 2 para a linha seguinte.

Após a execução dos passos citados acima, todos elementos abaixo da diagonal principal serão iguais a 0, o que torna a matriz mais simplificada. O conjunto solução não foi alterado pois foram aplicadas apenas operações elementares.

Exemplo: Triangular a matriz do sistema linear abaixo:

$$\begin{cases} 5x + 5y & = 15 \\ 2x + 4y + z & = 10 \\ 3x + 4y & = 11 \end{cases}$$

A matriz correspondente é:

$$\left[\begin{array}{ccc|c} 5 & 5 & 0 & 15 \\ 2 & 4 & 1 & 10 \\ 3 & 4 & 0 & 11 \end{array}\right] \tag{10}$$

Segue a sequência de operações:

$a = 1,\ p = 5$
$b = 2,\ f = \frac{2}{5}$
$L_2 = \frac{2}{5} \cdot L_1 - L_2$

$$\left[\begin{array}{ccc|c} 5 & 5 & 0 & 15 \\ 0 & -2 & -1 & -4 \\ 3 & 4 & 0 & 11 \end{array}\right] \tag{11}$$

$a = 1,\ p = 5$
$b = 3,\ f = \frac{3}{5}$
$L_3 = \frac{3}{5} \cdot L_1 - L_3$

$$\left[\begin{array}{ccc|c} 5 & 5 & 0 & 15 \\ 0 & -2 & -1 & -4 \\ 0 & -1 & 0 & -2 \end{array}\right] \tag{12}$$

$a = 2,\ p = -2$
$b = 3,\ f = \frac{1}{2}$
$L_3 = \frac{1}{2} \cdot L_2 - L_3$

$$\left[\begin{array}{ccc|c} 5 & 5 & 0 & 15 \\ 0 & -2 & -1 & -4 \\ 0 & 0 & -\frac{1}{2} & 0 \end{array}\right] \tag{13}$$

Caso o processo de triangulação resultar em uma matriz que tenha uma linha nula, o sistema não tem solução trivial, e com isso existem infinitos conjuntos de solução (Sistema impossível indeterminado), exemplo:

$$\left[\begin{array}{ccc|c} 5 & 5 & 0 & 15 \\ 0 & -2 & -1 & -4 \\ 0 & 0 & 0 & 0 \end{array}\right] \tag{14}$$

Caso o processo de triangulação resultar em uma matriz que tenha uma linha cujo todos os coeficientes de variáveis são nulos, mas o coeficiente independente não, o sistema é inconsistente e não tem nenhuma solução válida (Sistema impossível), exemplo:

4.2 Tringulação superior da matriz do sistema / determinação do valor de cada variável

Após a obtenção da matriz 14, é mais simples a determinação do valor de cada variável. Os seguintes passos podem ser seguidos:

1. Começar a trabalhar na última linha
2. Para as células da linha que são diferentes de zero e que o valor da variável já foi determinado, multiplique o coeficiente pela variável correspondende.
3. Subtrair da última coluna, na mesma linha, o valor obtido no item 2.
4. Multiplicar o valor obtido no item anterior pelo inverso do coeficiente da variável x_i, que está indeterminada. Esse é o valor da variável x_i
5. Repetir o passo 2 para a linha anterior.

Veja a realização desse procedimento para a matriz 14:

$$\left[\begin{array}{ccc|c} 5 & 5 & 0 & 15 \\ 0 & -2 & -1 & -4 \\ 0 & 0 & -\frac{1}{2} & 0 \end{array}\right] \tag{15}$$

- Linha 3:
  - Começar da linha 3 (Determinar variável z). Todos os coeficientes de variáveis são zero, exceto o de z.
  - Valor de $z = 0 \cdot (-\frac{1}{2})^{-1} = 0$ (Zero vezes o inverso do coeficiente da variável z
- Linha 2:
  - Ir para a linha 2 (Determinar variável y). Multiplicar o coeficiente da variável z (terceira coluna), pelo valor de z: $s = -1 \cdot 0 = 0$.
  - Subtrair o valor obtido anteriormente de -4: $s = -4 - 0 = -4$.
  - Multiplicar o valor obtido anteriomente pelo inverso de -2 (Coeficiente da variável y na linha 2). O resultado é o valor de $y = -4 \cdot (-2)^{-1} = 2$

- Linha 1:
  - Nesse ponto, os valores de y e z já foram determinados (colunas 2 e 3).
  - Deve-se multiplicar os coeficientes pelos valores das respectivas variáveis y e z: $s = 2 \cdot 5 + 0 \cdot 0 = 10$.
  - Subtrair de 15 (valor da última coluna), o resultado obtido anteriormente: $s = 15 - 10 = 5$.
  - Multiplicar o resultado anterior pelo inverso de 5 (Coeficiente da variável x). O resultado é o valor de $x = 5 \cdot (5)^{-1} = 1$

Com esses passos foram definidos os valores para x, y e z:

$$\begin{cases} x &= 1 \\ y &= 2 \\ z &= 0 \end{cases}$$

4.3 Resolução de sistemas de congruências lineares

4.3.1 Fundamentação teórica

Definição: Elemento neutro é o elemento de um conjunto que não altera o valor de uma soma. No conjunto dos reais, corresponde ao número 0.

Definição: Inverso multiplicativo modular de a módulo P é um número b tal que $(a \cdot b)$ mod P = 1.

