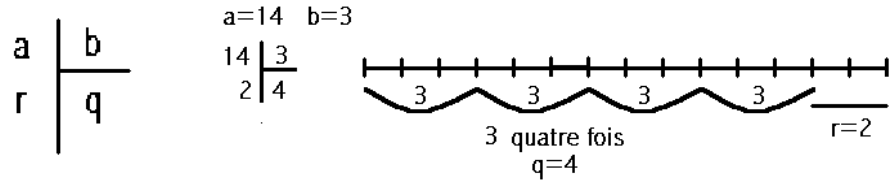
11. Division euclidienne, pgcd et algorithme d'Euclide,

L'arithmétique consiste à travailler exclusivement avec des nombres entiers. Quand on additionne deux nombres entiers, on obtient un nombre entier, et de même en soustraction. Quand on multiplie deux nombres entiers, on trouve encore un nombre entier. Mais quand on divise ? En général, la division ne tombe pas juste, et le résultat n'est pas un nombre entier. On sait que diviser, c'est multiplier par l'inverse. Mais l'inverse d'un nombre entier n'est pas un entier, en général. Prenons 3, son inverse est 1/3 qui n'est pas un entier. Cela signifie qu'on ne peut pas trouver un entier 3^{-1} tel que $3\times3^{-1} = 1$. En fait les seuls nombres entiers ayant un inverse entier sont 1 et –1, qui ont pour inverses eux-mêmes. On est dans un contexte très différent de celui des nombres réels ou des nombres rationnels, qui eux, à part 0, ont toujours un inverse, comme 3 qui a pour inverse 1/3. Toute l'arithmétique tourne autour de cet écueil propre aux nombres entiers, à savoir le problème de la division.

1. Division euclidienne

Il s'agit de la division la plus simple, celle où n'interviennent que des nombres entiers (pas de nombres à virgule). Donnons-nous deux nombres entiers positifs *a* et *b*. La division de *a* par *b* donne un quotient *q* et un reste *r*. On appelle *a* le dividende et *b* le diviseur. Mais qui sont *q* et *r* ? Par définition *q* est le plus grand nombre de fois que l'on peut mettre *b* dans *a*, et le résidu est le reste *r*. Par exemple quand on divise 14 par 3, on peut mettre au maximum 4 fois le 3 dans 14, d'où $q = 4$ et $r = 2$.



Ainsi définis, le quotient *q* est unique ainsi que le reste *r*, et ce dernier est forcément inférieur à *b* : $0 \le r < b$.

On peut écrire $a = bq + r$ avec $0 \le r < b$. Avec *a* et *b* donnés, cette équation ayant pour inconnues (des entiers positifs ou nuls) *q* et *r*, avec en plus la contrainte pour *r* d'être inférieur à *b*, admet une solution unique.

Autrement dit, une division euclidienne est fausse si l'on prend un quotient trop grand, avec *bq* qui dépasse *a* (le reste serait alors négatif) ou s'il est trop petit, auquel cas c'est le reste qui est trop grand : $r \ge b$.

Programmation

Avec *a* et *b* déclarés comme entiers (*int*), le fait d'écrire *a/b* donne *q*, et le reste *r* s'obtient en faisant *a modulo b*, soit *a%b* en langage *C*. Par exemple :

```
int a,b,q,r ;
a=14; b=3;
q=a/b; r=a%b;
printf("la division de %d par %d donne q=%d, r=%d", a,b,q,r);
```

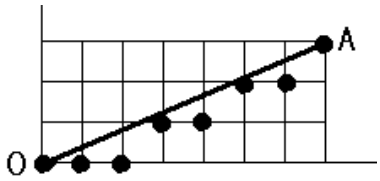
On peut aussi programmer soi-même l'opération de division :

```
a=14 ; b=3 ;
nbdefois=0 ;
while (nbdefois*b <= a) nbdefois++ ;
q=nbdefois-1 ; r=a-b*q ;
```

Remarque : La notion de division euclidienne peut s'étendre à des nombres entiers négatifs. Diviser par exemple –14 par –3 revient à diviser 14 par 3. Diviser 14 par –3 revient à diviser –14 par 3. Le seul cas nouveau est en fait *a* négatif et *b* positif. On s'arrange alors pour trouver *b* et *q* tels que $a = bq + r$ avec $0 \leq r < b$: le reste est toujours positif ou nul. Ainsi quand on divise –14 par 3, on trouve $q = -5$ et $r = 1$ (alors que $-14/3 \approx -4,66$).

Application : Comment tracer une droite sur un écran d'ordinateur ?

Prenons le cas d'un segment [*OA*] avec *A* de coordonnées entières positives *dx* et *dy* dans le repère orthonormé d'origine *O*, et supposons que sa pente est inférieure ou égale à 1, soit $dy \leq dx$. Pour tracer cette droite sur la grille de l'écran de l'ordinateur, où tous les pixels ont des coordonnées entières, on doit allumer des pixels qui en général ne sont pas exactement sur la droite puisque celle-ci n'a que peu de points à coordonnées entières sur elle. On va en fait construire ce que l'on appelle un chemin rasant par en-dessous. Voici un exemple avec $dx = 7$ et $dy = 3$.



Quand on prend les valeurs entières successives de *x*, de 0 à $dx = 7$, les points correspondants sur la droite ont pour ordonnée 0/7, 3/7, 6/7, 9/7, 12/7, 15/7, 18/7, 21/7=3, toutes de la forme $k\,dy / dx$, avec les numérateurs augmentant de $dy = 3$ à chaque fois. Il s'agit d'approcher ces points par des points à ordonnées entières situés au plus près d'eux et au-dessous. On va remplacer les ordonnées exactes sous forme de fraction $(k\,dy) / dx$ par le quotient euclidien de $k\,dy$ par dx : par exemple l'ordonnée 9/7 est remplacée par l'ordonnée 1. A cause de la pente inférieure ou égale à 1, chaque fois que *x* augmente de 1, l'ordonnée entière (le quotient euclidien) *y* reste soit fixe, soit augmente de 1.

