Teoria dos Números

Notas de aula da disciplina TE: Técnicas de Construção de Algoritmos

Fabiano de Souza Oliveira
(fabiano.oliveira@ime.uerj.br)

Paulo Eustáquio Duarte Pinto
(pauloedp arroba ime.uerj.br)

agosto/2020

TE: Técnicas de Construção de Algoritmos
Teoria dos Números

Problemas de 29/08/2020:

1807 - Triângulo Trinomial, a Vingança
2801 - Cifra Affine
2852 - Troca de Mensagens
2636 - 3-RSA
1716 - RSA

1807 - Triângulo Trinomial, a Vingança

Contexto: O triângulo trinomial é análogo ao de Pascal, só que cada elemento é a soma de 1, 2, ou 3 outros, aqueles acima, à esquerda e à direita de cada elemento, segundo a configuração:

```
                1
            1   1   1
        1   2   3   2   1
    1   3   6   7   6   3   1
1   4   10  16  19  16  10  4   1
```

Dada a linha R do triângulo, quer-se imprimir a soma dos elementos dessa linha.

Entrada: Uma único caso de teste, contendo o inteiro R ($0 \leq R \leq 999.999.999$).

Saída: Imprimir a soma dos elementos da linha R, em módulo $2^{31} - 1$.

Exemplo de entrada 1:
0

Exemplo de saída 1:
1

Exemplo de entrada 2:
2

Exemplo de saída 2:
9

1807 - Triângulo Trinomial, a Vingança

Dicas:

1. A nomenclatura não está de acordo com a Matemática. Na Matemática, triângulo trinomial é obtido tomando os coeficientes do desenvolvimento de $(a+b+c)^n$.

2. Somando cada linha obtemos, por indução, ...

3. Implementar Potência Modular

4. DESAFIO: Provar, por indução o resultado de 2.

2801 - Cifra Affine

Contexto: É definida a cifra Affine, baseada em 3 inteiros T, A, B, onde T é o tamanho do alfabeto (os símbolos vão de 0 a T-1). Para criptografar um número X, ele é substituido por Y = (X*A+B) mod T. Nesse problema quer-se resolver o problema inverso, ou seja, dado Y, qual o valor de X?

Entrada: Um único caso de teste, descrito em 3 linhas. Na primeira, o inteiro N ($1 \leq N \leq 10^5$), o número de símbolos criptografados. Na segunda linha N inteiros positivos entre 0 e T-1, resultados da criptografia. Na 3ª linha, os inteiros T, A e B ($1 \leq A, B, T \leq 10^9$).

Saída: Para cada teste, imprimir N inteiros correpondendo aos números cuja criptografia é dada, ou a mensagem "DECIFRAGEM AMBIGUA", se não for possível decifrar um número de modo único.

Exemplo de entrada:

```
3
63 60 49
119 25 48
```

Exemplo de saída:

```
1  10  100
```

2801 - Cifra Affine

Dicas:

1. Quer-se calcular X a partir de $Y = (X.A+B) \bmod T$.
   Ou seja $X.A + B \equiv Y \bmod T$, ou
   $X.A \equiv (Y-B) \bmod T$

2. Para encontrar X, temos que ter o inverso modular de A, A^{-1}.
   Como sabemos, isso só é possível se MDC(A,T) = 1. Se esse for o caso, então encontramos:
   $X = A^{-1}(Y-B) \bmod T$

3. No exemplo:
   MDC(25, 119) = 1. Inv modular (25, 119) = -19
   X.25 + 48 = 60 mod 119
   X = (60 - 48)*(-19) mod 119 = -228 mod 119 =
   -109 mod 119 = (-109+119) mod 119 = 10 mod 119 =
   10 (pois o símbolo deve estar entre 0 e 119).

2852 - Troca de Mensagens

Contexto: A cifra de Vigenère é uma modificação da cifra de César, usando uma palavra chave e a tabela:

	a	b	c	d	e	f		x	y	z
a	a	b	c	d	e	f		x	y	z
b	b	c	d	e	f	g		y	z	a
z	z	a	b	c	d	e		w	x	y

A palavra chave é repetida quantas vezes necessário e indica para cada letra da mensagem, qual linha usar para codificar. Neste problema só se codifica começada por consoantes.

Entrada: Um caso de teste descrito em várias linhas. A primeira linha contém um string K (tamanho entre 3 e 45), a palavra chave. Na segunda linha vem um inteiro N ($1 \leq N \leq 150$), o número de linhas a serem criptografadas. A seguir vêm N linhas de tamanho máximo = 100.000. Todos os caracteres envolvidos são letras minúsculas ou espaços.

Saída: Cada linha da entrada criptografada.

Exemplo de entrada:
```
informatica
2
ciencia da computacao
olimpiada brasileira de informatica
```

Exemplo de saída:
```
kvjbtua wi eouczhroah
olimpiada jefgzxebzc dm informatica
```

2852 - Troca de Mensagens

Exemplo: Palavra chave: etc Mensagem: curso na uerj

c	u	r	s	o		n	a		u	e	r	j
e	t	c	e	t	c	e	t	c	e	t	c	e

	a	b	c	d	e	f		r	s	t	u	v	w	x	y	z
e	e	f	g	h	i	j		v	w	x	y	z	a	b	c	d
t	t	u	v	w	x	y		k	l	m	n	o	p	q	r	s
c	c	d	e	f	g	h		t	u	v	w	x	y	z	a	b

c	u	r	s	o		n	a		u	e	r	j
g	b	t	w	h		r	t		u	r	r	j

2636 - 3-RSA

Contexto: Por analogia com o método 3-DES, que usa 3 chaves, a Criptografia 3-RSA usaria 3 primos como base cujo produto é igual a N. Dado um número n quer-se saber quais os primos base.

Entrada: Vários casos de teste, cada teste em uma linha. Cada teste contém um inteiro n, ($105 \leq n < 10^{18}$). A entrada termina com uma linha contendo 0, que não deve ser processada.

Saída: Para cada teste deve ser impressa a mensagem "n = p x q x r", onde p, q, e r são os primos base.

Exemplo de entrada 1:

105
231
7163
89348965057411

Exemplo de saída 1:

105 = 3 x 5 x 7
231 = 3 x 7 x 11
7163 = 13 x 19 x 29
89348965057411 = 17393 x 51437 x 99871

2636 - 3-RSA

1. O menor primo certamente é menor que 10^6. A descrição do problema esconde uma restrição: o segundo primo é menor que 3×10^7.

2. O problema se restringe a fatorar um número grande, sabendo que dois de seus fatores são menores ou iguais a 3×10^7.

1716 - RSA

Contexto: É descrito o método RSA, conforme dado em sala. O que se quer é quebrar a RSA, pois são dadas as chaves públicas (N, e) e uma mensagem C, criptografada. O objetivo é descriptografar C, obtendo a mensagem original, M.

Entrada: Um único caso com três inteiros, N ($15 \leq N \leq 10^9$), e e C ($1 \leq e, C < N$), onde o par (N, e) é a chave pública e C a mensagem criptografada.

Saída: Um inteiro M ($1 \leq M < N$), contendo a mensagem original.

Exemplo de entrada 1:
1073 71 436

Exemplo de saída 1:
726

1716 - RSA

Dicas:

1. Nesta situação só será possível quebrar a RSA, porque é possível fatorar N, pois ele é pequeno.

2. Portanto, trata-se de fatorar N, obter os primos e aplicar o método estudado em sala.

FIM