DCC-UFRJ–Números Inteiros e Criptografia–Primeira Prova–2022.2

Justifique cuidadosamente todas as suas respostas.

Questão 1 (2,5 pontos)

Uma empresa doou 2051 canetas e 3223 lápis ao professor de matemática de uma escola, que distribuiu todas as canetas e todos os lápis aos seus alunos sem que sobrasse nenhuma caneta ou lápis.

(a) Quantos alunos o professor tem nesta escola? Euclides estendido

(b) Quantos lápis e quantas canetas cada aluno recebeu?

Questão 2 (2,5 pontos)

Sabe-se que $n = 437561$ é o produto de dois primos p e q. Determine p e q usando o algoritmo de Fermat.

Questão 3 (2,5 pontos)

Ache um fator primo de $a + b$ sabendo-se que a e b são inteiros maiores que 2^{100} que satisfazem $56a = 65b$.

Dica: aplique o teorema da fatoração única à equação dada.

Questão 4 (2,5 pontos)

Sejam a, b e c números inteiros maiores que 2^{100} e considere a equação diofantina $ax + by = c$. Sabe-se que $\text{mdc}(a, b) = 1$ e que α e β são os números obtidos como saída do algoritmo euclidiano estendido.

(a) Escreva a solução geral desta equação a partir de α e β.

(b) Mostre que se $\text{mdc}(a, b) = 1$ e $c \geq ab$ então a equação diofantina $ax + by = c$ tem soluções não negativas.

DCC-UFRJ–Números Inteiros e Criptografia–Segunda Prova–2022.2

Justifique cuidadosamente todas as suas respostas.

Questão 1 (3,0 points)
Seja $p > 30$ um número primo e r o resto da divisão de p por 30.

(a) Mostre que se $n > 30$ é um inteiro, cujo resto da divisão por 30 é divisível por 2, 3 ou 5, então n é composto.

(b) Mostre que se r não tem fator comum com 30, então r é primo.

(c) Use (a) e (b) para mostrar que r também é um número primo.

Questão 2 (2,0 points)
Sabe-se que 953 e $1907 = 2 \cdot 953 + 1$ são primos.

(a) Determine a ordem de 9 módulo 1907.

(b) Calcule o resto da divisão de 9^{4767} por 1907.

Dica para (a): aplica o Teorema de Fermat à base 3.

Questão 3 (3,0 points)
Seja $F = 2^{2^{10}} + 1$.

(a) Explique porque a ordem de 2 módulo F não pode ser um divisor de 2^{10}.

(b) Determine um inteiro m tal que $2^m \equiv 1 \pmod{F}$.

(c) Use o Lema Chave para calcular a ordem de 2 módulo F a partir de (a) e (b).

Questão 4 (2,0 points)
Sabe-se que $11 \cdot 83$ é a a fatoração em primos de $n = 913$.

(a) Use o Teorema de Fermat para calcular o resto da divisão de 5^{9763} por 11 e por 83.

(b) Use (a) e o algoritmo chinês do resto para calcular o resto da divisão de 5^{9763} por n.

DCC-UFRJ–Números Inteiros e Criptografia Terceira Prova 2022.2

Justifique cuidadosamente todas as suas respostas.

Questão 1 (3,0 points)
Prove, por indução, que $2^{n+3} \geq 4n$. Sua solução deve indicar claramente os vários passos da indução, incluindo a conclusão.

Questão 2 (3,0 points)
Sabe-se que $793 = 13 \cdot 61$.

(a) Calcule a ordem de 11 módulo 61.

(b) Calcule o resto de 11^{99} módulo 13 e módulo 61.

(c) Use o algoritmo chinês do resto para calcular o resto da divisão de 11^{99} por 793.

(d) Determine se 793 é um pseudoprimo forte para a base 11.

(e) Determine se 793 é um pseudoprimo para a base 11.

Questão 3 (2,0 points)
Sabe-se que 1151 é primo e que $9209 = 8 \cdot 1151 + 1$. Use que $11^{1151} \equiv 8580 \pmod{9209}$ e o teorema de Lucas para provar que 9209 é um número primo.

Questão 4 (2,0 points)
Considere a chave de RSA $n = 12193$ e $e = 7979$.

(a) Fatore n usando o algoritmo de Fermat e ache o parâmetro de decodificação d.