Fractions :	0/7	3/7	6/7	9/7	12/7	15/7	18/7	21/7
Quotient euclidien *y* :	0	0	0	1	1	2	2	3
Augmentation de *y* :	0	0	0	1	0	1	0	1
Reste euclidien :	0	3	6	2	5	1	4	0

Pour tracer la «droite», on va utiliser la suite des restes euclidiens. Quand le numérateur $k\,dy$ de la fraction augmente de dy=3, le reste augmente de 3 aussi, le quotient restant fixe, mais il peut devenir trop grand en dépassant $dx = 7$, dans ce cas on doit rectifier l'erreur de la division en augmentant le quotient de 1 et en diminuant le reste de $dx = 7$. A chaque fois que l'on fait cette rectification, *y* augmente de 1. Ainsi la droite parfaite est remplacée par un cheminement à base de pas horizontaux $\rightarrow$ ou diagonaux $\nearrow$.

D'où le programme :

```
On se donne dx et dy entiers positifs avec dy≤ dx
x=0 ; y=0 ; reste=0 ;  dessiner ce point x,y
for(i=1 ; i <= dx ; i++)
  {x++ ; reste+=dy ; if (reste > =dx) {reste - = dx ; y ++ ;}  dessiner le point x,y}
```

Extension : La division avec virgule

On a deux nombres entiers positifs *a* et *b* et l'on veut diviser *a* par *b*. Au lieu de se contenter de la division euclidienne, on continue au-delà de la virgule, comme on apprend à le faire à l'école. Après avoir fait la division euclidienne classique, on ajoute un 0 au reste et on refait une division euclidienne, ce qui donne le premier chiffre derrière la virgule, puis on rajoute un 0 au reste et on fait la division pour avoir un deuxième chiffre derrière la virgule… Et l'on continue autant qu'on le désire. On obtient de la sorte l'écriture du nombre rationnel a/b sous forme d'un nombre à virgule avec une infinité de chiffres derrière la virgule. Mais n'oublions pas que tous les restes successifs sont inférieurs à *b*, donc en nombre limité. On est sûr, au bout d'un nombre fini de divisions, de retrouver un reste que l'on avait déjà trouvé. Cela signifie que les mêmes chiffres vont revenir par blocs dans les quotients successifs. Autrement dit, le développement décimal du nombre rationnel (de la fraction d'entiers) finit toujours par devenir périodique, éternellement.

Exemple :

```
759     | 28
199     |-----------
  30    | 27, 10  714285
  200
    40
   120
    80
   240
   160
    20
```

Le bloc 714285 va se répéter indéfiniment

Programmation

```
Les restes et quotients successifs sont placés dans des tableaux r[] et q[]
On se donne a et b entiers positifs, par exemple a=759  et  b=28.
r[0]=a%b;    q[0]=a/b;
printf("quotient: %ld , ", q[0]);   /* c'est la partie entière du quotient, 27 dans l'exemple */
i=0;  flag=0;
for(;;)      /* boucle infinie qui sera arrêtée par un break  */
  {   i++;  r[i]=(10*r[i-1])%b;  q[i]=(10*r[i-1])/b;  /* quotient et reste derrière la virgule */
     for(j=0; j<i; j++)    if (r[j]==r[i])  /* on teste si on déjà trouvé ce reste */
        {  flag=1;
           for(k=1; k<=j; k++) printf("%ld",q[k]);   printf("  ");
                       for(k= j+1; k<=i; k++)  printf("%ld",q[k]);   break;
        }
     if (flag==1) break;
  }
T=i-j ; printf("\nLa longueur de la période est %ld ",T);
```

2. Diviseurs d'un nombre

On dit qu'un nombre *d* est un diviseur (positif) d'un nombre *a* (positif), ou encore que *d* divise *a*, lorsque la division de *a* par *d* tombe juste, ou encore si l'on peut trouver un nombre *k* entier tel que $a = k\,d$. Par exemple 3 est un diviseur de 15 puisque la division de 15 par 3 donne un reste nul, avec $15 = 5 \times 3$. Un nombre *a* (autre que 0) admet un nombre fini de diviseurs, qui sont tous inférieurs ou égal à lui. Parmi les diviseurs, le plus petit est 1 et le plus grand le nombre lui-même. Et l'on a une propriété évidente de transitivité : si un nombre *d* divise *a* et qu'à son tour *a* divise *b*, à son tour *d* divise *b*.

Comment obtenir tous les diviseurs d'un nombre ?

Partons d'un exemple, en cherchant les diviseurs du nombre $a = 30$. On écrit, en partant de 1 :

$30 = 1 \times 30$ 1 et 30 sont deux diviseurs
$30 = 2 \times 15$ 2 et 15 sont des diviseurs
$30 = 3 \times 10$ 3 et 10 sont des diviseurs
$30 = 5 \times 6$ 5 et 6 sont des diviseurs.

Il n'y a pas d'autres diviseurs, car au-delà du diviseur 5 écrit en premier, on retrouve les autres diviseurs. On vient d'obtenir tous les diviseurs de 30, qui sont au nombre de 8.

Autre exemple, avec $a = 25$ on a : $25 = 1 \times 25$, et $25 = 5 \times 5$, d'où 25 admet 3 diviseurs.

D'où la méthode : On essaye les nombres inférieurs ou égal à *a*, à partir de 1, par ordre croissant. On prend ceux qui divisent *a*. A chaque fois, on obtient deux diviseurs (sauf cas exceptionnel où les deux diviseurs sont les mêmes, comme pour $25 = 5 \times 5$). On continue tant que le premier diviseur est inférieur ou égal au second.

