PRÀCTICA DE MATEMÀTICA DISCRETA

María del Mar Cardona Aranda

Les expressions que trobam en negreta al desenvolupament de l'exercici és el codi emprat a Sage.

1. **Pregunta:** Els alumnes de primer d'informàtica son 78 homes, i 75 dones. De quantes maneres es pot formar un grup de 67 membres si en aquest hi ha d'haver més homes que dones?.

Com bé diu l'enunciat hi ha d'haver més homes que dones, el que vol dir que n'hi ha d'haver com a màxim 67 homes (el grup estarà format totalment per homes) i el mínim l'hem de calcular. Per calcular-ho empram el principi del colomar on n = 67 persones i k=2 grups (homes i dones).

Aquest principi consisteix en fer l'operació n / k i si el resultat dóna un nombre sencer el deixam tal com està però, si el resultat no és sencer el que hem de fer és arrodonir-lo cap amunt (fer el nombre més gran) per aconseguir un nombre sencer.

Calculam: n / k = 67 / 2 = 33,5 —> 34. Per tant l'interval d'homes que pot haver és [34,67] i n'hi haurà per tant [0,33] dones.

```
i=34
cont = (factorial(78) / (factorial (i) * factorial (67-i))) * (factorial(75) / (factorial(67-i) * factorial(75-(67-i))))
while i<68:
   print cont
   i+=1
```

cont és la el producte de les combinacions que hi ha d'entre 78 homes agafar ***i*** homes per les combinacions que hi ha d'entre 75 dones agafar-ne ***67-i*** dones on ***i*** és el nombre d'homes que agafam (saben que ***i*** està comprès entre [34,67]) i ***67-i*** és el nombre de dones que agafam (deim ***67-i*** perquè si el grup pot constar de 67 persones i ja hem dit que n'hi haurà ***i*** homes idò agafarem tantes dones com se necessitin per completar el grup i sempre n'hi haurà més homes que dones).

Això que hem calculat amb el *Sage* ens dona una llista de nombres de resultat

- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0

- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0
- 898272646535051444428817912675635009585301090793951148800000 0

3680464335173825701707888385980392598007555653271605398784610402509590572550537774173 81
823426980026635487745092099117999981270282950870547097804026400105495606071964335542720
019516797286635583504551228737793286625608597296414591964819488039775225699291549978160
683766201423281544667079082112278632314736608929652655702828257519831221288677069828203
573342134642819673683733932458217105941874195824604212052643827869984944043239320908063
677073431617010095928570198669296679256064000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000

I aquest és el nombre de maneres que hi ha de formar un grup de 67 persones on n'hi ha d'aver més homes que dones.

---

2. **Pregunta:** El DMI ha comprat 69 llibres nous de Matemàtica Discreta, 69 de Calcul Numèric i 56 d'Anàl·lisi Matemàtic. La bibliotecària vol col·locar-los tots en el mateix prestatge de tal manera que els llibres de la mateixa assignatura vagin junts. Els llibres de la mateixa assignatura son diferents entre ells. De quantes formes pot fer-ho?

El primer és calcular el nombre de maneres que hi ha d'ordenar els tres grups de llibres ja que l'enunciat diu que tots els llibres de la mateixa assignatura vagin junts, per tant, estan agrupats per assignatures.

factorial (3) = 6 maneres

Ara hem de calcular les maneres d'ordenar els 69 llibres de Matemàtica Discreta.

factorial (69) = 171122452428141311372468338881272839092270544893520369393648040923
2572797541406474240000000000000000 maneres.

A més de les maneres d'ordenar els 69 llibres de Càlcul Numèric.

factorial (69) = 171122452428141311372468338881272839092270544893520369393648040923
2572797541406474240000000000000000 maneres.

I les maneres d'ordenar els 56 llibres d'Anàl·lisi Matemàtic.

factorial (56) = 13868311854568983573793901972038940634590287677268743254082129494
0160000000000000 maneres.

Una vegada calculat obtindrem el resultat final que és saber de quàntes maneres podem ordenar 69 llibres nous de Matemàtica Discreta, 69 de Calcul Numèric i 56 d'Anàl·lisi Matemàtic sabent que els de la mateixa assignatura han d'estar junts.

factorial (3) * factorial (69) * factorial (69) * factorial (56) = 124920576511981044907434860067
710442718987054555870834490715745548740345025729701156584681015353334759370665675740185
524864448280386496832818482350411367453607854310390949652717526459244118788261312046585
5555171828317934429038182400000000000000000000000000000000000000000 maneres.

---

3. **Pregunta:** Quants de nombres mes grans que 10^{45} es poden formar amb les xifres següents: un zero, 19 dosos, 12 quatres, i 14 nous?

El nombre 10^{45} s'escriu un 1 al començament i va seguit de 45 zeros. Llavonces, qualsevol nombre que comenci per 1 i vagi seguit de 45 nombres on almenys un de ells és diferent de zero serà major que 10^{45}.
Per tant, com l'exercici ens dona 46 nombres a ordenar de tal forma que obtinguem un nombre major que 10^{45}, ja sabem que el zero a ordenar, per el que hem dit en el paràgraf anterior no pot estar al començament però si que pot haver-hi un 2, un 4 o un 9 al començament.

