(version dimanche 14 janvier 2007 : 12h14)

L'épigramme qui suit a été découverte (sous la forme d'un poême de 32 distiques : groupe de paires de vers) par GOTTHOLD EPHREIM LESSING, alors conservateur de la bibliothèque Wolfenbüttel, et publiée par lui en 1773. *(APM 358+ Dorrie p5).*

Épigramme adressée, selon les anciens, par ARCHIMÈDE (Syracuse 287 av. J.-C. 212 av. J.-C.) à son ami ERATOSTHÈNE de CYRÈNE (Cyrène 276 av. J.-C., Alexandrie 194 av. J.-C.)-auteur du crible- ((Troisième siècle avant notre ère). *(traduction du grec, par Paul VER EECKE, Itard p 101).*

AMI, si tu as la sagesse en partage, apporte grand soin à calculer à combien s'élevait la multitude des bœufs du SOLEIL qui, jadis dans les plaines de l'île de la SICILE THRINACIENNE *(n.d.t. nom que donnèrent les grecs au 7-ième siècle Avant J.-C. : Τρινακρια, "aux trois sommets", (à cause des trois promontoires) nom rencontré chez THÉOCRITE poête du 3-ème siècle avant J.-C., Trinacria, Trinacrie, au "pays en forme de triangle")*, paissaient, répartis en quatre troupeaux de couleur différentes, l'un blanc de lait, l'autre d'un noir luisant, le troisième brun et le quatrième tavelé. Il y avait dans chaque troupeau un nombre considérable de taureaux répartis dans les proportions suivantes : imagine, mon ami, que les blancs étaient en nombre égal à la moitié augmentée du tiers des taureaux noirs, et augmentée de tous les bruns, tandis que les noirs étaient en nombre égal aux quatrième et cinquième parties des tavelés, accrues de tous les bruns. Considère d'autre part, que les tavelés restants, étaient en nombre égal aux sixième et septième parties des blancs, accrues de tous les bruns. Les vaches étaient réparties de la manière suivante : les blanches étaient en nombre précisément égal aux troisième et quatrième parties de tout le troupeau noir, tandis que les noires étaient de nouveau en nombre égal aux quatrième et cinquième parties des tavelées qui étaient toutes venues paître en compagnies des taureaux. Les tavelées étaient, d'autre part, en nombre égal aux cinquième et sixième parties de tout le troupeau brun, tandis que les brunes étaient en nombre égal à la moitié de la troisième partie accrue de la septième partie du troupeau blanc.

AMI, si tu me dis exactement combien il y avait de bœufs du SOLEIL, quel était en particulier le nombre des taureaux gras et en particulier le nombre des vaches pour chacune des couleurs, on ne te qualifiera ni d'ignorant ni de malhabile en matière de nombres ; mais tu ne pourras cependant pas encore compter parmi les savants. Dès lors, observe encore les diverses manières dont les bœufs du SOLEIL étaient disposés : lorsque les taureaux blancs joignaient leur multitude aux noirs, ils se maintenaient en un groupe compact ayant la même mesure en profondeur qu'en largeur, et ce carré remplissait entièrement les immenses plaines de la THRINACIE. D'autre part, les bruns et les tavelés réunis, sans que les taureaux d'autres couleurs fussent présents ou sans qu'ils manquassent, étaient groupés de telle sorte que, le premier rang était constitué par un seul, ils formaient graduellement une figure triangulaire.

AMI, si tu trouves toutes ces choses de pair, et si, en un mot, concentrant tes esprits, tu exprimes toutes les mesures de ces multitudes, va, te glorifiant d'avoir remporté la victoire, et persuadé que l'on te juge complètement consommé dans cette science.

