Números Inteiros e Criptografia, PLE 2020, Lista de Exercícios 9
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049873

Questão 1. Use o Pequeno Teorema de Fermat para determinar:
* a. o resto de 10^10^100 dividido por 7.

Pelo Teorema de Fermat II temos a^(p-1) ≡ 1 (mod p)
Como queremos achar a forma reduzida de 10^10^100 mod 7, podemos escrever como:
10^10^100 ≡ 10^((6)q+r)≡ (10^6)^q * 10^r mod 7

Ou seja, precisamos descobrir principalmente r em 10^100 = 6q+r

Dividindo 10^100 por 6:

```
10 * 10^99 | 6
  4 * 10^98|---------
 40 * 10^98| 166666...
  4 * 10^98|
 40 * 10^97
       .
       .
       .
       4
```

Temos então que o resto dessa divisão é 4, logo:

10^10^100 ≡ 10^((6)*(1666….)+4) ≡ (10^6)^(16666….) * 10^4 mod 7

Como:
10^2 ≡ 2 mod 7
10^6 ≡ (10^2)^3 ≡ 2^3 ≡ 8 ≡ 1 mod7
10^4 ≡ $(10\text{^}2)^2 \equiv 2^2$ ≡ 4 mod 7

Vamos assim achar que

(10^6)^(16666….) * 10^4 ≡ (1)^(1666…) * 4 ≡ 4 mod 7

Logo: o resto da divisão de 10^10^100 dividido por 7 é 4

*Questão 3. Prove que se um n ímpar é um pseudoprimo de Fermat para alguma base, então ele é pseudoprimo de Fermat para um número par de bases.

Questão 5. Em cada item abaixo, use o Teste de Fermat com a base b indicada e conclua que o número n dado é composto. Você deve fazer as contas à mão; só pode contar com ajuda de computador ou calculadora para efetuar adições, multiplicações, subtrações e divisões.

* a. n = 1687, b = 4

    Temos que $4^{12} \equiv 1 \bmod 1687$

    4^1687 ≡ (4^{12})^140 * 4^7 ≡ 1^140 * 16384 mod 1687

    Como 4^1687 ≡ 16384 mod 1687 e não 4^1687 ≡ 4 mod 7, então 1687 é composto

* b. n = 2107, b = 7

    7^2107 ≡ 1813^301 ≡ (1813^7)^43

    49^3 * 1813 ≡ 1764 * 1813 mod 2107

Questão 6. Estes são todos os primos até 317:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317

* a. Usando esta lista, escreva uma função em Python que receba como entradas naturais limite e base, com limite ≤ 10^5 e base ≥ 2, e retorne uma lista contendo exatamente os números entre 2 e limite (incluindo limite, se for o caso) que são pseudoprimos de Fermat para a base dada.

* b. Usando sua função, responda: quantos pseudoprimos para base 2 existem entre 2 e 10^5 ? E para a base 7 entre 2 e 10^5 ?

    Para a base 2, entre 2 e 10^5 existem 78 pseudoprimos

    Para a base 7, entre 2 e 10^5 existem 73 pseudoprimos

Questão 7.
* a. Sabendo que os únicos números de Carmichael até 10.000 são 561, 1105, 1729, 2465, 2821, 6601 e 8911, escreva um algoritmo que responda corretamente se um número natural n dado como entrada, com 1 < n ≤ 10.000, é um número primo ou composto. Seu algoritmo deve ser baseado no Teste de Fermat e não precisa ser muito eficiente, mas não deve testar se o número é primo apenas pela definição, nem implementar um crivo, nem testar exaustivamente usando a lista de primos dada na Questão 6, etc.

    Precisamos,primeiramente, verificar se n está entre 1 e 1000. Então:

    Se ele estiver na lista de números de Carmichael, ele é composto:

    Senão, testar 2<=b<=n-1 para b^n ≡ b mod(n), se b^n ≡/≡ b mod(n), então é composto

Se não satisfazer nenhum dos passos anteriores, então ele é primo

* b. Implemente seu algoritmo em Python.

Questão 8.
 * a. Prove que, para todo natural $n \geq 1$, se $p1, p2, \ldots, pn$ são naturais primos distintos então para todos inteiros x, y temos:

$x \equiv y \pmod{p1 \cdot p2 \cdots pn}$
sse
para todo $i \leq n$ temos $x \equiv y \pmod{pi}$
(Dica: indução.)

1) $x \equiv y \pmod{p1 \cdot p2 \cdots pn} \rightarrow \forall i <= n, x \equiv y \pmod{pi}$
   Pela definição temos que:
   $x-y = (p1 \cdot p2 \cdots pn)K$
   Colocando algum pi, de i<n, em evidência vamos ter:
   x- y= pi(q),onde (q) é o produtório multiplicado por K, mas sem o pi, que é exatamente o que $\forall i <= n, x \equiv y \pmod{pi}$ quer dizer

2) $\forall i <= n, x \equiv y \pmod{pi} \rightarrow x \equiv y \pmod{p1 \cdot p2 \cdots pn}$

