Relatório Tp5

Diana Magalhães A81545
Raquel Gonçalves A79906

Primeira Parte

Nesta primeira parte resolveu-se os sistemas de congruências modulares a) e b).

a)

$$\begin{cases} x \equiv 48 \pmod{13} \\ x \equiv 57 \pmod{23} \\ x \equiv 39 \pmod{27} \end{cases}$$

Como o máximo divisor comum de 13, 23 e 27 é 1, podemos, então, para resolução deste sistema de congruências modulares, utilizar o **Teorema Chinês do Resto**.

Para a aplicação do teorema consideramos:

$N = 13 \times 23 \times 17 = 8073$

$N1 = 23 \times 27 \times 27 = 621$

$N2 = 13 \times 27 = 351$

$N3 = 13 \times 23 = 299$

De seguida calculamos as seguintes congruências:

(1): $621y1 \equiv 1 \pmod{13}$

(2): $351y2 \equiv 1 \pmod{23}$

(3): $299y3 \equiv 1 \pmod{27}$

Começando pela primeira congruência, ao dividir 621 por 11, podemos escrever a congruência (1) da seguinte forma:

$(13 \times 47 + 10)y1 \equiv 1 \pmod{13}$

Como (13×47) é congruente a 0 (mod13) , desprezamos essa parte. Assim sendo, podemos simplificar a congruência (1):

$10y1 \equiv 1 \pmod{13}$

Para se verificar esta conrguência o $y1 = 4$, de tal forma que:

$40 \equiv 1 \pmod{13}$

Podemos então verificar que $40 \div 13 = 3$ com resto 1.

Para a segunda congruencia utlizamos o mesmo pensamento, inicialmente decompusemos 351, dividindo por 23, obtendo-se o seguinte:

$(23 \times 15 + 6)y2 \equiv 1 \pmod{23}$

Como $(23 \times 15) \equiv 0 \pmod{23}$, desprezamos essa parte, ficando da seguinte forma:

$6y2 \equiv 1 \pmod{23}$

De forma a que a congruência apresentada em cima se verifique, $y2 = 4$.

Por fim, para a congruencia (3), decompusemos 299, dividindo por 27:

$(27 \times 11 + 2)y3 \equiv 1 \pmod{27}$

Desprezou-se (27×11), ficando assim da seguinte forma:

$2y3 \equiv 1 \pmod{27}$

Para que este caso se verifique, $y3 = 14$.

A solução deste sistema vai ser:

$x = 621 \times 48 \times 4 + 351 \times 57 \times 4 + 299 \times 39 \times 14 = 362514$

Como 362514 (mod8073) é 7302, podemos escrever o resultado da seguinte forma:

$x = 7302 + 8073n$

Para $n = 0$, obtemos a menos solução do sistema $x = 7302$.

b)

Nesta alínea, primeiro simplificamos as seguintes congruências de maneira a remover os coeficientes:

$$\begin{cases} 19x \equiv 21 \pmod{16} \\ 37x \equiv 100 \pmod{15} \end{cases}$$

Como a inversa multiplicativa modulo 16 de 19 é 11, podemos simplificar a primeira congurência da seguinte forma:

$19x \times 11 \equiv 21 \times 11 \pmod{16}$

$x \equiv 231 \pmod{16}$

$x \equiv 7 \pmod{16}$

Como a inversa multiplicativa modulo 15 de 37 é 13, podemos simplificar a segunda congruência da seguinte forma:

$37x \times 13 \equiv 100 \times 13 \pmod{15}$

$x \equiv 1300 \pmod{15}$

$x \equiv 10 \pmod{15}$

Através desta simplificação obteu-se o seguinte sistema:

$$\begin{cases} x \equiv 7 \pmod{16} \\ x \equiv 10 \pmod{15} \end{cases}$$

Para a resolução deste sistema utilizou-se o mesmo procedimento apresentado na alĩnea a). Posto isto, consedirou-se:

$N = 16 \times 15 = 240$

$N1 = 15$

$N2 = 16$

Calculou-se as seguintes congruências:

(1): $15y1 \equiv 1 \pmod{16}$

(2): $16y2 \equiv 1 \pmod{15}$

Para a congruência (1), ao dividir 15 poe 16, obtemos um resto de 15 logo não se altera esta congurenência.

Deste modo, para que ela se verifique o $y1 = 15$, pois:

$225 \equiv 1 \pmod{16}$

Para a segunda congruência, ao dividir 16 por 15, obtemos um resto igual 1. Sendo assim, podemos simplificar a expressão:

$y2 \equiv 1 \pmod{15}$

Para que esta expressão se verifique o $y2 = 16$.

A solução deste sistema vai ser:

$x = 15 \times 7 \times 15 + 16 \times 10 \times 16 = 4135$

Como 4135 (mod240) é 55, podemos escrever o resultado da seguinte forma:

$x = 55 + 240n$

Para $n = 0$, obtemos a menos solução do sistema $x = 55$.

Segunda Parte

Nesta segunda parte teve como objetivo decifrar uma cifra encriptada com RSA com os seguintes parâmetros $e = 17$, $n = 213271$. Visto que o valor de n é pequeno, podemos calcular a fatorização em números primos.

Podemos calcular a chave privada, d, a partir de:

$d = e^{-1} \pmod{t}$

Esta chave pode ser calculada sabendo o valor de e e de t, sendo t o Mínimo Múltiplo Comum de p e q, onde p e q são o resultado da fatorização de n.

Além disso, como o inteiro foi codificado através de um esquema específico, desenvolveu-se duas funções de modo a fazer a conversão deste esquema:

codificar(l1, l2, l3) = n e descofidicar(n) = l1, l2, l3

Por fim, ao obter d podemos decifrar o criptograma ao descoficiar pelo esquema apresentado no enunciado.

Texto limpo:
"LET US THEREFORE PERMIT THESE NEW HYPOTHESES TO BECOME KNOWN TOGETHER WITH THE ANCIENT HYPOTHESES WHICH ARE NO MORE PROBABLE LET US DO SO ESPECIALLY BECAUSE THE NEW HYPOTHESES ARE ADMIRABLE AND ALSO SIMPLE AND BRING WITH THEM A HUGE TREASURY OF VERY SKILLFUL OBSERVATIONS SO FAR AS HYPOTHESES ARE CONCERNED LET NO ONE EXPECT ANYTHING CERTAIN FROM ASTRONOMY WHICH CANNOT FURNISH IT LEST HE ACCEPT AS THE TRUTH IDEAS CONCEIVED FOR ANOTHER PURPOSE AND DEPART FROM THIS STUDY A GREATER FOOL THAN WHEN HE ENTERED IT FAREWELL".Prefácio a Copérnico Sobre a Revolução das Esferas Celestes - Andreas Osiander