(b) Decodifique a mensagem 7213.

DCC-UFRJ–Números Inteiros e Criptografia–Prova Final–2022.2

Justifique cuidadosamente todas as suas respostas.

Questão 1 (1,5 pontos)
Prove, por indução em n, que

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1.$$

Sua solução deve indicar claramente os vários passos da indução, incluindo a conclusão.

Questão 2 (2,0 pontos)
Calcule a ordem de 7 módulo 29 e use isto para determinar o resto da divisão de $7^{8^{1024}}$ por 29.

Questão 3 (2,5 pontos)
Considere o número $6601 = 7 \cdot 23 \cdot 41$.

(a) Calcule o resto da divisão de 2^{825} por 6601 pelo algoritmo chinês do resto.

(b) Determine se 6601 é um pseudoprimo *forte* para a base 2.

(c) Determine se 6601 é um pseudoprimo para a base 2.

Questão 4 (4,0 pontos)
Considere a chave de RSA $n = 1089307$ e $e = 7^5$.

(a) Fatore n usando o algoritmo de Fermat.

(b) Determine a chave de decodificação desta versão do RSA, usando o algoritmo euclidiano estendido.

(c) Calcule o resto da divisão de 288810^7 por n sabendo-se que

$$288810^4 \equiv 288810 \pmod{n}.$$

(d) Codifique o número 288810 usando os valores de n e e dados.

Dica para o item (c): qual é o máximo divisor comum entre n e 288810?

Anna

DCC-UFRJ–Números Inteiros e Criptografia–Prova Final–2022.2

Justifique cuidadosamente todas as suas respostas.

Questão 1 (2,0 pontos)
Prove, por indução em n, que

$$n < 2^n$$

para todo $n \geq 1$. Sua solução deve indicar claramente os vários passos da indução, incluindo a conclusão.

Questão 2 (3,0 pontos)
Seja $607 = 6 \cdot 101 + 1$. Sabendo-se que $3^{101} \equiv 211 \pmod{607}$:

(a) mostre que 607 é primo usando o teorema de Lucas;

(b) calcule a ordem de $3^6 = 729$ módulo 607;

(c) calcule o resto da divisão de 5^{27272} por 607.

Questão 3 (3,0 pontos)
Considere o número $671 = 11 \cdot 61$.

(a) Calcule o resto da divisão de 3^{670} por 671 pelo algoritmo chinês do resto.

(b) Determine se 671 é um pseudoprimo *forte* para a base 3.

(c) Determine se 671 é um pseudoprimo para a base 3.

Questão 4 (2,0 pontos)
Considere a chave de RSA $n = 24257$ e $e = 31$.

(a) Fatore n usando o algoritmo de Fermat.

(b) Determine a chave de decodificação desta versão do RSA, usando o algoritmo euclidiano estendido.

2.2.2.7 (a) = 5.13(b)

NÚMEROS INTEIROS E CRIPTOGRAFIA–IC–UFRJ

ATIVIDADE 1

17,55

1. Para criar sua versão do RSA você vai precisar das seguintes funções do MAXIMA:

   - `next_prime(m)` acha o menor primo maior que m;
   - `gcd(a,b)` calcula o máximo divisor comum entre a e b;
   - `remainder(a,m)` calcula o resto da divisão de a por m;
   - `b^m` calcula a potência b^m.

Para atribuir à variável x o valor a escrevemos `x:a`. Finalmente, vamos precisar da função `igcdex(e,f)` que retorna uma lista com três números inteiros. Se `l:= igcdex(a,b)` então, tomando α como sendo o valor de `l[1]`, β como sendo o valor de $l[2]$ e d como sendo o valor de $l[3]$, temos que δ é o máximo divisor comum de a e b e que $a\alpha+b\beta = \delta$.

