Teoria dos números IV
Aplicações de congruências

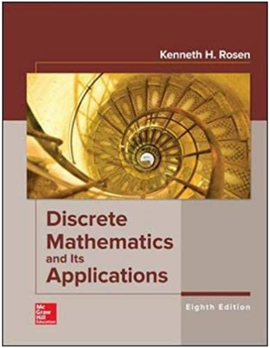
André Gustavo dos Santos[1]

[1] Departamento de Informática
Universidade Federal de Viçosa

INF230 - 2021/1

Conteúdo

Os slides seguintes são baseados nas seções 4.4 e 4.5 do livro texto da disciplina:



ROSEN, Kenneth H.
Discrete mathematics and its applications.
McGraw-Hill Education, 8th edition, 2018

Pequeno teorema de Fermat

Pequeno teorema de Fermat

Se p é primo e a é um inteiro não divisível por p, então $a^{p-1} \equiv 1 \bmod p$.

- Além disso, para todo inteiro a, $a^p \equiv a \bmod p$.

Calcule $7^{222} \bmod 11$

Usando o pequeno teorema de Fermat em vez do alg. de potenciação modular rápida:

- Pelo pequeno teorema de Fermat $7^{10} \equiv 1 \bmod 11$
- Então $(7^{10})^k \equiv 1 \bmod 11$ para todo inteiro positivo k
- Para aproveitar esta última congruência, dividimos o expoente 222 por 10
- $7^{222} = 7^{22 \cdot 10+2} = (7^{10})^{22} 7^2 \equiv 1^{22} \cdot 49 \equiv 5 \bmod 11$
- Então, $7^{222} \bmod 11 = 5$.

Pequeno teorema de Fermat

- De uma forma geral, podemos calcular $a^n \bmod p$ quando p é primo e $p \nmid a$
- Usar o algoritmo da divisão para o resto de n por $p-1$: $n = q(p-1) + r$
- $a^n = a^{q(p-1)+r} = (a^{p-1})^q a^r \equiv 1^q a^r \equiv a^r \bmod p$, pois $r \nmid p$ já que $0 \leq r < p-1$
- Então, para calcular $a^n \bmod p$, basta calcular $a^r \bmod p$

Pseudoprimos

- Vimos que n é primo se não tem um divisor primo p com $p \leq \sqrt{n}$
- Usar este critério requer a lista de primos até $\sqrt{n}$ e uma divisão por cada um
- Há uma forma mais eficiente de determinar se um número inteiro é primo?
- De acordo com algumas fontes, matemáticos chineses acreditavam que n ímpar é primo se e somente se

$$2^{n-1} \equiv 1 \bmod n$$

- Se isto fosse verdade, teríamos um teste de primalidade muito eficiente!
- Por que eles acreditavam nisso?
  - Por que valia para primos ímpares. Por exemplo, $2^{5-1} = 2^4 = 16 \equiv 1 \bmod 5$.
  - Por que não acharam um número composto que valia.
- Hoje sabemos que estavam parcialmente corretos
  - Realmente vale para primos ímpares (prova: pequeno teorema de Fermat)
  - Mas pode valer para números compostos (contra-exemplo: $2^{340} \equiv 1 \bmod 341$)

Pseudoprimos

- Como 341 satisfaz mas não é primo, ele é chamado pseudoprimo na base 2
- Dado n, testar a validade de $2^{n-1} \equiv 1 \mod n$ fornece alguma evidência sobre sua primalidade. Em particular, se não vale, certamente é um número composto.
- Os que passam no teste são primos ou pseudoprimos na base 2
- Existem relativamente poucos pseudoprimos. Por exemplo, entre os inteiros até 10^{10} existem 455.052.512 primos, mas apenas 14.884 pseudoprimos na base 2

- Podemos usar outras bases em vez de 2 para definir os pseudoprimos

Definição

Se n é inteiro positivo composto e b é inteiro positivo com $b^{n-1} \equiv 1 \mod n$, então n é chamado de pseudoprimo na base b.

- Se n passa no teste para base 2, podemos testar outras bases
- Infelizmente há números compostos n que passam em todas as bases b coprimo

Números de Carmichael

Definição

Um número composto n que satisfaz a congruência $b^{n-1} \equiv 1 \bmod n$ para todo inteiro positivo b com $\text{mdc}(n, b) = 1$ é chamado número de Carmichael.

Números de Carmichael

Definição

Um número composto n que satisfaz a congruência $b^{n-1} \equiv 1 \mod n$ para todo inteiro positivo b com $\text{mdc}(n, b) = 1$ é chamado número de Carmichael.

Exemplo: 561 é um número de Carmichael

Raiz primitiva e logaritmo discreto

- No conjunto dos reais, se $b > 1$ e $x = b^y$, dizemos que y é o logaritmo de x na base b, denotado por $y = \log_b x$
- Este conceito pode ser estendido para números inteiros módulo p, onde p é primo

Definição

Uma raiz primitiva módulo um primo p é um inteiro r em $\mathbb{Z}_p$ tal que todo elemento $\neq 0$ de $\mathbb{Z}_p$ é potência de r.

2 e 3 são raízes primitivas módulo 11?