Programme :

```
On se donne le nombre a (>1)
d1=1 ; d2= a ; compteur= 2;  afficher d1 et d2 ;
for (d1=2 ; d1*d1<=a ; d1++)  if (a % d1= =0)
  { afficher d1; compteur++;
    d2= a/d1 ; if (d2 !=d1) { afficher d2 ; compteur ++ ;}
  }
afficher compteur      /* c'est le nombre de diviseurs */
```

3. Nombres premiers

On dit qu'un nombre (positif) est premier s'il admet exactement deux diviseurs, à savoir 1 et lui-même. Notamment 1 n'est pas premier, puisqu'il n'a qu'un diviseur. Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, etc.

3.1. Théorème d'Euclide

Il existe une infinité de nombres premiers

Pour le prouver, faisons un raisonnement par l'absurde. Supposons qu'il n'existe qu'un nombre fini de nombres premiers. Prenons le plus grand d'entre eux : *P*. Puis formons le nombre $Q = P !+ 1 = 2 \times 3 \times 4 \times 5 \ldots \times P + 1$. Ce nombre *Q* n'est pas divisible par 2 puisque la division euclidienne donne comme reste 1. Il n'est pas divisible par 3 non plus, à cause du reste 1. Et il en est de même jusqu'à *P*. Le nombre *Q* n'est divisible par aucun des nombres premiers qui sont tous inférieurs ou égal à *P*. Mais on sait [1] qu'un nombre non premier admet toujours un diviseur premier (c'est le plus petit diviseur autre que 1). Le nombre *Q* est donc premier, et supérieur à *P* qui était supposé être le plus grand. Contradiction. Notre supposition était fausse. Il existe un nombre infini de nombres premiers. Précisons que cette démonstration, attribuée à Euclide, date de 2500 ans.

3.2. Théorème fondamental de l'arithmétique

Tout nombre entier (supérieur à 1) se décompose en produit de nombres premiers, et cette décomposition est unique.

Les nombres premiers sont en quelque sorte les atomes constitutifs de tout nombre (à condition de les mettre en multiplication). Par exemple :

$5 = 5$ on obtient un atome

[1] Voir cette propriété plus bas.

$15 = 3 \times 5$
$45 = 3^2 \times 5$

Pour obtenir la décomposition d'un nombre en produit de nombres premiers, on procède par divisions successives de nombres premiers de plus en plus grands à partir de 2. Cela s'écrit ainsi, par exemple pour le nombre 6468 :

6468	2
3234	2
1617	3
539	7
77	7
11	11
1	

D'où $6488 = 2^2 \times 3 \times 7^2 \times 11$

3.3 Applications

- **Nombre de diviseurs d'un nombre *a***

Ecrivons *a* comme produit de nombres premiers, grâce au théorème fondamental de l'arithmétique: $a = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$. Tout diviseur *d* de *a* est formé d'un *morceau* de cette décomposition, puisque *a* = *k d*, d'où $d = p_1^{b_1} p_2^{b_2} ... p_k^{b_k}$, avec $0 \le b_1 \le a_1$, $0 \le b_2 \le a_2$, …, $0 \le b_k \le a_k$. Le nombre de diviseurs de *a* est donc $(a_1 + 1)(a_2 + 1)\ldots (a_k + 1)$.

- **Plus petit diviseur d'un nombre**

Le plus petit diviseur (autre que 1) d'un nombre *a* est un nombre premier.

En effet, si ce plus petit diviseur *d* n'était pas premier, il admettrait un diviseur autre que 1 et lui même, soit *d '*, avec $1 < d' < d$. A son tour *d '*, déjà diviseur de *d*, diviserait le nombre *a*, et *d* ne serait plus le plus petit. Contradiction. Finalement ce nombre *d* est forcément premier.

On sait déjà qu'un nombre premier a comme plus petit diviseur autre que 1 lui-même, à savoir un nombre premier. Mais si un nombre (> 1) n'est pas premier, il admet toujours au moins trois diviseurs, notamment un diviseur (autre que 1 et lui-même) qui est premier et c'est ce diviseur qui est le plus petit diviseur après 1.

4. Diviseurs communs à deux nombres et pgcd. Multiples communs à deux nombres et ppmc

Considérons deux nombres (positifs) *a* et *b*. Les diviseurs de *a*, comme ceux de *b*, sont en nombre fini. Prenons leurs diviseurs communs, eux aussi en nombre fini. Le plus grand de ces diviseurs communs est appelé le pgcd de *a* et *b*.

On a la propriété suivante: les diviseurs du pgcd de *a* et de *b* sont exactement les diviseurs communs de *a* et *b*. [2]

[2] D'abord, tout diviseur *d* du pgcd divise *a* et *b* : en effet, *d* divise le pgcd, et celui-ci divise *a* et *b*, d'où *d* divise *a* et *b*.

Inversement, tout diviseur *d '* commun à *a* et *b* divise leur pgcd : en effet, si *d '* divise *a* et *b*, il divise une combinaison linéaire de *a* et *b*, notamment la plus petite positive, qui n'est autre que le pgcd., comme on le verra ci-dessous avec l'algorithme d'Euclide étendu.

Le pgcd intervient implicitement lorsque l'on simplifie une fraction. Prenons par exemple la fraction $\frac{210}{392}$. Pour la simplifier, on divise en haut et en bas par le même nombre. Et cela tant que c'est possible. Dans le cas présent, on divise en haut et en bas par 2, puis par 3, puis par 7 :

$$\frac{210}{588}=\frac{105}{294}=\frac{35}{98}=\frac{5}{14}$$

En résumé, on a divisé par le plus grand diviseur commun à 210 et 588, qui n'est autre que $2\times3\times7 = 42$.