W(HITE),X,Y,Z, représentant respectivement les nombres des bœufs blancs, noirs, tavelés et bruns et w,x,y,z les nombres des vaches de même couleur, voici sous forme moderne le système proposé :

(1) $\mathbf{W=(\frac{1}{2}+\frac{1}{3})X+Z}$ **(2)** $\mathbf{X=(\frac{1}{4}+\frac{1}{5})Y+Z}$
(3) $\mathbf{Y=(\frac{1}{6}+\frac{1}{7})W+Z}$ **(4)** $\mathbf{w=(\frac{1}{3}+\frac{1}{4})(X+x)}$
(5) $\mathbf{x=(\frac{1}{4}+\frac{1}{5})(Y+y)}$ **(6)** $\mathbf{y=(\frac{1}{5}+\frac{1}{6})(Z+z)}$
(7) $\mathbf{z=(\frac{1}{6}+\frac{1}{7})(W+w)}$
(8) $\mathbf{W+X=c^2}$ **(un nombre carré)** *(c=m de Gomez)*
(9) $\mathbf{Y+Z=\frac{t(t+1)}{2}=1+2+....+t}$ **(un nombre triangulaire)** *(t=n de Gomez)*

1) RÉSOLVONS, avec l'aide de Maple, le système (1) (2) (3) (4) (5) (6) (7). Ce système est un système linéaire et homogène de 7 équations à 8 inconnues, il est de rang 7, il y a donc une inconnue secondaire.

En écrivant sous Maple $systeme\_bovins := \{W=\frac{5}{6}X+Z, X=\frac{9}{20}Y+Z, Y=\frac{13}{42}W+Z, w=\frac{7}{12}X+\frac{7}{12}x, x=\frac{9}{20}Y+\frac{9}{20}y, y=\frac{11}{30}Z+\frac{11}{30}z, z=\frac{13}{42}W+\frac{13}{42}w\}$; et $S := solve(systeme\_bovins, \{W,X,Y,Z,w,w,y,z\})$; on obtient en 5 centièmes de seconde :

$S := \{x=\frac{815541}{585970}y, z=\frac{1813071}{1171940}y, w=\frac{17158}{8371}y, W=\frac{246821}{83710}y, Z=\frac{125739}{106540}y, Y=\frac{367903}{175791}y, X=\frac{1243419}{585970}y, y=y\}$.

2) MAIS solve n'ordonne pas lexicographiquement les identificateurs des indéterminées, ce que nous allons faire : $with(linalg) : V := vector(subs(S,[W,X,Y,Z,w,x,y,z]))$; donne :

$\left[\frac{246821}{83710}y, \frac{1243419}{585970}y, \frac{367903}{175791}y, \frac{125739}{106540}y, \frac{17158}{8371}y, \frac{815541}{585970}y, y, \frac{1813071}{1171940}y\right]$.

Pour dissocier les solutions, je dédouble les identificateurs, car écrire par exemple $W := V[1]$ est interdit *(Il est pourtant interdit d'interdire ?)* parce que W est protégé en Maple à cause de la fonction de Lambert. Mais auparavant à l'aide du PPCM des dénominateurs, je cherche le changement de variable le mieux adapté pour y :

$ilcm(83710, 585970, 175791, 106540, 1171940)$; donne 3515820.

Alors les commandes : $y := 3515820 * k; WW := V[1]; XX := V[2]; YY := V[3]; ZZ := V[4]; ww := V[5]; xx := V[6]; zz := V[8];$ donnent immédiatement :

$$\begin{cases} y = 3515820 * k \\ WW := 10366482 * k \\ XX := 7460514 * k \\ YY := 7358060 * k \\ ZZ := 4149387 * k \\ ww := 7206360 * k \\ xx := 4893246 * k \\ zz := 5439213 * k \end{cases}$$

---

3) La condition (8) du système est $W+X = c^2$: On calcule donc $WW+XX; ifactor(op(1, \%);$ soit $17826996*k$ et $(2)^2(3)(11)(29)(4657)$;

La condition (8) est donc $17826996 * k = c^2$

Nous avions anticipé par le ifactor, car il faut maintenant que k complète les facteurs non carrés de la décomposition de 17826996.

Il faut donc prendre $\boxed{\mathbf{k := 3 * 11 * 29 * 4657 * v^2 = (957) * (4657)v^2 = 4456749v^2}}$

---

4) La condition (9) exprime que $Y + Z$ est un nombre triangulaire. On calcule donc $somme := YY + ZZ;$ ce qui donne $somme := 51285802909803v^2 = \frac{t(t+1)}{2}$.

Comme $4t(t + 1) + 1 = (2t + 1)^2$, on pose $\boxed{\mathbf{U=2t+1}}$.