El que farem serà agafar un nombre inicial i ordenar els 45 nombres restants amb la fòrmula de les permutacions amb repeticions fixades, de tal forma que ja tenim assegurat que el nombre serà major de 10^{45}.

Si el nombre comença per dos:

f**actorial (45) / (factorial (1) * factorial (18) * factorial (12) * factorial(14))** = 447430437543115026000 maneres

Si el nombre comença per 4:

factorial (45) / (factorial (1) * factorial (19) * factorial (11) * factorial (14)) = 282587644764072648000 maneres.

Si el nombre comença per 9:

factorial (45) / (factorial (1) * factorial (19) * factorial (12) * factorial (13)) = 282587644764072648000 maneres.

El resultat final s'obté multiplicant els 3 resultats anteriors.

447430437543115026000 + 282587644764072648000 + 282587644764072648000 = 1012605727071260322000 maneres.

---

4. **Pregunta:** Un director de teatre esta fent un càsting per a cobrir 24 personatges diferents, dels quals 12 han de ser nens i 12 has de ser nenes. Si a les proves hi assisteixen 58 nens i 59 nenes, de quantes formes diferents es poden assignar els personatges?

Hem de calcular les combinacions que hi ha d'entre 58 nens agafar-ne 12.

factorial (58) / (factorial(12) * factorial (58-12)) = 891794789340 combinacions.

I les combinacions que hi ha d'entre 59 nenes agafar-ne 12.
factorial (59) / (factorial(12) * factorial (59-12)) = 1119487075980 combinacions.

I ara les multiplicam per obtenir-ne el resultat.
891794789340 * 1119487075980 = 998352741092436674053200 combinacions.

---

5. **Pregunta:** Codifica el missatge El nom que surt a Campus Extens **: Maria del Mar Cardona Aranda** utilitzant el xifrat RSA havent usat primer la codificació ASCII per blocs de longitud 5, com a primers els dos primers següents al teu DNI (43215599) i com a d 1329495028797739.

Com bé posa l'enunciat hem de començar codificant el nom amb la codificació ASCII per blocs de longitud 5.

```
from sage.crypto.util import ascii_integer
bin = BinaryStrings()
myName = list("Maria del Mar Cardona Aranda")
N = 128 N és el nombre de caràcters que conté la taula ASCII
C = 0
pos = 0
for element in myName:myValue=ascii_integer(list(bin.encoding(element)))
C = C+myValue*N^pos
pos= pos+1
print C
```

c = 767281613380528008069866352987210733100293757940036479674 37 on C és el meu nom codificat en ASCII

Ara per fer-lo amb codificació en RSA primer hem de fer unes passes prèvies. Hem de trobar p i q que són els dos nombres primers tal que $43215599 < p < q$. Primer hem de cercar p per després cercar q. Emprant el Sage n'hi ha una manera de trobar el primer nombre primer i que aquest sigui major que 43215599 i és de la següent manera:

```
43215599.next_prime()
```

p = 43215619

I per trobar q el que hem de fer és quasi el mateix:

```
43215619.next_prime()
```

q = 43215631

```
n = p*q
```

1867590244140589

```
phy_n = (p-1)*(q-1)
```

1867590157709340

phy_n l'emprarem juntament amb *d* per trobar *e* on d és l'invers d'*e* i, a més *phy_n* i *e* són coprims. Això se fa amb l'algorisme d'Euclides estès.

```
def QuocientResidu(a,b):
   q = a//b
   r = a%b
   return [q,r]

def extended_gcd(a,b,prints=false):
   x1=1
   x2=0
   y1=0
   y2=1
   r1=a
   r2=b

   while r2!=0:
      q,r = QuocientResidu(r1,r2)
      r1,r2 = [r2,r]
      x1,x2 = [x2, x1-q*x2]
      y1,y2 = [y2, y1-q*y2]
   if(prints):
      print "Identitat de Bézout: "
```

```
        print str(r1)+" = "+str(a)+"*"+str(x1)+" +"+str(b)+"*"+str(y1)
    return [r1, [x1,y1]]
```

extended_gcd(phy_n,d, prints = “true”)

Identitat de Bézout:
1 = 1867590157709340*608905825459495 +1329495028797739*-855352221684041
[1, [608905825459495, -855352221684041]]

```
e = -855352221684041;
while e < 0:
    e = e + phy_n;
print e
```

e = 1012237936025299

Ara que tenim e, comprovarem que és correcte:

(e * d) % phy_n
1

Com el resultat de l’operació anterior és 1 vol dir que el procediment és correcte. Llavonces hem de cercar *kp* i *ks* on *kp* és l’anomenada clau pública i *ks* és la clau privada.

```
kp = [n, e]; print kp
ks = [n, d]; print ks
```

[1867590244140589, 1012237936025299]
[1867590244140589, 1329495028797739]

Finalment hem de fer el darrer pas per codificar que és:

((C % n) ^ e) % n

Aquest resultat és massa gros com per a calcular-lo. Aquest és el missatge del Sage:
python(11636,0x7fff79a3a300) malloc: ***
mach_vm_map(size=6326487100162048) failed (error code=3)
*** error: can't allocate region
*** set a breakpoint in malloc_error_break to debug
Traceback (click to the left of this block for traceback)
…
MemoryError: failed to allocate 6326487100158144 bytes