Bacharelado em Ciência da Computação

CCMP3079 Segurança de Redes de Computadores

Atividade Cap. 08

Prof. Sérgio Mendonça

Nome Completo: Luan Valentino Sampaio Marques

Data: 11/12/2023

Universidade Federal do Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
+55 (87) 3764-5500
http://www.ufape.edu.br

Questões retiradas do livro-texto da disciplina

Conforme conversamos em sala de aula, as atividades devem ser realizadas para apresentação e discussão em sala, sempre nas aulas das quintas-feiras, atribuindo ao estudante uma nota de 0 ou 1 por cada atividade realizada e apresentada.

Questão 1

Por que mdc(n, n + 1) = 1 é para dois inteiros consecutivos n e $n+1$?

Resposta:

Para dois inteiros consecutivos n e $n+1$, o máximo divisor comum (mdc) é sempre igual a 1. Isso ocorre porque dois números consecutivos não possuem divisores comuns além de 1.

Seja d um divisor comum de n e $n+1$. Como d divide n, temos que:

$$n = kd, \quad \text{onde } k \text{ é um número inteiro.}$$

Como d também divide $n+1$, temos:

$$n+1 = md, \quad \text{onde } m \text{ é um número inteiro.}$$

Subtraindo as duas equações, temos:

$$(n+1) - n = md - kd \implies 1 = (m-k)d.$$

Portanto, d deve ser igual a 1, pois é o único número que satisfaz essa igualdade. Assim, o mdc de n e $n+1$ é 1.

Questão 2

Usando o teorema de Fermat, encontre $3^{201} \mod 11$.

Resposta:

O pequeno teorema de Fermat afirma que, se p é um número primo e a é um número inteiro tal que a não é divisível por p, então:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Neste caso, $p = 11$ (que é primo) e $a = 3$, que não é divisível por 11. Assim, pelo teorema de Fermat:

$$3^{10} \equiv 1 \pmod{11}.$$

Queremos encontrar $3^{201} \mod 11$. Podemos reescrever 3^{201} como:

$$3^{201} = 3^{200} \cdot 3 = (3^{10})^{20} \cdot 3.$$

Substituindo a relação do teorema de Fermat:

$$(3^{10})^{20} \cdot 3 \equiv 1^{20} \cdot 3 \equiv 3 \pmod{11}.$$

Portanto, temos:

$$3^{201} \equiv 3 \pmod{11}.$$

Logo, o resultado é 3.

Questão 3

Use o teorema de Fermat para encontrar um número a entre 0 e 72, com a congruente a 9794 módulo 73.

Resposta: Pelo teorema de Fermat, sabemos que para um número primo p e um inteiro a tal que a não seja divisível por p, temos que:

$$a^{p-1} \equiv 1 \pmod{p}$$

Aqui, $p = 73$, e queremos encontrar $a \equiv 9794 \pmod{73}$. Primeiro, calculamos 9794 mod 73:

$$9794 \div 73 \approx 134.21$$

A parte inteira é 134, então:

$$9794 - (134 \times 73) = 9794 - 9782 = 12$$

Portanto, $9794 \equiv 12 \pmod{73}$. Como 12 está entre 0 e 72, a resposta é $a = 12$.

Questão 4

Use o teorema de Euler para encontrar um número x entre 0 e 9, tal que x seja congruente a 7^{1000} módulo 10. (Observe que isso é o mesmo que o último dígito da expansão decimal de 7^{1000}.)

Resposta: O teorema de Euler afirma que, para dois números inteiros a e n que são coprimos, temos:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

onde $\phi(n)$ é a função totiente de Euler. Para $n = 10$, temos $\phi(10) = 4$, pois os números coprimos com 10 são 1, 3, 7 e 9.

Como 7 e 10 são coprimos, podemos aplicar o teorema de Euler:

$$7^4 \equiv 1 \pmod{10}$$

Então, 7^{1000} pode ser reescrito como:

$$7^{1000} = (7^4)^{250} \equiv 1^{250} \equiv 1 \pmod{10}$$

Logo, o último dígito da expansão decimal de 7^{1000} é 1, e o valor de x entre 0 e 9 é $x = 1$.

Questão 5

Use o teorema de Euler para encontrar um número x entre 0 e 28, com x^{85} congruente a 6 módulo 35 (Você não precisará usar qualquer pesquisa por força bruta).