$8 * somme;$ soit $410286423278424 * v^2 = 4t(t + 1) = 4t^2 + 4t = (2t + 1)^2 - 1 = U^2 - 1$

Pour simplifier *(sinon les coefficients de l'équation de Pell seraient trop grands et la solution fondamentale plus difficile à trouver)* l'équation finale, on factorise le facteur de v^2, par $(ifactor(410286423278424);$ ce qui donne $410286423278424 = (2)^3(3)(7)(11)(29)(353)(4657)^2 = (2 * 4657)^2 * (2 * 3 * 7 * 11 * 29 * 353) = (9314)^2 * (4729494)$.

On pose alors $\boxed{\mathbf{V=2*4657*v=9314*v}}$ et on obtient l'équation du type PELL-FERMAT :

$\boxed{\mathbf{1 = U^2 - V^2 * (4729494)}}$.

Notons qu'il faudra bien faire attention qu'une solution V (s'il en existe) pour être acceptable doit être paire et divisible par 4657. De plus s'il y a existence, quel est l'ensemble des solutions ? 2200 ans après Archimède, son problème est encore intéressant !

---

5) Résolvons l'équation de PELL-FERMAT obtenue : Maple heureusement nous gagne du temps, car il fait le calcul en 6 dixièmes de seconde.

$restart : with(numbertheory) : d := 4729494 :$

$S := [isolve(u^2 - d * v^2 = 1, n)];$ La lettre n est utilisée pour le paramètre de sortie puissance.

$S := eval(subs(n = 1, S[1])) : U_0 := subs(S, u); V_0 := subs(S, v);$

Ce qui donne :

U_0=1099319867328297349798662328214335439010880 49	V_0=505494852343150330744778197355404089863 40

On rappele dans l'encadré ci-dessous un peu de théorie sur l'équation de Pell-Fermat :

Rappel de la théorie de recherche de la plus petite solution de l'équation de PELL-FERMAT : la théorie des fractions continues permet (voir Descombes p43-44, Parent p263, Chapelon, **Ivan Ninen an introduction to the theory of Numbers 5ème édition chez Wiley p 353**, *TP info Pascal 94-95 /travail inffermat.tex (avec bibliographie renforcée sur PELL-FERMAT) b: pelferma.pas) de trouver la plus petite solution > 1 : le développement en FRACTION CONTINUE de $\sqrt{d}$ est périodique : si on écrit $\sqrt{d} = (a_0, a_1, ..)$ la période T est le plus petit entier tel que* $\boxed{\mathbf{a_T = 2a_0}}$, *on rappelle que $a_0 = [\sqrt{d}]$. Si on note $\frac{p_n}{q_n}$ la réduite d'ordre n de $\sqrt{d}$ alors si T est PAIR les solutions positives sont $U = p_{nT-1}, V = q_{nT-1}$, la plus petite pour $n = 1$, et si T est IMPAIR les solutions positives sont $U = p_{2nT-1}, V = q_{2nT-1}$ et donc la plus petite est obtenue pour $n = 1$.*

En Maple :

with(numtheory); (package qui contient isolve et issqrfree ; st:=time(): for d from 4729494 to 4729494 do if issqrfree(d) then S:=[isolve($u^2 - dv^2 = 1, x$)]; (la lettre x est utilisée pour le paramètre de sortie puissance ; S:=eval(subs(x=1,S[1])); N:=subs(S,u); P:=subs(S,v); print('d=',d,'N=',N,'P=',P); fi; od; temps(time()-st);

Maple donne (on vient de le voir ci-dessus de manière plus concise) :

U_0=109 931 986 732 829 734 979 866 232 821 433 543 901 088 049 et

V_0=50 549 485 234 315 033 074 477 819 735 540 408 986 340 ;

6) Mais il ne faut pas oublier que V_0 n'est pas la solution attendue pour V, car celle ci doit être divisible par 9314. Or la théorie de l'équation de PELL $U^2 - dV^2 = 1$ dit que : $U + V\sqrt{d} = (U_0 + V_0\sqrt{d})^n$: Ce qui par la formule du développement du binôme de NEWTON, et identifiant les coefficients en $\sqrt{d}$ des deux membres donne : $U = \sum_{p=0}^{2p\leq n} C_n^{2p} V_0^{2p} d^p U_0^{n-2p}$ et $\boxed{\mathbf{V = V_0 \sum_{p=0}^{2p+1\leq n} C_n^{2p+1} V_0^{2p} d^p U_0^{n-2p-1}} \text{ (p indice muet)}}$

On veut ici, compte tenu des calculs précédents, que n soit un entier convenable tel que V soit pair et divisible par 2*4657=9314.