Inversement, si un nombre *a* est un diviseur d'un nombre *m*, on dit que *m* est un multiple de *a*. Les multiples de *a* sont tous de la forme $m = k\,a$, avec *k* entier relatif. Les multiples d'un nombre (autre que 0) sont en nombre infini.

Par exemple les multiples de 7 sont : … -28, -21, -14, -7, 0, 7, 14, 21, 28, …

Prenons maintenant les multiples positifs communs à deux nombres, et notamment le ppmc, le plus petit multiple commun positif. Les multiples communs à *a* et *b* sont exactement les mêmes que les multiples du ppmc. [3] Notamment les multiples communs sont en nombre infini.

Programme pour avoir le ppmc

On se donne les deux nombres *a* et *b*. Puis on prend les multiples successifs de *a*, soit *a*, 2*a* , 3*a*,… jusqu'à ce que l'on tombe sur un multiple de *b*. On a alors le ppmc. D'où le programme :

```
multiple= a ;
while (multiple%b !=0)  multiple+= a;
afficher multiple  /* c'est le pgcd */
```

Lien entre le pgcd et le ppmc de deux nombres a et b

On a la formule : **pgcd** $\times$ **ppmc** = ***a b***

Autrement dit, il suffit d'avoir le pgcd pour connaître le ppmc, ou inversement.

5. Algorithme d'Euclide pour avoir le pgcd de deux nombres

Prenons deux nombres *a* et *b* (que nous supposons positifs). La division de *a* par *b* donne un quotient *q* et un reste *r* : $a = b\,q + r$ avec $0 \le r < b$. Nous allons vérifier que le pgcd de *a* et *b* est aussi celui de *b* et *r*. En effet tout diviseur de *a* et *b* divise *b* et aussi $a - bq = r$ qui est une combinaison linéaire de *a* et *b*. Inversement tout diviseur de *b* et *r* divise aussi *b* et $a = bq + r$ comme combinaison linéaire de *b* et *r*. Les diviseurs communs de *a* et *b* sont exactement les mêmes que les diviseurs communs de *b* et *r*. Et en particulier le plus grand d'entre eux.

Pour harmoniser les notations, posons $r_0 = a$, et $r_1 = b$. La division de r_0 par r_1 donne un quotient q_0 et un reste r_2 : $r_0 = q_0 r_1 + r_2$, et $\text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2)$ comme nous venons de le voir. Recommençons en divisant r_1 par r_2 : $r_1 = q_1 r_2 + r_3$ et l'on a comme précédemment : $\text{pgcd}(r_1 , r_2) = \text{pgcd}(r_2 , r_3)$. Et l'on continue ainsi en faisant des divisions successives.

Prenons un exemple : $a = 15$, $b = 9$

[3] Les multiples du ppmc sont des multiples communs à *a* et *b*. Et inversement les multiples communs sont des multiples du ppmc.

$15 = 1\times 9 + 6$ pgcd(15, 9) = pgcd(9, 6)
$9 = 1\times 6 + 3$ pgcd(9, 6) = pgcd(6, 3)
$6 = 2\times 3 + 0$ pgcd(6, 3) = pgcd(3, 0)

Or le pgcd de 3 et 0 est 3. A cause des égalités entre les pgcd, on trouve que le pgcd de 15 et 9 est 3. Autrement dit, on s'arrête lorsque l'on tombe sur un reste nul, et le pgcd n'est autre que le dernier reste non nul.

Généralisons : Faisons ces divisions successives à partir de $r_0 = a$ et $r_1 = b$

$r_0 = q_0 r_1 + r_2$
$r_1 = q_1 r_2 + r_3$
$r_2 = q_2 r_3 + r_4$
…..
$r_{n-1} = q_{n-1} r_n + 0$

On obtient cette suite d'égalités sur les pgcd :
$\text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \ldots = \text{pgcd}(r_{n-1}, r_n) = \text{pgcd}(r_n, 0) = r$

Le pgcd est le dernier reste non nul.

Un seul problème reste en suspens : la succession des divisions et des pgcd doit s'arrêter, car si elle se poursuivait éternellement, on ne trouverait jamais le pgcd. Mais un nombre fini de divisions suffit pour tomber à coup sûr sur un reste nul. En effet, lors de chaque division, par exemple $r_{k-1} = q_{k-1} r_k + r_{k+1}$, on a $0 \le r_{k+1} < r_k$. La suite des restes est strictement décroissante : $r_0 > r_1 > r_2 > r_3 > \ldots$ Il s'agit de nombres entiers, tous supérieurs ou égal à 0, qui diminuent de un au moins à chaque fois, avec un butoir que est le nombre 0. Il est donc certain qu'en un nombre fini d'étapes, on va tomber sur un reste nul.

C'est cela l'algorithme d'Euclide :

Lorsque l'on effectue des divisions successives, à partir de celle de *a* par *b*, et ensuite sur les restes successifs, le dernier reste non nul est le *pgcd* de *a* et *b*.

Programmation

On se donne a et b (*les deux entiers positifs dont on veut le pgcd*).
r0=a ; r1=b;
do { r2=r0 % r1; r0=r1; r1=r2; }
while (r2!=0) ; /* *au lieu de* r2!=0, on *pourrait aussi bien mettre* r1!=0 */
afficher r0 /* *c'est le pgcd* */

6. Algorithme d'Euclide étendu

Définition préalable

On appelle combinaison linéaire de deux nombres entiers *a* et *b*, tout nombre de la forme *k* fois *a* plus *k*' fois *b*, soit $k\,a + k'\,b$, avec *k* et *k*' entiers positifs, nuls ou négatifs. On peut aussi dire que c'est la somme de multiples de *a* et de multiples de *b*.

Par exemple, certaines des combinaisons linéaires de 9 et de 15 sont :

$1\times 9 + 1\times 15 = 24$, $-1\times 9 + 1\times 15 = 6$, $2\times 9 - 1\times 15 = 3$, etc. Il en existe une infinité.

