P2 2017.1

1- Inverso multiplicativo → O inverso de um número a, é o número b, que, multiplicado por a, gera a identidade multiplicativa (elemento neutro). Quando o inverso de a é único, pode ser representado por 1/a (a^{-1}).

Ordem de um elemento $\bar{a} \in \mathbb{Z}_n$ → é o menor inteiro positivo K, tal que $a^K \equiv 1 \pmod{n}$. Somente os elementos de $U(n)$ possuem ordem. Seja t um múltiplo de K, $t = K \cdot l$

$$a^t = a^{K \cdot l} = (a^K)^l = 1^l \equiv 1 \pmod{n}$$

portanto $a^t \equiv 1 \pmod{n}$

* $U(n)$ → conjunto dos elementos de $\mathbb{Z}_n$ que possuem inverso multiplicativo

(1) Um elemento $\bar{a} \in \mathbb{Z}_n$, possui inverso em $\mathbb{Z}_n$

(2) $mdc(a, n) = 1$

(3) Um elemento $\bar{a} \in \mathbb{Z}_n$, possui ordem em $\mathbb{Z}_n$

teorema da inversão modular (teorema da divisão)

(1) → (2)

Se $mdc(a, n) = 1$, pelo AEE, existe α e β tq $\alpha \cdot a + \beta \cdot m = 1$

$\alpha \cdot a - 1 = m \cdot (-\beta)$ ↔ m divide $\alpha \cdot a - 1$

Logo → $\alpha \cdot a \equiv 1 \pmod{n}$

Isso prova que $\bar{a}$ tem inverso em $\mathbb{Z}_n$, e esse inverso é α

(2) → (1)

Sendo a^{-1} o inverso de a

$a \cdot a^{-1} \equiv 1 \pmod{n}$

$a \cdot a^{-1} - 1 = K \cdot n$

$a \cdot a^{-1} - Kn = 1$

Como $d = mdc(a, n) = 1$ → $d(a \cdot a^{-1} - Kn) = 1$

Logo d divide 1, portanto $d = 1$

(1) → (3)

Supondo que $\bar{a}$ possui inverso em $\mathbb{Z}_n$.

Consideremos a sequência de potências $a, a^2, a^3 \dots$ reduzidas módulo n.

Suponha, por contradição, que nenhuma é congruente à 1 módulo n.

Como $\mathbb{Z}_n$ é um conjunto finito, essa sequência não pode conter para sempre valores distintos entre si.

Em algum momento, para algum inteiro positivo l, o valor de $a^l \bmod n$, será igual ao de uma potência anterior $a^m \bmod n$, com $m < l$.

Logo $a^{l} \equiv a^{m} \pmod{n}$

Seja α, o inverso de a

Multiplicamos ambos os lados por $\alpha^{m} \leftrightarrow a^{l}\alpha^{m} \equiv a^{m}\alpha^{m} \pmod{n}$

que pode ser escrito como $a^{l-m} \equiv 1 \pmod{n}$, que é

contradição com a hipótese anterior que nenhuma potência de

a é congruente a 1

3) → 1) Supondo que existe um K tal que $a^{K} \equiv 1 \pmod{n}$

o que significa que a^{K-1} é o inverso

$a \cdot a^{K-1} \equiv 1 \pmod{n}$, o que significa que

multiplicativo de a módulo n

2- Calcular da forma mais eficiente $*^{***}$ mod 191

* Ilegível na foto

191 é primo, poderia aplicar Fermat e depois potenciação modular

Por Miller-Rabin: $n = 191$ $\quad a^{q} \equiv \pmod{191}$

$n-1 = 2^{1} \cdot 95$ $\quad 2^{95} \equiv \pmod{191}$

R	a	e	ímpar?
1	2	95	S
2	4	47	S
8	16	23	S
128	65	11	S
107	23	5	S
169	147	2	N
169	26	1	S
1	103	0	N

Resultado foi igual a 1 (inconclusivo), porém é sabido que o menor número de Carmichael é 561, portanto 191 é primo.

3- a) Após obter K e q ($n-1 = 2^{K} \cdot q$), e calcular a sequência de potências $a^{2^{i}q}$ (reduzidas a módulo n), se a primeira potência for diferente de 1 e $n-1$, e as demais potências forem diferentes de $n-1$, então n com certeza é composto.

Se n é ímpar, $n-1$ é par, assim podemos escrever $n-1 = 2^{K} \cdot q$, com $K \geq 1$

Supondo que n seja primo, e b um inteiro tq $2 \leq b \leq n-1$, então pelo teorema de Fermat $b^{n-1} \equiv 1 \pmod{n}$

Logo $1 \equiv b^{n-1} \equiv b^{2^{K}q} \pmod{p}$

Digitalizado com CamScanner

Isso significa que n divide $b^{2^k q} - 1$.
Como $k \geq 1$, então $b^{2^k q} - 1$ é uma diferença de dois quadrados
$b^{2^k q}$ é o quadrado de $b^{2^{k-1} q}$, e 1 é quadrado de si mesmo
Podemos então escrever $b^{2^k q} - 1$ como:

$$(b^{2^{k-1}} q + 1)(b^{2^{k-1}} q - 1)$$

Como n é primo e divide $b^{2^k q} - 1$, ele deve dividir um dos termos acima.