La divisibilité par 2 est assurée parce que V_0 est pair. On pose $\boxed{\mathbf{p= 4657 ; p \text{ est premier}}}$.

- $\boxed{\mathbf{Un\ peu\ de\ théorie}}$ (voir le Mini cours flash sur les corps finis, dans la page suivante).

On sait que **p=4657** est premier (table ou vérification par isprime de Maple). la vérification maple msqrt(d,p) permet de vérifier que d n'est pas un carré dans F_p ; on peut le vérifier aussi par le point (6) du mini cours flash donné dans l'annexe, en calculant $d^{\frac{p-1}{2}}$ modulo p, on constate qu'il est -1 ; Mais d'après le point (7) il l'est dans F_{p^2}. $(U_0 + V_0\sqrt{d})^n$ n'est pas dans F_p (p est la caractéristique du corps F_p), mais dans F_{p^2} ; Comme on veut que V *(que l'on sait aussi d'après PELL-FERMAT, être égal à* $\frac{(U_0+V_0\sqrt{d})^n-(U_0-V_0\sqrt{d})^n}{2\sqrt{d}}$*)* soit nul modulo p, il faut et il suffit que $(U_0 + V_0\sqrt{d})^n - (U_0 - V_0\sqrt{d})^n = 0$ dans F_{p^2}, c'est à dire que $\left(\frac{(U_0+V_0\sqrt{d})}{(U_0-V_0\sqrt{d})}\right)^n = 1$ dans F_{p^2} ; on veut donc trouver le plus petit $n > 0$ tel que $(U_0 + V_0\sqrt{d})^{2n} = 1$ modulo p^2. *(car* $\frac{1}{U_0-V_0\sqrt{d}} = \frac{U_0+V_0\sqrt{d}}{U_0^2-V_0^2 d} = \frac{U_0+V_0\sqrt{d}}{1}$*).* Or par le théorème de LAGRANGE, l'ordre d'un sous groupe divise l'ordre du groupe *(Grâce à la partition en classes par la relation d'équivalence $xRy \Leftrightarrow x - y \in g$: card(classes)*card(g)=card(G)).* n qui doit être l'ordre du sous groupe de F_{p^2} engendré par $(U_0 + V_0\sqrt{d})^2$, doit diviser $p^2 - 1$ sans diviser p-1, (puisque $(U_0 + V_0\sqrt{d})^2$ n'est pas dans F_p*). Or $p^2 - 1 = (p+1)(p-1)$ et le seul facteur commun possible à p+1 et p-1, doit diviser leur différence p+1-(p-1)=2 ; Donc l'ordre cherché doit être un diviseur impair de p+1=4657+1=4658=2*17*137. Ce ne peut donc être que 17, 137, et 2329=17*137 : il suffit de les essayer ;

Pour cela, on fait deux procédures en MAPLE : l'une "produit" qui permet de calculer, modulo p, $ab = (a[1] + a[2]\sqrt{d}) * (b[1] + b[2]\sqrt{d}) = a[1] * b[1] + d * a[2] * b[2] + \sqrt{d} * (a[1] * b[2] + a[2] * b[1])$, puis une autre qui permet de décider quelle est la valeur de n, qu'il faut choisir.

La procédure "produit" est :

produit:=$(a, b) -> [(a[1] * b[1] + d * a[2] * b[2]) modp, (a[1] * b[2] + a[2] * b[1]) modp]$;

puissance := proc(a,k) local b,c ; if k=0 then $[1, 0]$ else if k=1 then a else b := puissance(a,iquo(k,2)) ; c:= produit(b,b) ; if irem(k,2)=1 then c:= produit(a,c) fi; c; fi fi; end:

On énumére les diviseurs de p+1 ; p étant comme dans la théorie le nombre premier p=4657 : (div := sort (divisors (p+1),list));).

a := puissance($[N_0$ mod p, P_0 mod $p], 2]$; i:='i'; for i in op(div) while(evalb(puissance(a,i) <> $[1, 0]$)) do od; i; (evalb = évaluation booléenne) ; On trouve *a* := $[262, 551]$; et i=2329 ;

Le plus petit n qui convient est : 2329

Mais par la même occasion, tous les n qui sont tels que V_n est divisible par par 9314, sont de la forme

n=2329 s avec s entier ≥ 1

On a alors $U+V\sqrt{d}=(U_0+V_0\sqrt{d})^{2329}$ donc $V=\frac{(U_0+V_0\sqrt{d})^{2329}-(U_0-V_0\sqrt{d})^{2329}}{2\sqrt{d}}$.