3. As chaves do RSA são pares de números inteiros positivos. Denotaremos sua chave pública por $[n, e]$ e sua chave secreta por $[n, d]$. Para construir n, precisamos de dois números primos distintos p e q. Siga a seguinte receita para construir suas chaves públicas no MAXIMA:

   Escolha dos primos: use `next_prime` para obter dois primos distintos p e q com entre 10 e 12 algarismos cada;
   Cálculo de n e f: $n : p * q$ e $f : (p-1) * (q-1)$;
   Escolha de e: escolha um número inteiro positivo qualquer $e > 10^{10}$ cujo mdc com f é 1;
   Cálculo de d: use `igcdex(e,f)` para calcular inteiros α e β tais que $e\alpha + f\beta = 1$ e tome

$$d = \begin{cases} \alpha & \text{se} \quad \alpha > 0 \\ f + \alpha & \text{se} \quad \alpha < 0. \end{cases}$$

Sua *chave pública* será o par $[n, e]$ e sua *chave secreta* será o par $[n, d]$. As receitas para encriptar e decriptar com estas chaves são as seguintes:

   Encriptação: se $0 \leq b < n$ for um bloco da mensagem que você quer encriptar, então `remainder(b^e,n)` será o resultado da encriptação RSA do bloco b;

[3365

boa

tatakae

Decriptação: se $0 \leq a < n$ for um bloco da mensagem que você quer decriptar, então `remainder(a^d,n)` será o resultado da decriptação RSA do bloco a.

Usando as chaves que você construiu:

(a) envie os números n e e de sua chave pública para o(a) colega cujo email você recebeu, por sua vez ele(a) vai lhe mandar a chave pública dele(a);
(b) converta uma mensagem de sua escolha em um número inteiro usando a tabela de conversão entre letras e números ao final do laboratório;
(c) subdivida o número obtido em (b) em blocos menores que n;
(d) encripte cada bloco usando **a chave pública do seu(sua) colega** e envie a lista de blocos encriptados para ele(a);
(e) em troca, ele(a) vai lhe mandar uma mensagem, encriptada com sua chave pública, para **você decriptar usando sua chave secreta.**

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Checklist

- ☐ Qual o papel de $f = (p-1)(q-1)$ no RSA?
- ☐ Por que e tem que ser escolhido sem fator comum com f?
- ☐ Por que d tem que ser positivo?
- ☐ Por que d tem que satisfazer $ed + fm = 1$?
- ☐ Por que $D(C(b)) = b$?
- ☐ Por que os blocos da mensagem a ser codificada têm que ser menores que n?
- ☐ Como achar primos grandes para usar no RSA?

Como funcionam as seguintes funções do MAXIMA?

- ☐ `gcd`
- ☐ `igcdex`
- ☐ `next_prime`
- ☐ `power_mod`
- ☐ `primep`
- ☐ `eulerPhi`

Tatakae

29302930203034

B

INSTITUTO DE COMPUTAÇÃO–UFRJ

NÚMEROS INTEIROS E CRIPTOGRAFIA – ESTUDO DIRIGIDO 1

Estudo dirigido 1

Sejam b um número real e $n \geq 0$ um número inteiro. Definimos

$$b^n = \begin{cases} 1 & \text{se } n = 0 \\ \underbrace{b \cdot b \cdots b}_{n \text{ vezes}} & \text{se } n \geq 1. \end{cases}$$

1. Sejam b um número real e m e n inteiros:

   (a) use a definição de potência para provar que

   $$b^n \cdot b^m = b^{n+m};$$

   (b) use (a) e a definição de potência para provar que

   $$(b^m)^n = b^{mn}.$$

2. Sejam b um número real e k, m e n inteiros. Escreva $(b^{k^m})^{k^n}$ como uma potência na base b.

3. Usando as fórmulas dos exercícios anteriores simplifique os números abaixo o mais possível, escrevendo-os como potências de uma mesma base:

   (a) $2^5 \cdot 3^5$;
   (b) $(2^5)^6 \cdot 2^7$;
   (c) $(2^{3^4})^{3^9}$;
   (d) $(2^{3^4})^{5^4}$.

4. Determine o inteiro n tal que $(3^{2^8})^{2^5} \cdot (3^{2^6})^{2^7}$ é igual a 3^{2^n}.

INSTITUTO DE COMPUTAÇÃO – UFRJ – 2022.2

NÚMEROS INTEIROS E CRIPTOGRAFIA–ESTUDO DIRIGIDO 2

Neste estudo dirigido investigaremos como resolver *equações diofantinas lineares*

(1) $\qquad ax + by = c$ em que a, b e c são números inteiros e x e y são variáveis,

usando o algoritmo euclidiano estendido. Isto é buscaremos inteiros x_0 e y_0 tais que $ax_0 + by_0 = c$.