Como citado na seção 3, um sistema de congruencias lineares tem a seguinte forma:

$$\begin{cases} A_{1,1} \cdot D_1 + A_{1,2} \cdot D_2 + \cdots + A_{1,n} \cdot D_n \equiv B_1 \pmod{P} \\ A_{2,1} \cdot D_1 + A_{2,2} \cdot D_2 + \cdots + A_{2,n} \cdot D_n \equiv B_2 \pmod{P} \\ \vdots \\ A_{n,1} \cdot D_1 + A_{n,2} \cdot D_2 + \cdots + A_{n,n} \cdot D_n \equiv B_n \pmod{P} \end{cases} \tag{16}$$

Todos os passos vistos na seção 4 podem ser aplicados a qualquer sistema de equações definido fora dos conjuntos dos reais ($\mathbb{R}$), contanto que este mantenha as propriedades de corpo, que consiste em basicamente:

- Todo elemento que não seja o elemento neutro possui um **inverso multiplicativo** (seção 4).

- A multiplicação $m = a \cdot b$ é igual ao elemento neutro apenas se a ou b também correspondem ao elemento neutro do conjunto. O cálculo $[(2 \cdot 4) \bmod 8]$ resulta em zero, ainda que nem um dos elementos da multiplicação 2 e 4 sejam iguais a zero. Isso mostra que o conjunto das congruências de módulo 8 não é um corpo.

O segundo item permite demonstrar que um conjunto de congruências só é um corpo se for em relação ao módulo de um número primo. Com isso, para resolver o sistema de congruências lineares 16 com o método apresentado na seção 4 é necessário que P seja um número primo, o que é garantido pelo enunciado do problema.

A diferença de procedimento nesse caso são as seguintes modificações nas operações:

- **Soma:** A soma de dois números a e b deve ser seguida da operação mod P. Com isso, $S = (a + b) \bmod P$.
- **Multiplicação:** A multiplicação de dois números a e b deve ser seguida da operação mod P. Com isso, $S = (a \cdot b) \bmod P$.
- **Subtração:** A subtração de dois números a e b deve ser seguida da soma do número P e da operação mod P. Com isso, $S = (a - b + P) \bmod P$.
- **Divisão:** A divisão de um número a por b deve ser substituida pela multiplicação de a pelo inverso multiplicativo modular (seção 4.3.1) de b com relação ao módulo de P, seguida da operação mod P. Com isso, $S = (a \cdot b^{-1}) \bmod P$, onde b^{-1} é o inverso multiplicativo modular de b.

4.3.2 Exemplo

Seja o seguinte sistema de congruências lineares:

$$\begin{bmatrix} 5 & 0 & 0 \\ 0 & 0 & 1 \\ 3 & 2 & 2 \end{bmatrix} \begin{bmatrix} D_1 \\ D_2 \\ D_3 \end{bmatrix} = \begin{bmatrix} 5 \\ 4 \\ 23 \end{bmatrix} \pmod{23} \tag{17}$$

Na forma matricial compacta:

$$\left[\begin{array}{ccc|c} 5 & 0 & 0 & 5 \\ 0 & 0 & 1 & 4 \\ 3 & 2 & 2 & 23 \end{array}\right] \pmod{23} \tag{18}$$

Seja os inversos multiplicativos modulares de módulo 23 dos seguintes números:

n	n^{-1} **mod** 23
1	1
5	14
21	11

A sequência de operações na matriz é:

$a = 1$, $p = 5$
$b = 3$, $f = 3 \cdot 5^{-1} = 3 \cdot 14 = 42$
$L_3 = ((42 \cdot L_1) \bmod 23 - L_3 + 23) \bmod 23$

$$\left[\begin{array}{ccc|c} 5 & 0 & 0 & 5 \\ 0 & 0 & 1 & 4 \\ 0 & 21 & 21 & 3 \end{array}\right] \pmod{23} \tag{19}$$

Inverter linhas 2 e 3:

$$\left[\begin{array}{ccc|c} 5 & 0 & 0 & 5 \\ 0 & 21 & 21 & 3 \\ 0 & 0 & 1 & 4 \end{array}\right] \pmod{23} \tag{20}$$

Com a matriz triangulada inferiormente, determinar os valores de D_1, D_2 e D_3:

Determinação de D_3 (linha 3):
$D_3 = 4 * 1^{-1} \bmod 23 = 4$

Determinação de D_2 (linha 2):
$21 \cdot 4 \bmod 23 = 15$
$(3 - 15 + 23) \bmod 23 = 11$
$D_2 = 11 \cdot 21^{-1} \bmod 23 = 11 \cdot 11 \bmod 23 = 6$

Determinação de D_1 (linha 1):
$D_1 = 5 \cdot 5^{-1} \bmod 23 = 5 \cdot 14 \bmod 23 = 1$

Com isso, o conjunto solução é:

$$\begin{cases} D_1 & = 1 \\ D_2 & = 6 \\ D_3 & = 4 \end{cases}$$

Esse é o resultado esperado pelo algoritmo desse problema. As condições citadas na seção 4 quanto ao sistema ser impossível ou possível indeterminado vale também para um sistema de congruências lineares.

Referências

[1] Bruce Ikenaga, 2015. **Systems of Congruences**. Disponível em: [http://sites.millersville.edu/bikenaga/number-theory/systems-of-congruences/systems-of-congruences.html] Acesso em 26 de Novembro de 2018.

[2] Rodney Josué Biezuner. **Sistemas Lineares**. Disponível em: [http://www.mat.ufmg.br/~rodney/notas_de_aula/sistemas_lineares.pdf] Acesso em 26 de Novembro de 2018.

[3] Marathoncode, 2012. **Inverso Multiplicativo**. Disponível em: [http://marathoncode.blogspot.com/2012/04/inverso-multiplicativo.html] Acesso em 26 de Novembro de 2018.