Or 2329 a justement été calculé pour que V soit divisible par 9314 et avec les notations de **4)** on a $V=9314v$ donc $v=\frac{(U_0+V_0\sqrt{d})^{2329}-(U_0-V_0\sqrt{d})^{2329}}{9314*2\sqrt{d}}$.

Il suffit de remplacer 2329 par $2329s$ pour avoir toutes les solutions v_s convenant. Nous rappelons qu'ici **d=4729494**

et enfin $\mathbf{k=4456749*v^2=\frac{3*11*29}{4657}\Big[\frac{(U_0+V_0\sqrt{d})^{2329}-(U_0-V_0\sqrt{d})^{2329}}{4\sqrt{d}}\Big]^2=\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{4658}+\frac{1}{\varepsilon_0^{4658}}-2\Big]}$ où

l'on a posé $\boxed{\varepsilon_0=U_0+V_0\sqrt{d}}$

Dans le cas général

$$\mathbf{k_s=4456749*v_s^2=\frac{3*11*29}{4657}\Big[\frac{(U_0+V_0\sqrt{d})^{2329s}-(U_0-V_0\sqrt{d})^{2329s}}{4\sqrt{d}}\Big]^2=\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{2329s}+\frac{1}{\varepsilon_0^{2329s}}-2\Big]}$$

Ainsi la solution générale au problème du troupeau du Soleil d'Archimède est donnée par :

$$\begin{cases}
W_s:=10366482*k_s=10366482*\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\frac{159}{5648}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\mathbf{Ent}\big(\frac{159}{5648}\varepsilon_0^{4658s}\big)\\
X_s:=7460514*k_s=7460514*\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{4658}+\frac{1}{\varepsilon_0^{4658}}-2\Big]=\frac{801}{39536}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\mathbf{Ent}\big(\frac{801}{39536}\varepsilon_0^{4658s}\big)\\
Y_s:=7358060*k_s=7358060*\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{4658}+\frac{1}{\varepsilon_0^{4658}}-2\Big]=\frac{395}{19768}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\mathbf{Ent}\big(\frac{395}{19768}\varepsilon_0^{4658s}\big)\\
Z_s:=4149387*k_s=4149387*\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{4658}+\frac{1}{\varepsilon_0^{4658}}-2\Big]=\frac{891}{79072}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\mathbf{Ent}\big(\frac{891}{79072}\varepsilon_0^{4658s}\big)\\
w_s:=7206360*k_s=7206360*\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{4658}+\frac{1}{\varepsilon_0^{4658}}-2\Big]=\frac{128685}{6575684}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\mathbf{Ent}\big(\frac{128685}{6575684}\varepsilon_0^{4658s}\big)\\
x_s:=4893246*k_s=4893246*\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{4658}+\frac{1}{\varepsilon_0^{4658}}-2\Big]=\frac{2446623}{184119152}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\mathbf{Ent}\big(\frac{2446623}{184119152}\varepsilon_0^{4658s}\big)\\
y_s=3515820*k_s=3515820*\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{4658}+\frac{1}{\varepsilon_0^{4658}}-2\Big]=\frac{125565}{13151368}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\mathbf{Ent}\big(\frac{125565}{13151368}\varepsilon_0^{4658s}\big)\\
z_s:=5439213*k_s=5439213*\frac{3*11*29}{4657*16*d}\Big[\varepsilon_0^{4658}+\frac{1}{\varepsilon_0^{4658}}-2\Big]=\frac{5439213}{368238304}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\mathbf{Ent}\big(\frac{5439213}{368238304}\varepsilon_0^{4658s}\big)
\end{cases}$$