Propriété

Chaque reste r_k obtenu dans l'algorithme d'Euclide est une combinaison linéaire de *a* et de *b*, soit $r_k = x_k\, a + y_k\, b$. En particulier le pgcd de *a* et *b* est une combinaison linéaire de *a* et de *b*, et parmi toutes les combinaisons, c'est la plus petite positive.

Démontrons cette propriété en faisant un raisonnement par récurrence.

* La propriété est vraie au départ :
$r_0 = a = 1\times a + 0\times b$, d'où $x_0 = 1$, $y_0 = 0$,
et $r_1 = b = 0\times a + 1\times b$, d'où $x_0 = 0$, $y_0 = 1$.

* Supposons la propriété vraie jusqu'à un certain rang *k*, et montrons qu'elle reste vraie au rang *k*+1 :

On sait que $r_{k+1} = r_{k-1} - q_{k-1}\, r_k$. d'après l'algorithme d'Euclide. Par hypothèse de récurrence

$r_{k-1} = x_{k-1}\, a + y_{k-1}\, b$ et $r_k = x_k\, a + y_k\, b$, d'où

$r_{k+1} = (x_{k-1}\, a + y_{k-1}\, b) - q_{k-1}(x_k\, a + y_k\, b) = (x_{k-1} - q_{k-1}\, x_k)\, a + (y_{k-1} - q_{k-1}\, y_k)\, b$. On a bien trouvé que r_{k+1} est une combinaison linéaire de *a* et de *b*. Elle est de la forme $r_{k+1} = x_{k+1}\, a + y_{k+1}\, b$, avec :

$\boldsymbol{x_{k+1} = x_{k-1} - q_{k-1}\, x_k}$ **et** $\boldsymbol{y_{k+1} = y_{k-1} - q_{k-1}\, y_k}$.

Il ne reste plus qu'à faire marcher la récurrence. Comme la formule est vraie au rang 0 et au rang 1, c'est-à-dire jusqu'au rang 1, elle est vraie au rang 2. Etant vraie jusqu'au rang 2, elle est vraie au rang 3, etc. Il en est ainsi jusqu'au dernier reste non nul, à savoir le pgcd.

Comme le pgcd divise *a* et *b*, il divise toute combinaison linéaire $k\, a + k'\, b$, et notamment la plus petite combinaison linéaire positive. Comme il est lui-même positif et qu'il est une combinaison linéaire, il ne peut qu'être égal à la plus petite combinaison linéaire positive.

Cet algorithme permet non seulement d'avoir le pgcd, mais aussi de l'écrire sous forme de combinaison linéaire. On l'appelle algorithme d'Euclide étendu.

Exemple 1 : Reprenons $a = 15$ et $b = 9$., en utilisant les quotients précédemment trouvés, et les formules de récurrence précédentes :

$r_2 = x_2\, 15 + y_2\, 9$, avec $x_2 = x_0 - q_0\, x_1 = 1 - 1\times 0 = 1$ et $y_2 = y_0 - q_0\, y_1 = 0 - 1\times 1 = -1$. On retrouve bien $r_2 = 1\times 15 - 1\times 9 = 6$.
$r_3 = x_3\, 15 + y_3\, 9$ avec $x_3 = x_1 - q_1\, x_2 = 0 - 1\times 1 = -1$ et $y_3 = y_1 - q_0\, y_2 = -1 - 1\,(-1) = 2$. On retrouve bien $r_3 = -1\times 15 + 2\times 9 = 3$ qui est le pgcd comme combinaison de 15 et 9.

Exemple 2 $a = 97$, $b = 18$

$97 = 5\times 18 + 7$ $\qquad$ $7 = 1\times 97 - 5\times 18$
$18 = 2\times 7 + 4$ $\qquad$ $4 = -2\times 97 + 11\times 18$
$7 = 1\times 4 + 3$ $\qquad$ $3 = 3\times 97 - 16\times 18$
$4 = 1\times 3 + 1$ $\qquad$ $1 = -5\times 97 + 27\times 18$
$3 = 3\times 1 + 0$
Le pgcd de 97 et 18 est 1 et l'on a la combinaison linéaire $1 = -5\times 97 + 27\times 18$.

Programme de l'algorithme d'Euclide étendu

Il suffit d'ajouter le calcul des coefficients x_k et y_k à l'algorithme d'Euclide précédent.

```
On se donne a et b
r0=a ; r1=b ; x0=1 ; x1=0 ; y0=0 ; y1=1 ;
while (r1 !=0)
  { q=r0/r1 ; r2=r0 – q*r1 ; x2=x0 - q*x1 ; y2=y0 - q*y1 ;
    r0=r1 ; r1=r2 ; x0=x1 ; y0=y1, x1=x2 ; y1 =y2 ;
  }
```

7. Nombres premiers entre eux et théorème deBezout

Définition

On dit que deux nombres sont premiers entre eux lorsque leur pgcd vaut 1**.** Très concrètement, cela signifie que les ces nombres n'ont aucun *atome* (nombre premier) en commun (en multiplication en leur sein).

Inversement, deux nombres qui ne sont pas premiers entre eux ont un pgcd supérieur à 1, on peut aussi dire qu'ils sont composites.

Théorème de Bezout

Si deux nombres *a* et *b* sont premiers entre eux, alors il existe deux nombres entiers relatifs *x* et *y* tels que l'on ait l'égalité $a\,x + b\,y = 1$. Inversement, s'il existe deux nombres *x* et *y* tels que l'on ait $a\,x + b\,y = 1$, alors *a* et *b* sont premiers entre eux. [4]

Quelques autres propriétés

- Si *a* et *b* ont pour pgcd *g*, *ka* et *kb* ont pour pgcd *kg*.
- Si *g* est le pgcd de *a* et de *b*, *a/g* et *b/g* sont premiers entre eux (leur pgcd vaut 1).
- Si *a* divise le produit *b c*, et que *a* est premier avec *b*, alors il divise *c*.