Passar de k para $k-1$
$j \leq k$

Assim $\to$ $b^{2^{k-1} q} \equiv -1 \pmod{n}$
ou
$b^{2^{k-1} q} \equiv 1 \pmod{n}$

No segundo caso, temos uma congruência semelhante à original.
Assim, denotamos j o menor expoente tq $b^{2^j q} \equiv 1 \pmod{n}$

Se $j = 0 \to b^q \equiv 1 \pmod{n}$
Porém, se $j \geq 1$, podemos repetir o raciocínio da diferença de quadrados. $\to b^{2^j q} - 1 = (b^{2^{j-1} q} + 1)(b^{2^{j-1} q} - 1)$
Entretanto, agora, o segundo caso já não é mais possível.
Se n dividisse $(b^{2^{j-1} q} - 1)$, teríamos $b^{2^{j-1} q} \equiv 1 \pmod{n}$, que é contradição com nossa escolha de j como menor expoente tq $b^{2^j q} \equiv 1 \pmod{n}$. Logo, obrigatoriamente:

$$b^{2^{j-1} q} \equiv -1 \pmod{n}$$

Recapitulando que $b^q \equiv 1 \pmod{n}$ e $b^{2^i q} \equiv -1 \pmod{n}$
Se temos um b tq $2 \leq b \leq n-1$ tq $b^q \not\equiv 1 \pmod{n}$
e $\forall i$ em $0 \leq i \leq k-1$, $b^{2^i q} \not\equiv -1 \pmod{n}$, se n fosse primo, estes resultados contradizem o resultado anterior.
Neste caso, n é composto

b) $n = 2465$ $\quad a = 3$
$n - 1 = 2^5 \cdot 77$

$b^q \not\equiv 1 \bmod n$
$b^{2^i q} \not\equiv -1 \bmod n$

$a^q \equiv 3^{77} \equiv 2018 \pmod{2465}$
$a^{2q} \equiv 3^{154} \equiv 2018^2 \equiv 144 \bmod 2465$
$a^{2^2 q} \equiv 3^{308} \equiv 144^2 \equiv 1016 \bmod 2465$
$a^{2^3 q} \equiv 3^{616} \equiv 1016^2 \equiv 1886 \bmod 2465$
$a^{2^4 q} \equiv 3^{1232} \equiv 1886^2 \equiv 1 \bmod 2465$

R	a	e	ímpar?
1	3	77	S
3	9	38	N
3	81	19	S
243	1631	9	S
1933	426	4	N
1933	1531	2	N
1933	2211	1	S
2018	426	0	//

Como nenhuma das condições do teste foram satisfeitas, n é composto

c) Não é pseudoprimo forte, pois o resultado é diferente de 1 e n-1. (base 3)

Pelo teorema de Korselt, um ímpar composto é um número de Carmichael quando cada um de seus fatores primos satisfaz:

→ p^2 não divide n
→ $p-1$ divide $n-1$

Como $n = 2465$
$n = 5 \cdot 17 \cdot 29$

5^2 não divide 2465 ; 4 divide 2464
17^2 não divide 2465 ; 16 divide 2464
29^2 não divide 2465 ; 28 divide 2464

Logo, 2465 é um número de Carmichael

4- a) Determinar $*^{***}$ mod 3171

3171 é composto → $3 \cdot 7 \cdot 151$ → Fatoração Miller-Rabin

Calculemos:

$x = *^{**} \bmod 3$
$y = *^{**} \bmod 7$
$z = *^{**} \bmod 151$

Aplica Fermat (Potência modular)
O resultado é colocado num sistema de congruências

Achar t:

$$\begin{cases} t \equiv x \pmod 3 \\ t \equiv y \pmod 7 \\ t \equiv z \pmod{151} \end{cases}$$

→ Substituições sucessivas

b)
```
def main():
    n = input()
    for i in range(n):
        l1, l2 = input()
        alfa, beta = aee(l2[0], l2[1])
        print alfa, beta
```

→

```
mod= l2[0]*l2[1]
X=( (l1[0]*beta*l2[1]) + (l1[1]*alfa*l2[0]))%mod
print x,mod

i=2
while (i<len(l2)):
      alfa,beta = ae(mod,l2[i])
      print alfa,beta
      mod_ori = mod
      mod*=l2[i]
      X=( (X*beta*l2[i]) + (l1[i]*alfa*mod_ori))%mod
     print x,mod
      i+=1
print '---'

def ae (a,b):
    x1=y2=alfa=1
    x2=y1=beta=0
    print a,'-',x1,y1
    print b,'-',x2,y2
    resto = a%b
    div = a//b
    temp=b
    while (resto!=0):
          alfa = x1-(x2*div)
          beta = y1-(y2*div)
          print resto,div,alfa,beta
          a=temp
          b=resto
         resto=a%b
          div = a//b
          temp=b
          X1=X2
          Y1=Y2
          x2=alfa
          Y2=beta
   print resto,div,'- -'
   return alfa,beta
```