L'effectif total général du troupeau est $\mathbf{T_s=W_s+X_s+Y_s+Z_s+w_s+x_s+y_s+z_s=(10366482+7460514+7358060+4149387+7206360+4893246+3515820+5439213)k_s=(50389082)*k_s=\frac{(50389082)*33*29}{4657*16*4729494}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\frac{25194541}{184119152}\Big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\Big]=\mathbf{Ent}\big(\frac{25194541}{184119152}\varepsilon_0^{4658s}\big)}$

On remarque que $W_s, X_s, Y_s, ..., w_s, w_s, y_s, z_s, T_s$ sont tous entiers (Ce ne sont pas des morceaux de bovins, on n'est pas des bouchers) et s'écrivent tous sous la forme $m\big[\varepsilon_0^{4658s}+\frac{1}{\varepsilon_0^{4658s}}-2\big]$ avec m rationnel positif, le plus grand d'entre eux $M=\frac{25194541}{184119152}=0.1368382416...<0.2$ étant celui associé à T_s. Dans tous les cas on a $-1<r_m=m\big(\frac{1}{\varepsilon_0^{4658s}}-2\big)<0$ (rappelons que $s\geq 1$), et tous ces nombres entiers $W_s...$ s'écrivent $W_s=m\varepsilon_0^{4658s}+r_m$ soit $m\varepsilon_0^{4658s}=W_s-r_m$ avec $0<-r_m<1$, par conséquent (et de même pour les autres effectifs) $W_s=Ent(m\varepsilon_0^{4658s})$ où $Ent(x)$ désigne la partie entière de x c'est à dire le plus grands entier $\leq x$. (*) C'est pour cela que par anticipation nous avons mis ce résultat **en caractères gras** dans la dernière colonne des formules de l'accolade.

Or $(U_0+V_0\sqrt{d})(U_0-V_0\sqrt{d})=1$ et comme $0<U_0-V_0\sqrt{d}<U_0+V_0\sqrt{d}$ on a $0<U_0-V_0\sqrt{d}<1<U_0+V_0\sqrt{d}$ et $(U_0-V_0\sqrt{d})^n\to 0$. En considérant $U_0\approx V_0\sqrt{d}$ la formule précédente donne $k\approx\frac{2^{4653}V_0^{4658}}{4657*7*353}$;

Pour savoir le nombre de chiffres de k on calcule : $log_{10}(k)\approx 206537,187538$. Soit $k\approx 1,54*10^{206537}$, k est un nombre à 206 538 chiffres ; les effectifs des bœufs et vaches en découlent : le total du troupeau est :

T=50 389 082 * k $\simeq 7,760*10^{206544}$ *(le calcul est fait en moins de 70 secondes dans le fichier Maple joint)* soit un nombre de 206 545 chiffres, qui commence à gauche par 7760 et qui demande 46 pages à l'impression, et même 60 (le format des chiffres utilisé diffère) sur le site indiqué en lien dans le préambule à cet article.

(*) *Je pense qu'il y a une coquille dans l'article du Monthly AMM avril 1998 p 312 et 306, où au lieu d'Ent est utilisé le plus petit entier supérieur ou égal à x (ceil en Maple).*

Or la SICILE fait 25500 kilomètres carrés (plus précisément 25708 d'après le dictionnaire Larousse), cela fait $3 * 10^{206534}$ bovins par mètre carré, pauvres bêtes ! (*) C'est d'actualité avec les programmes de COMPRESSION des données ! Ici c'est une compression TROU-NOIR, 23 siècles après avoir été proposé, le problème d'ARCHIMÈDE est toujours intéréssant !

BIBLIOGRAPHIE **carrés** : ITARD Les nombres premiers (PUF) p71-81 ; SAMUEL théorie Algébrique des nombres (Hermann 1967) p92,95,29,30 ; PERRIN cours d'algèbre (ENS sèvres numéro 18 1981) p82 ; Leichtnam tome 1 Ellipse p25-26 ; SERRE arithmétique (PUF 1970) p 10-14 Bréal 89 p212-213 ; TAUVEL Mathématiques générales pour l'Agrégation (Masson 1992) p54,319 ; FRANCINOU Exercices de mathématiques pour l'Agrégation (Masson 1994) p 85, 134, 143 ; DESCOMBES éléments de théorie des nombres (PUF 1986) p 13 ; TISSIER Mathématiques générales pour l'Agrégation interne (Bréal 1991) p21 ; APOSTOL introduction to analytic number theory (Springer Verlag 1976) p179,186 ; TD0 ; br 94 p156-157 ; Lepez MPCI ; APM 403 ; APM 206 p 616-618 ;