8. Equation de Diophante du premier degré

Il s'agit d'une équation du premier degré (linéaire) de la forme :

$a\,x + b\,y = c$

à deux inconnues *x* et *y*, et avec des coefficients *a*, *b*, *c* entiers naturels (dans ***N***), en supposant *a* et *b* tous les deux non nuls. L'objectif est de trouver les solutions entières (dans ***Z***) de cette équation.

Comment procède-t-on ?

On commence par chercher le pgcd *g* de *a* et de *b*. On distingue deux cas :

1) Si *g* ne divise pas *c*, alors que *g* divise toute combinaison linéaire $a\,x + b\,y$, l'égalité n'est jamais possible. L'équation n'admet aucune solution.

2) Si *g* divise *c*, on peut poser $a' = a/g$, $b' = b/g$ et $c' = c/g$, l'équation devient :

---

[4] En effet, prenons deux nombres *a* et *b* premiers entre eux . Leur pgcd vaut 1. Le pgcd est une combinaison linéaire de *a* et *b*, il existe *x* et *y* tels que $a\,x + b\,y = 1$.

Inversement, si l'on a deux nombres *x* et *y* tels que $a\,x + b\,y = 1$, cela signifie que l'on a trouvé une combinaison linéaire de *a* et *b* , soit $a\,x + by$, qui vaut 1. Cette combinaison est forcément la plus petite positive, c'est donc le pgcd de *a* et *b*, qui vaut bien 1. Les nombres *a* et *b* sont premiers entre eux.

$a' x + b' y = c'$ avec maintenant a' et b' premiers entre eux.

Commençons par traiter l'équation annexe $a' x + b' y = 1$ (et non pas c'). On sait, grâce au théorème de Bezout, qu'il existe x_0 et y_0 vérifiant cette équation. On vient de trouver une solution de cette équation, et l'algorithme d'Euclide étendu nous permet de la trouver. A son tour, en posant $x'_0 = c'x_0$, $y'_0 = c'y_0$, (x'_0, y'_0) est une solution de l'équation $a' x + b' y = c'$. Mais y en a-t-il d'autres ?

Ecrivons :

$a' x + b' y = c'$
$\underline{a'x'_0 + b'y'_0 = c'}$
$a'(x - x'_0) + b'(y-y'_0) = 0$ par soustraction.

Précisons que cette équation a exactement les mêmes solutions que l'équation initiale (elle est équivalente). Elle s'écrit aussi :

$b'(y - y'_0) = - a'(x - x'_0)$: b' divise $a'(x - x'_0)$ et b' est premier avec a', donc b' divise $x - x'_0$, ce qui donne $x - x'_0 = k\, b'$ avec k entier relatif quelconque. Par substitution dans l'équation, on trouve alors $b'(y - y'_0) = - a'k\, b'$, ou encore $y - y'_0 = - k\, a'$.

L'équation admet donc une infinité de solutions :

$\begin{cases} x = x'_0 + k\, a' \\ y = y'_0 - k\, b' \end{cases}$ avec k entier quelconque dans **Z**, ou encore $\begin{cases} x = x'_0 - k\, a' \\ y = y'_0 + k\, b' \end{cases}$.

Exemples

1) Résoudre $63\, x + 105\, y = 177$.

Le pgcd de 63 et 105 est $21 = 3 \times 7$. Mais 7 (et aussi 21) ne divise pas 177. L'équation n'admet aucune solution.

2) Résoudre $63\, x + 105\, y = 357$.

Le pgcd 21 de 63 et 105 divise 357. Divisons tout par 21. L'équation devient :
$3\, x + 5\, y = 17$ avec 3 et 5 premiers entre eux.

Commençons par chercher une solution particulière de $3\, x + 5\, y = 1$. On trouve facilement $x = 2$, $y = -1$. Une solution particulière de $3\, x + 5\, y = 17$ est :

$x_0 = 2 \times 17 = 34$, $y_0 = - 17$.

La solution générale est

$\begin{cases} x = 34 + k \times 5 \\ y = -17 - k \times 3 \end{cases}$ Une autre solution particulière, pour $k = -6$ est $x_0 = 4$, $y_0 = 1$. C'est la plus petite solution positive (x_0 et $y_0 > 0$). La solution générale s'écrit :

$\begin{cases} x = 4 + k \times 5 \\ y = 1 - k \times 3 \end{cases}$ On constate que (4, 1) est la seule solution positive.

Cas particulier où *a* et *b* (entiers positifs) sont premiers entre eux

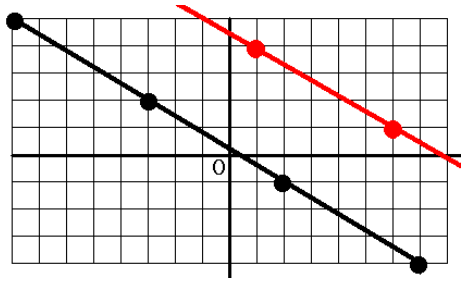
1) Equation $a\,x + b\,y = c$, avec *a* et *b* premiers entre eux (et positifs) et *c* positif

On cherche une solution particulière (x_0, y_0), grâce à l'algorithme d'Euclide étendu, et l'on en déduit la solution générale:

$$\begin{cases} x = x_0 + kb \\ y = y_0 - ka \end{cases} \quad \text{avec } k \text{ dans } \boldsymbol{Z}$$

Vision géométrique

Prenons l'exemple $3\,x + 5\,y = 1$, qui s'écrit aussi $y = (-3/5)\,x + 1/5$. Il s'agit de l'équation d'une droite de pente –3/5 qui est une fraction irréductible. Le problème revient à chercher les points à coordonnées entières de cette droite. Une fois trouvé un point, ici (2 , –1), on sait qu'en avançant de 5 et en descendant de 3 -ce qui correspond à la pente-, on trouve un autre point. Et ainsi de suite en avançant horizontalement de 5 en 5 ou en reculant d'autant. On trouve ainsi une infinité de points régulièrement espacés sur la droite. Et il n'y en a pas d'autres. Remarquons que toutes les solutions sont telles que *x* et *y* sont de signe contraire. Les deux solutions les plus intéressantes sont d'une part celle avec *x* positif le plus petit possible et d'autre part celle avec *y* positif le plus petit possible. Il s'agit des deux points successifs les plus près de l'origine, dans le cas présent (2 , –1) et (–3, 2).