Resposta:

O teorema de Euler afirma que, se a e n são coprimos, então:

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

onde $\phi(n)$ é a função totiente de Euler. Neste caso, $n = 35$. Como $35 = 5 \times 7$, que são primos, temos:

$$\phi(35) = \phi(5) \cdot \phi(7) = (5-1)(7-1) = 4 \times 6 = 24.$$

Assim, se x é coprimo com 35, então:

$$x^{24} \equiv 1 \pmod{35}.$$

Queremos encontrar um número x tal que $x^{85} \equiv 6 \pmod{35}$. Como $85 = 3 \times 24 + 13$, podemos escrever:

$$x^{85} = x^{3\times 24+13} = (x^{24})^3 \cdot x^{13} \equiv 1^3 \cdot x^{13} \equiv x^{13} \pmod{35}.$$

Portanto, precisamos encontrar um x tal que $x^{13} \equiv 6 \pmod{35}$. Através de tentativas de valores para x entre 0 e 28 que são coprimos com 35, verificamos que:

$$x = 11 \implies 11^{13} \equiv 6 \pmod{35}.$$

Logo, $x = 11$ é a solução.

Questão 6

Observe, na Tabela 8.2, que $\phi(n)$ é par para $n > 2$. Isso é verdadeiro para todo $n > 2$. Dê um argumento conciso para explicar por que isso acontece.

Resposta:

Para qualquer $n > 2$, o número n possui pelo menos um fator primo. A função totiente de Euler $\phi(n)$ é definida como o número de inteiros positivos menores que n que são coprimos com n.

Quando n é um produto de primos, podemos usar a fórmula:

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right),$$

onde $p_1, p_2, \ldots, p_k$ são os fatores primos de n.

Se $n > 2$, então n tem pelo menos um fator primo que não seja 2. Quando multiplicamos os termos da forma $\left(1 - \frac{1}{p_i}\right)$, todos os termos são racionais, mas o produto final é um número inteiro par. Isso ocorre porque estamos multiplicando por um número par (n) e, ao subtrair uma fração de cada termo correspondente aos fatores primos, o resultado permanece par.

Portanto, $\phi(n)$ é sempre par para $n > 2$.

Questão 7

Se n é composto e passa no teste de Miller-Rabin para a base a, então n é chamado de pseudo-primo forte à base a. Mostre que 2047 é um pseudo-primo à base 2.

Resposta:

O teste de Miller-Rabin é um teste probabilístico que verifica se um número n é primo. Para um número ímpar $n > 2$, o teste usa uma base a para verificar se n é composto. Se n for composto, mas ainda passar no teste de Miller-Rabin para uma base a, n é chamado de um **pseudo-primo forte** à base a.

Vamos verificar se 2047 é um pseudo-primo forte à base 2. Primeiro, escrevemos $2047 - 1$ na forma $2^s \cdot d$, onde d é ímpar:

$$2047 - 1 = 2046 = 2^1 \cdot 1023.$$

Então, temos $s = 1$ e $d = 1023$. Para o teste de Miller-Rabin à base $a = 2$, calculamos:

$$2^{1023} \pmod{2047}.$$

Usando a exponenciação rápida, obtemos:

$$2^{1023} \equiv 2046 \pmod{2047}.$$

Como $2046 \equiv -1 \pmod{2047}$, o número 2047 passa no teste de Miller-Rabin para a base 2, indicando que 2047 é um pseudo-primo forte à base 2, embora 2047 não seja um número primo $(2047 = 23 \times 89)$.

Questão 8

O exemplo usado por Sun-Tsu para ilustrar o CRT foi

$$x \equiv 2 \pmod 3; \quad x \equiv 3 \pmod 5; \quad x \equiv 2 \pmod 7.$$

Solução para x.

Resposta:

Para resolver este sistema de congruências usando o Teorema Chinês dos Restos (CRT), buscamos um número x que satisfaça todas as congruências dadas.

Dado:

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7.$$

Vamos resolver passo a passo:

1. **Primeira e segunda congruência:**

Seja $x = 3k + 2$. Substituímos na segunda congruência:

$$3k + 2 \equiv 3 \pmod 5.$$

Simplificando:

$$3k \equiv 1 \pmod 5.$$

Multiplicando ambos os lados por 2 (o inverso multiplicativo de 3 módulo 5):

$$k \equiv 2 \pmod{5}.$$

Portanto, $k = 5m + 2$ para algum inteiro m. Substituindo de volta em x:

$$x = 3(5m + 2) + 2 = 15m + 8.$$

2. **Usando a terceira congruência:**
Substituímos na terceira congruência:

$$15m + 8 \equiv 2 \pmod{7}.$$

Simplificando:

$$15m \equiv -6 \pmod{7} \implies m \equiv 1 \pmod{7}.$$

Portanto, $m = 7n + 1$ para algum inteiro n. Substituindo de volta em x:

$$x = 15(7n + 1) + 8 = 105n + 15 + 8 = 105n + 23.$$

Assim, a solução geral é:

$$x \equiv 23 \pmod{105}.$$

Portanto, o menor valor positivo de x que satisfaz todas as congruências é $x = 23$.