1. Comece aplicando o algoritmo euclidiano estendido para calcular $d = \text{mdc}(a, b)$ e inteiros α e β tais que $\alpha \cdot a + \beta \cdot b = d$, quando $a = 99918$ e $b = 5471$ e quando $a = 17652$ e $b = 12672$.

2. Seja $d = \text{mdc}(a, b)$ e digamos que $x = x_0$ e $y = y_0$ são soluções de (1).

   (a) Explique porque existem inteiros a' e b' tais que $a = da'$ e $b = db'$.
   (b) Substitua $a = da'$ e $b = db'$ em $ax_0 + by_0 = c$ e mostre que d tem que dividir c.
   (c) Use (b) para inventar dois exemplos de equações diofantinas lineares que *não* têm solução.

3. Considere a equação diofantina $99918x + 5471y = 7$. No exercício 1 calculamos inteiros α e β tais que $99918\alpha + 5471\beta = 1$.

   (a) Por que número $99918\alpha + 5471\beta = 1$ deve ser multiplicada para que o lado direito seja 7?
   (b) Compare $99918x + 5471y = 7$ com a expressão obtida em (a) e determine uma solução desta equação, usando os valores de α e β calculados no exercício 1.
   (c) Faça o mesmo para $17652x + 12672y = 36$ e $17652x + 12672y = 28$.

4. Nesta questão analisaremos, em detalhe, o método utilizado para resolver as equações dos exercícios acima. Seja $d = \text{mdc}(a, b)$ e digamos que $a = da'$, $b = db'$ e $c = dc'$, em que $a', b', c' \in \mathbb{Z}$.

   (a) Por que número devemos multiplicar $\alpha \cdot a + \beta \cdot b = d$ para que o lado direito passe a ser c, quando α e β foram calculados pelo algoritmo euclidiano estendido?
   (b) Comparando a equação diofantina (1) com a expressão obtida em (a) determine uma fórmula para a solução de (1) em função de α, β e c'.

5. Suponhamos que você encontrou uma solução $x = x_0$ e $y = y_0$ para a equação diofantina (1). Mostre que se a' e b' são inteiros tais que $a = da'$ e $b = db'$, então $x = x_0 + kb'$ e $y = y_0 - ka'$ também nos dão uma solução da mesma equação, qualquer que seja o número inteiro k. Use as fórmulas desta questão e da anterior para encontrar as soluções gerais das equações do exercício 3. Veremos mais adiante neste curso que estas fórmulas nos dão a solução geral da equação (1).

INSTITUTO DE COMPUTAÇÃO – UFRJ – 2022.2

NÚMEROS INTEIROS E CRIPTOGRAFIA–ESTUDO DIRIGIDO 3

Sejam $n > 1$ e b números inteiros. A *ordem* de b módulo n é o menor inteiro positivo k tal que $b^k \equiv 1 \pmod{n}$. Os principais resultados que você precisar saber para resolver os exercícios deste estudo dirigido são os seguintes:

Existência da ordem: b só tem ordem módulo n se $\text{mdc}(b, n) = 1$;

Lema chave: $b^m \equiv 1 \pmod{n}$ se, e somente se, a ordem de b módulo n divide m;

1. Calcule as ordens de todos os inteiros módulo 10 e módulo 11.

2. Calcule a ordem de 2 módulo p, quando $p = 11$ e $p = 17$.

3. Use o exercício anterior para calcular o resto de 2^{99876} na divisão por 11 e na divisão por 17.

4. Sabendo-se que $3^{82} \equiv 1 \pmod{83}$, determine:

   (a) a ordem de 3 módulo 83, usando o lema chave;
   (b) o resto da divisão de 3^{99876} por 83.

5. Seja $n = 2^{61} - 1$. Determine:

   (a) a ordem de 2 módulo n, usando o lema chave;
   (b) o resto da divisão de 2^{868221} por n.

6. Considere o primo $p = 10^9 + 21$ e seja $n = 16p + 1$. Sabe-se que $3^{8p} \equiv -1 \pmod{n}$.

   (a) Use o lema chave para mostrar que a ordem 3 módulo n não pode dividir $8p$.
   (b) Ache uma potência de 3 que seja congruente a 1 módulo n.
   (c) Use (a), (b) e o lema chave para calcular a ordem 3 módulo n.