Bœufs : ITARD arithmétique et théorie des nombres (PUF) p 101-103 (page 103 2ème ligne : pas de carré pour 8(Y+Z)); GOMEZ CALCUL FORMEL (Masson 1995) p 108-109 (page 109 1ère ligne $4729494P^2$ et non P) ; cité ALLEMBY (pile info) ; number theory p269 cattles of Archimède (éditions Arnold 1989) ; DORRIE Henrich 100 great Problems in elementary mathematics p3-7 (Bovinum) (Dover 1958) ; WELLS David le dictionnaire Pinguin des nombres curieux (Eyrolles mai 1995) p193 à 4 729 494 (Problème du bétail) ; pour la science janvier 96 (26 12 95) p90 colonne 2 article Houzel, erratum sur les trois derniers chiffres de d ; APM 358 avril 1987 p161-174 Article de Michel CHAMBON (Masny) ; Fractions continues : Parent, Descombes, quadrature 1 et 2. APM 403 ; APM 406 réponse AR (survol) ; APM 407 dec 96 p741-742 ; AMM avril 98 Ilan Vardi Archimedes's Cattle Problem p 305-319 ; Pour la Science mai 2000 p 100-101 et novembre 2001 p 99 ; (lettre en grec : Apm 358 p167 : l'épigramme qui suit a été découvert par Gotthold Ephraim LESSING, alors alors conservateur à la bibliothèque WOLFENBÜTTEL et publié par lui en 1773 + Dorrie 100 great PB P 5) ; Par Orsay 30 6 98 adreses internet où l'on peut lire cette lettre en grec : *http///www.astro.virginia.edu/ ew...ath/Archimedes'CattleProblem.html* ;

(*) *(Cela ridiculise au point de vue record, le décompte multiple du bétail dans une ile Française de Méditerranée...)*

ANNEXE

MINI COURS FLASH CORPS FINI VIDIANI

• **1) La caractéristique** *(plus petit k entier tel que k.1=0)* **d'un corps fini $\mathbb{K}$ est un nombre PREMIER noté p :** Sinon $k = n_1.n_2$ et $(n_1.1).(n_2.1) = (n_1.n_2).1 = 0$, il y aurait des diviseurs de zéro.

• **2) Par exemple $F_p = \mathbb{Z}/p\mathbb{Z}$ est un corps :** C'est déja un anneau, il reste à prouver que tout élément a non nul a un inverse : considérons l'application *(fondamentale en théorie des groupes finis g(x)=a*x pour la loi *)* $g : F_p \mapsto F_p$ telle que $g(x) = ax$, elle est injective, car $ax = ax'$ donne $a(x - x')$ divisible par p et par GAUSS, puisque a est non nul, $x - x' = 0$; Mais F_p étant fini, elle est surjective *(des éléments distincts ont des images distinctes)*, donc 1 a un antécédent par g : a est inversible.

• **3) Tout corps fini $\mathbb{K}$ (de caractéristique p) a un cardinal q qui est p-primaire (alias $q = p^s$, s entier > 0) :** $\mathbb{K}$ est un espace vectoriel de dimension finie s (puisque de cardinal fini) sur F_p ; Sur une base finie (qui existe...), $e_1, ..., e_s$, tout élément x de $\mathbb{K}$ s'écrit $x = u_1e_1 + ... + u_se_s$, où les $u_i \in F_p$; Le nombre des vecteurs, est $\boxed{\mathbf{q = p^s}}$.