   Caso base:
   $x \equiv y \pmod{pi} \rightarrow x \equiv y \pmod{pi}$

   Passo indutivo:
   P(k)
   /\
   \/
   $x \equiv y \pmod{pk} \rightarrow x \equiv y \pmod{p1 \cdot p2 \cdots pk}$
   /\
   \/
   $x-y = (\text{mod } p1 \cdot p2 \cdots pk)(q)$
   /\
   \/
   $p1 \cdot p2 \cdots pk \mid x-y$ |
   /\ |----------> Como o mdc $(p1 \cdot p2 \cdots pk, pk+1) = 1$
   \/ | Temos que $(pk+1)(p1 \cdot p2 \cdots pk) \mid x-y$, logo
   $pk+1 \mid x-y$ | $x \equiv y \pmod{p1 \cdot p2 \cdots pk+1}$
   /\
   \/
   $x-y = (pk+1)(q')$
   /\
   \/
   $x \equiv y \pmod{pk+1} \rightarrow x \equiv y \pmod{p1 \cdot p2 \cdots pk+1}$
   /\
   \/

P(k)

* b. Mostre que a hipótese de que os primos p1, . . . pn são distintos é importante: encontre algum contraexemplo para o falso teorema: “Para todo natural $n \geq 1$, se p1, p2, . . . , pn são naturais primos então para todos inteiros x, y temos:

$x \equiv y$ (mod p1 · p2 · · · pn)
sse
para todo $i \leq n$ temos $x \equiv y$ (mod pi)

Se tivermos p1=2, p2=2 e p3=3
então
6≡0 mod2
6≡0 mod3

entretanto 6≡/≡0 mod 12, logo ∀i<= n, $x \equiv y$ (mod pi) → $x \equiv y$ (mod p1 · p2 · · · pn) é falsa

* e. Mostre que, para todo natural $n \geq 0$, $n(n + 1)(2n + 1)$ é divisível por 6 usando o Teorema de Fermat e o Teorema do item a.

$n(n + 1)(2n + 1) \equiv (n^2+n)(2n+1) \equiv 2n^3+n^2+2n^2+n \equiv 2n^3+3n^2+n$ mod(6), logo queremos mostrar que:
$2n^3+3n^2+n \equiv 0$ mod(6),
temos que 6 = 2*3,então
$2n^3+3n^2+n \equiv 2n \equiv 0$ mod(2)
$2n^3+3n^2+n \equiv 2n^3+n \equiv 2n+n \equiv 3n \equiv 0$ mod 3
logo $2n^3+3n^2+n \equiv 0$ mod(6)

Questão 15. O objetivo desta questão é dar uma demonstração do teorema de Fermat, devida a L. Euler, e que não usa indução. Seja p um primo e a um elemento de Up = Zp \ {0} (Up é o conjunto com todas as classes de Zp que tem inverso multiplicativo). Considere o subconjunto S = {a, 2a, 3a, . . . ,(p − 1)a} de Up.

* a. Mostre que os elementos de S são todos distintos e conclua que S = U(p).

Assumindo que <u>ka</u> e <u>ma</u> pertencem a S, para chegaremos em uma contradição vamos assumir que eles são iguais, <u>ka</u> = <u>ma.</u>
Sabemos que a é inversível em Zp, pois o mdc(a,p) = 1, então vamos multiplicar pelo inverso de a, no qual chamamos de “α”:
<u>k</u>*<u>a</u>*<u>(α)</u> = <u>m</u>*<u>a</u>*<u>(α)</u>
Como <u>a</u> e <u>(α)</u> são inversos, temos que <u>a</u>*<u>(α)</u> = 1, logo:
<u>k</u> = <u>m</u>
Chegamos então que k-m = pq, que é uma contradição, visto que k e m <= p-1.

Como todos os elementos são diferentes, S possui (p-1) elementos, mas como S é subconjunto de Up, no qual também possui (p-1) elementos. Logo S = Up

* b. Mostre que o produto de todos os elementos de S é igual a (p − 1)! = 1 · 2 · · · p − 1.

Sendo os elementos de Up = { 1,2, …. , p-1}
Logo o produto dos elementos de Up, será p-1!
Como vimos na letra a) que S=Up, então temos que o produto de todos os elementos de S também é igual a (p-1)!

* c. Mas, diretamente pela definição de S, o produto dos elementos de S pode ser escrito de outra forma. Encontre essa forma e prove o teorema de Fermat. (Dica: em algum momento você deve precisar argumentar que (p − 1)! é invertível em Zp.)

Pelo raciocínio da letra b) sabemos que:
O produto de elementos de S é igual a (p-1)!
Onde também pode ser escrito como: a * $\underline{2a}$ * $\underline{3a}$ * . . . * $\underline{(p-1)a}$,onde por algebrismo, chegamos em: $\underline{a}$^(p-1) * $\underline{(p-1)!}$

Temos que (p-1)! é igual $\underline{a}$^(p-1) * $\underline{(p-1)!}$

Sabemos que (p-1)! = (p-1) * (p-2) * …* 2 * 1
Podemos dizer que o mdc(p,(p-1)!) = 1, pois p não é um fator de (p-1)!

Dividindo então tudo por (p-1)!, chegamos em $\underline{a}$^p-1 = 1
Logo a^p-q ≡ 1 (mod p), se se assemelha com o PTF

*Questão 16. Seja p um número primo e a um inteiro que não é divisível por p. Mostre que o inverso de a em Zp é a p−2

Como p é primo e a não é divisível por p, temos que mdc(p,a) = 1
Sabemos pelo PTF2: ā^(p -1) = 1 mod (p), por algebrismo chegamos em:
ā*ā^(p - 2) ≡ 1 mod p
Logo concluímos que ā^(p - 2) é o inverso de ā