

## 1 CAPÍTULO 1

- **pag 2 linha 9:** pelo menos dois deles são disjuntos dados quaisquer dois entre eles, são disjuntos.
- **pag 6 linha -9:** ~~temos o dobro de pares ordenados como dois conjuntos com dois elementos~~ temos o dobro de pares ordenados que de conjuntos com dois elementos
- **pag 13 par 2 linha 3:** ~~o incremento da tripla~~ a tripla crescente
- **pag 13 par 3 linha 4:** ~~o número de subconjuntos de um conjunto~~ o número de subconjuntos com dois elementos de um conjunto
- **pag 16 linha 15:** (em um conjunto) ~~um elemento pode aparecer mais de uma vez~~ um elemento pode aparecer no máximo uma vez

## 2 CAPÍTULO 2

- **pag 56 linha -12:** ~~Criptografia usando módulo de adição n~~ Criptografia usando adição módulo n
- **pag 57 linha -17:** ~~Criptografia usando módulo de multiplicação n~~ Criptografia usando multiplicação módulo n
- **pag 57 linha -15:** ~~multiplicar um módulo de mensagem por..~~ multiplicar módulo n, uma mensagem, por..
- **pag 57 linha -7,-8:** ~~tirar uma mensagem de x .... para algum valor que o emissor...~~ pegar uma mensagem x .... para algum valor a que o emissor...
- **pag 64 linha 6:** ~~marcando~~ checando
- **pag 64 linha 7:** ~~que um múltiplo de 2, exatamente, é igual a 1~~ que exatamente um múltiplo de 2 é igual a 1
- **pag 66 linha -7:** ~~a tem um módulo multiplicativo inverso n~~ a tem um inverso multiplicativo, modulo n
- **pag 66 linha -4:** ~~módulo inverso triplicativo de n ao calcular inverso multiplicativo,~~ modulo n, calculando
- **pag 66 linha -4:** ~~tal algoritmo não existe~~ tal algoritmo existe
- **pag 66 linha -1:** ~~nossa afirmação conjecturada inversa~~ nossa afirmação invarsa, que conjecturamos.
- **pag 67 linha -5:** ~~se não existir~~ se existir

- **pag 85 linha -14:** ~~e elevar um número de 150 dígitos  $a$  a  $10^{120}$  potência do módulo de 300 dígitos inteiros  $n$  elevar um número de 150 dígitos  $a$  à  $10^{120}$ -ésima potência, módulo um inteiro de 300 dígitos  $n$~~  **e ainda cobram por esta porcaria!!**
- **pag 88 linha -1..:** ~~se escolhermos cerca de  $m$  números de forma aleatória e verificarmos se cerca de  $\ln(m)$  números ao redor de  $m$  são primos, seria de esperar que um desses fosse primo~~ se escolhermos um número  $m$  de forma aleatória e verificarmos  $\ln(m)$  números ao redor de  $m$ , seria de esperar que um desses fosse primo.
- **pag 89 linha 24:** ~~limitado anteriormente~~ limitado superiormente

### 3 CAPÍTULO 3

- **pag 95 - primeiro quadradinho, pag 98 linha 2:** ~~instruções~~ afirmações
- **pag 96 - linha -3:** ~~demonstrações~~ afirmações
- **pag 98 - Lema 3.1:** sempre falta  $w$  antes do símbolo  $\wedge$
- **pag 101 - linha 7:** ~~declarações~~ afirmações *(isso em muitos outros pontos, no capítulo inteiro: ex pag 105 linha -2... a palavra declaração é sempre afirmação, exceto quando é no sentido de declaração de variável em um programa, como na nota 5 no fundo da página 105)*
- **pag 105 - seção 3.2 - linha 7:** ~~varia por~~ varia entre
- **pag 105 - seção 3.2 - linhas 10-11:** ~~varia por~~ ~~posses~~ varia entre as pessoas
- **pag 122 - linha -6:** ~~consideramos~~ supusemos  
~~..uma solução verdadeira ...uma solução fosse verdadeira~~

### 4 CAPÍTULO 4

- **pag 136 - linha -6:** ~~as dimensões resolvidas ....que a dimensão atual o tamanho do problema resolvido .... que o tamanho do problema atual~~
- **pag 136 - linha -3:** ~~as dimensões consideradas .... menores que a dimensão atual as afirmações assumidas .... para um parâmetro menor que o atual~~
- **pag 191 - linha 7:** ~~há muitos casos entre..~~ há um número finito de casos entre...