• **4)** $\boxed{\textbf{Théorème de FERMAT : } \mathbf{a^q = a :}}$ On admet le théorème de Joseph, Henry, Maclagan WEDDDERBURN (1905) (1882-1948) *(Itard p110, Tauvel p179, Perrin p90, Dubreuil p370, Leichtnam et Schauer Ellipses (1982) p30, on le trouve aussi en tapant sous google "theorème de Weddeburn)* : Tout corps fini est commutatif : Alors a étant non nul de $\mathbb{K}$, posons $g : \mathbb{K}* \mapsto \mathbb{K}*$ telle que $g(x) = ax$, g est injective, donc (car $card(\mathbb{K}*)$ est fini) surjective et $\{g(x_1), ..., g(x_{q-1})\} = \{x_1, .., x_{q-1}\}$, où les x_i sont les éléments de $\mathbb{K}*$; par conséquent $g(x_1)..g(x_{q-1}) = a^{q-1}x_1..x_{q-1} = x_1..x_{q-1}$, comme $\mathbb{K}$ est un corps, on peut simplifier par le produit des x_i et on a : $a^{q-1} = 1$, qui donne le théorème de FERMAT (cas particulier de celui, d'EULER (en remplaçant q par $\varphi(q)$), en multipliant par a.

• **5) Tout corps fini de cardinal q est isomorphe à $\mathbf{F_q}$ (ensemble des racines de $\mathbf{X^q = X = 0}$) :** Soit Ω un corps algébriquement clos de caractéristique p (il en existe cf Francinou p142-143) l'application $h : x \mapsto x^q$, puissance s-ième de l'automorphisme $\sigma : x \mapsto x^p$, $(\sigma(xy) = \sigma(x)\sigma(y)$ et $\sigma(x + y) = \sigma(x) + \sigma(y)$ car $C_p^k \equiv 0$ mod p pour $1 < k < p)$ est un automorphisme de Ω : en effet, il est surjectif, puisque Ω est algébriquement clos ; Les éléments $x \in \Omega$ invariants par $x \mapsto x^q$ forment un sous corps noté F_q de Ω. Ce corps a bien q éléments : En effet la dérivée du polynôme $X^q - X$ est $qX^{q-1} - 1 = p.p^sX^{q-1} - 1 = -1 \neq 0$; Il en résulte (puisque Ω est algébriquement clos) que $X^q - X$, a q racines distinctes. Inversement si K est un sous corps de Ω à q éléments, ses éléments vérifient (FERMAT) $x^q = x$: K est égal à F_q puisque $K \subseteq F_q$ et de même cardinal. On remarque que par référence à un exercice classique de Sup on a : $pgcd(X^r - 1, X^s - 1) = X^{pgcd(r,s)} - 1$ donc $F_{p^r} \cap F_{p^s} = F_{p^{pgcd(r,s)}}$.

• **6) Caractérisation des carrés de $\mathbf{F_q}*$:** La relation xRx' définie par $x^2 = x'^2$ est une relation d'équivalence, chaque classe a deux éléments puisque $x^2 - x'^2 = (x - x')(x + x') = 0$ donne (corps) $x' = x$ ou $x' = -x$; Comme il y partition en classes : $2 * card(classes) = card(F_q*)$; Le nombre de carrés de F_q* *(suivant la notation de Tauvel pour ne pas préter à confusion on note ${}^2F_q*$, l'ensemble de ces carrés de F_q*)* est donc $\frac{q-1}{2}$, (on prend p premier > 2 donc impair, ainsi que q).

Si on pose $X = \{x \in F_q* | x^{\frac{q-1}{2}} = 1\}$ on a card$(X) \leq \frac{q-1}{2}$ car un polynôme de degré $\frac{q-1}{2}$ a au plus $\frac{q-1}{2}$ racines. D'autre part si x est un carré dans F_q*, il existe y de F_q* tel que, $x = y^2$ et $x^{\frac{q-1}{2}} = y^{q-1} = 1$ donc $x \in X$ soit ${}^2F_q* \subseteq X$, et par égalité des cardinaux : $X = {}^2F_q$. $\boxed{\mathbf{x \text{ carré dans } F_q* \Leftrightarrow x^{\frac{q-1}{2}} = 1}}$.

• **7) Si x n'est pas un carré dans $\mathbf{F_q}$ il l'est dans $\mathbf{F_{q^2}}$:** en effet s'il n'est pas un carré il vérifie d'après (4) $x^{\frac{q-1}{2}} = -1$, par conséquent $x^{\frac{q^2-1}{2}} = (x^{\frac{q-1}{2}})^{q+1} = (-1)^{pair} = 1$.

On pourrait aussi parler des résidus quadratiques et du symbole de LEGENDRE, et de son utilisation pour reconnaître si un élément d'un corps fini est un carré.