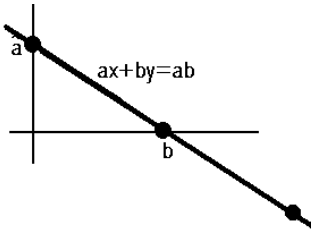
$3x + 5y = 23$

$3x + 5y = 1$

Sur le dessin, on a aussi pris l'exemple de $3\,x + 5\,y = 23$, où les points sont de la même façon régulièrement espacés par translation du vecteur (5, –3). Mais dans le cas présent, on constate qu'il existe deux solutions positives (x et $y > 0$).

L'équation générale $a\,x + b\,y = c$ admet une infinité de solutions régulièrement espacées sur la droite correspondante, se déduisant de l'une à la suivante située à sa droite en avançant horizontalement de *b* et en descendant verticalement de *a* (vecteur *b*, –*a*). A cause de la pente négative de la droite, l'équation générale admet toujours un nombre fini de solutions positives.

Reprenons l'équation particulière $a\,x + b\,y = 1$. Lorsque *a* et *b* sont tous deux différents de 1 (tout en étant positifs et premiers entre eux), la droite $a\,x + b\,y = 1$ coupe l' axe des *x* en $x = 1/a$ et l'axe des *y* en $y = 1/b$ et ces deux nombres sont strictement compris entre 0 et 1. Aucune solution ne peut se trouver sur la partie de la droite (avec *x* et *y* positifs) située entre eux. Les deux solutions les plus proches de *O* ont leur *x* et leur *y* de signe contraire, mais tels que $\mathbf{0} < |\boldsymbol{x}| < \boldsymbol{b}$ et $\mathbf{0} < |\boldsymbol{y}| < \boldsymbol{a}$.



Si l'on prend maintenant un autre cas particulier avec $a\,x + b\,y = ab$, on obtient exactement deux solutions positives ou nulles : l'une étant (*b*, 0) et l'autre (0, *a*), le vecteur qui les sépare étant exactement (*b*, –*a*).

Lorsque *c* est supérieur à *ab*, il y aura toujours au moins une solution positive, et lorsque *c* est inférieur à *ab*, il y en a au plus une.

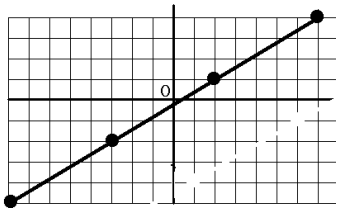
2) Equation $a\,x - b\,y = c$, avec a, b, c positifs et a premier avec b

On cherche une solution particulière (x_0,y_0), grâce à l'algorithme d'Euclide étendu, et l'on en déduit la solution générale :

$$\begin{cases} x = x_0 + kb \\ y = y_0 + ka \end{cases} \quad \text{avec } k \text{ dans } \boldsymbol{Z}$$

A noter que kb et ka sont maintenant tous deux précédés du même signe.

Géométriquement, les solutions sont situées sur la droite d'équation $y = (b/a)x - c/a$. Elles y sont régulièrement espacées, on passe de l'une à la suivante située à sa droite en avançant horizontalement de b et en montant de a. Comme la pente de la droite est positive, il existe une infinité de solutions positives.



Equation $3\,x - 5\,y = 1$

Dans le cas particulier de l'équation $a\,x - b\,y = 1$, toujours avec a et b premiers entre eux et autres que 1 (et 0), la droite coupe l'axe des x en $1/a$ qui n'est pas entier. On est alors sûr que la plus petite solution positive de l'équation est telle que $0 < x < b$, et $0 < y < a$. On en déduit ce que l'on peut appeler le théorème de Bezout étendu :

Avec a et b premiers entre eux (positifs et autres que 1), il existe un couple unique $(x\ ,\ y)$ d'entiers naturels tels que $0 < x < b$ et $0 < y < a$ vérifiant $a\,x - b\,y = 1$.

Prenons enfin l'équation $a\,x - b\,y = -1$. Pour les mêmes raisons que précédemment, la plus petite solution positive (x', y') est telle que $0 < x' < b$ et $0 < y' < a$. [5]

9. Exercices

9.1. *Avec 100 euros, que l'on entend dépenser en totalité, on veut acheter exactement 40 objets coûtant soit 1 euro, soit 4 euros, soit 12 euros. Combien va-t-on acheter d'objets de chacune de ces trois catégories, et combien y a-t-il de possibilités ?*

Appelons x , y , z les nombres respectifs d'objets achetés à un euro, 4 euros et 12 euros. Le problème se ramène au système d'équations :

$$\begin{cases} x + y + z = 40 \\ x + 4y + 12z = 100 \end{cases}$$

qui équivaut à :

$$\begin{cases} x + y + z = 40 \\ 3y + 11z = 60 \end{cases}$$ après avoir remplacé une équation par la soustraction des deux équations.