- Potências de 2 em $\mathbb{Z}_{11}$:
  - $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$
  - Todo elemento não nulo de $\mathbb{Z}_{11}$ é potência de 2, logo 2 é uma raiz primitiva módulo 11
- Potências de 3 em $\mathbb{Z}_{11}$:
  - $3^1 = 3$, $3^2 = 9$, $3^3 = 5$, $3^4 = 4$, $3^5 = 1$, e então o padrão se repete
  - Nem todo elemento não nulo de $\mathbb{Z}_{11}$ é potência de 3, logo 3 não é raiz primitiva módulo 11

UFV

Raiz primitiva e logaritmo discreto

- Um fato importante em teoria dos números é que existe raiz primitiva módulo p para todo primo p
- Seja p um primo e r uma raiz primitiva de p
  - Se a é um inteiro entre 1 e $p-1$, ou seja, um inteiro não nulo de $\mathbb{Z}_p$, então existe um único expoente e tal que $r^e = a$ em $\mathbb{Z}_p$, ou seja $r^e \bmod p = a$

Definição

Se p é primo, r uma raiz primitiva de p, a um inteiro entre 1 e $p-1$ inclusive, e $r^e \bmod p = a$, com $0 \leq e \leq p-1$, dizemos que e é o logaritmo discreto de a módulo p na base r, denotado por $\log_r a = e$ (com o primo p subentendido).

Calcule o logaritmo discreto de 3 e 5 módulo 11 na base 2

- Como $2^8 = 3$ e $2^4 = 5$ em $\mathbb{Z}_{11}$, temos que $\log_2 3 = 8$ e $\log_2 5 = 4$
  (Obs.: o módulo 11 fica subentendido e não é escrito na notação)

- Apesar do problema não parecer complicado, não existe algoritmo eficiente para cálculo de logaritmo discreto, e essa dificuldade é importante para a criptografia

Hashing

- Tabela hash é usada para armazenar e recuperar informação de forma eficiente
- A localização de um item é obtida aplicando-se uma função hash à chave

$h(k) = k \bmod 111$

- $h(064212848) = 064212848 \bmod 111 = 14$
- $h(037149212) = 037149212 \bmod 111 = 65$
- $h(107405723) = 107405723 \bmod 111 = 14$ ⚠

- Corre-se o risco de duas chaves gerarem a mesma posição, então deve haver um método para tratar este problema, chamado colisão

Números pseudoaleatórios

- Números aleatórios são necessários em muitos processos de simulação por computador
- Diferentes métodos foram criados para gerar números com propriedades de números escolhidos aleatoriamente
- Como números gerados de forma sistemática não são realmente aleatórios, são chamados pseudoaleatórios
- A forma mais comum de geração de números pseudoaleatórios é pelo método de congruência linear
  - Escolhemos um módulo m, um multiplicador a, um acréscimo c e uma semente x_0 com $2 \leq a < m, 0 \leq c < m, 0 \leq x_0 < m$
  - Uma sequência de números pseudoaleatórios $x_0, x_1, \ldots x_n$, $0 \leq x_i < m$, é gerada por:

$$x_{n+1} = (ax_n + c) \bmod m$$

- Para gerar números entre 0 e 1, basta dividir a lista pelo módulo, x_i/m

Números pseudoaleatórios

Escreva a lista dos números gerados com $m = 9$, $a = 7$, $c = 4$ e $x_0 = 3$.

- $x_0 = 3$
- $x_1 = (7x_0 + 4) \bmod 9 = (21 + 4) \bmod 9 = 7$
- $x_2 = (7x_1 + 4) \bmod 9 = (49 + 4) \bmod 9 = 8$
- $x_3 = (7x_2 + 4) \bmod 9 = (56 + 4) \bmod 9 = 6$
- $x_4 = (7x_3 + 4) \bmod 9 = (42 + 4) \bmod 9 = 1$
- $x_5 = (7x_4 + 4) \bmod 9 = (7 + 4) \bmod 9 = 2$
- $x_6 = (7x_5 + 4) \bmod 9 = (14 + 4) \bmod 9 = 0$
- $x_7 = (7x_6 + 4) \bmod 9 = (0 + 4) \bmod 9 = 4$
- $x_8 = (7x_7 + 4) \bmod 9 = (28 + 4) \bmod 9 = 5$
- $x_9 = (7x_8 + 4) \bmod 9 = (35 + 4) \bmod 9 = 3$
- como $x_9 = x_0$, a sequência se repete

- Muitos computadores usam este método para gerar números pseudoaleatórios
- São frequentes os geradores puramente multiplicativos, com $c = 0$
- O gerador com módulo $2^{31} - 1$ e multiplicador $7^5 = 16807$, por exemplo, gera $2^{31} - 2$ números antes de começar a repetir

Dígito verificador

- Congruências são usadas para verificar erros em strings de dígitos
- Uma técnica comum é adicionar um dígito extra no final, o dígito verificador
- Este dígito é calculado por uma função com os demais dígitos
- Para verificar se um string está correto, verifica-se se o dígito verificador é coerente
- Uma ideia semelhante é o uso de bit de paridade no envio e armazenamento de informação

UPC - *Universal Product Codes*

0 36000 29145 2

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3_x 11 + x_{12} \equiv 0 \bmod 10$$

ISBN-10 - *International Standard Book Number*

$x_{10} \equiv \sum_{i=1}^{9} ix_i (\mathrm{mod}\ 11)$, ou, de forma equivalente, $\sum_{i=1}^{10} ix_i \equiv 0 (\mathrm{mod}\ 11)$