[5] Prenons l'équation $ax - by = 1$, et sa plus petite solution positive x,y avec $0 < x < b$ et $0 < y < a$. On a aussi : $a(x - b) - b(y - a) = 1$, ou encore $a(b - x) - b(a - y) = -1$. On vient de trouver une solution $x' = b - x$, $y' = a - y$ de l'équation $ax - by = -1$. On a aussi x' et y' tels que $0 < x' < b$ et $0 < y' < a$. Il s'agit bien de la plus petite solution positive. Entre les deux solutions positives les plus petites (x, y) et (x', y') de $ax - by = 1$ et $ax - by = -1$, on a le lien $x + x' = b$ et $y + y' = a$.

Commençons par traiter l'équation $3y+11z=60$. Les nombres 3 et 11 sont premiers entre eux, il y a une infinité de solutions *y*, *z* dans Z. Une solution particulière de $3y+11z=1$ est manifestement *y* = 4, *z* = –1. Une solution particulière de $3y+11z=60$ est donc *y* = 240, *z* = – 60. La solution générale de l'équation (avec *y* et *z* dans ***Z***) est :

$$\begin{cases} y = 240 - k11 \\ z = -60 + k3 \end{cases}$$

Mais on ne peut prendre que les solutions positives ou nulles. On voit que pour *k* = 20, on a la plus petite valeur ≥ 0 pour *z*, soit *z* = 0 et *y* = 20, qui convient, puis on prend *k* = 21, *z* = 3, *y* = 9, qui convient aussi, puis pour *k* ≥ 22, on tombe sur *y* < 0. En reportant ces deux résultats dans la première équation, on trouve les deux solutions :

x =20, *y* = 20, *z* = 0, et *x* = 28, *y* = 9, *z* = 3.

9.2. Problème de divisions

1) Montrer que 2^{3n} –1 est divisible par 7.

$2^{3n}-1=(2^3)^n-1=8^n-1=(8-1)(8^{n-1}+8^{n-2}+...+1)$ grâce à l'identité remarquable bien connue. $2^{3n}-1$ est de la forme $7\,q$, et donc divisible par 7.

2) En prenant toutes les puissances de 2, et en écrivant leur exposant sous l'une des trois formes 2^{3n}, ou 2^{3n+1} ou 2^{3n+2}, montrer qu'il y a trois restes possibles lorsqu'on les divise par 7. Pour cela utiliser $2^{3n+1}-2$ et $2^{3n+2}-4$. En particulier, quel est le reste de la division de 2^{1000} par 7 ?

On a déjà vu que $2^{3n}-1=7q$, d'où $2^{3n}=7q+1$, ce qui signifie que le reste de la division de 2^{3n} par 7 est 1.

A son tour : $2^{3n+1}-2=2(2^{3n}-1)=2.7q$, d'où $2^{3n+1}=7(2q)+2$, le reste est 2.

Enfin $2^{3n+2}-4=4(2^{3n}-1)=4.7q$, d'où $2^{3n+2}=7(4q)+4$, le reste est 4.

Prenons l'exemple de 2^{1000}. Lorsque l'on divise 1000 par 3, le reste est 1, 1000 est de la forme 3*n*+1, donc le reste de la division de 2^{1000} par 7 est 2.

3) On considère les nombres $A_p = 2^p + 2^{2p} + 2^{3p}$, dépendant du nombre entier positif p.

a) Donner l'écriture de A_3 en binaire.

Puisque $A_3 = 2^3 + 2^6 + 2^9$ il s'écrit 1001001000 en binaire.

b) En prenant p sous l'une des trois formes 3n , 3n+1 ou 3n +2, montrer qu'il y a trois restes possibles lorsque l'on divise A_p par 7.

Lorsque $p = 3n$, avec $A_{3n} = 2^{3n} + 2^{6n} + 2^{9n}$, 2^{3n} donne comme reste 1 quand on le divise par 7, et de même pour 2^{6n} et 2^{9n}. Le reste de la division de A^{3n} par 7 est donc 3.

Pour $p = 3n+1$, avec $A_{3n+1} = 2^{3n+1} + 2^{6n+2} + 2^{9n+3}$, 2^{3n+1} donne comme reste 2 quand on le divise par 7, 2^{6n+2} donne comme reste 4, et 2^{9n+3} donne comme reste 1. On peut écrire $A_{3n+1} = 7q + 2 + 7q' + 4 + 7q'' + 1$, qui est finalement un multiple de 7. La division de A_{3n+1} par 7 donne un reste nul.

Pour $p = 3n + 2$, avec $A_{3n+2} = 2^{3n+2} + 2^{6n+4} + 2^{9n+6}$, 2^{3n+2} donne comme reste 4 quand on le divise par 7, $2^{6n+4} = 2^{3(2n+1)+1}$ donne comme reste 2, et 2^{9n+6} donne comme reste 1, soit un total égal à 7. D'où un reste égal à 0 aussi.

c) Quel est le reste de la division du nombre écrit en binaire 1000100010000 par le nombre 111 en binaire ?

Ce nombre n'est autre que A_4, avec 4 = 3 + 1. Le diviseur 111 n'étant autre que 7, le reste est nul.

9.3. Pgcd et équations diophantiennes

1) Déterminer le pgcd de 903 et 731

Appliquons l'algorithme d'Euclide :

$903 = 1\times 731 + 172$
$731 = 4\times 172 + 43$
$172 = 4\times 43 + 0$. Le pgcd vaut 43.

2) Rendre la fraction 903 / 731 irréductible.

Il suffit de diviser en haut et en bas par le pgcd 43. On obtient 903 / 731 = 21 / 17.

3) Résoudre l'équation 903 x + 731 y = 2100, avec x et y entiers relatifs.

On constate que le pgcd 43 de 903 et 731 ne divise pas 2100. L'équation n'a aucune solution.

4) Résoudre l'équation 903 x + 731 y = 2107.

Comme le pgcd 43 divise 2107, on divise tout par 43, et l'on obtient l'équation équivalente :
$21\,x + 17\,y = 49$. Maintenant 21 et 17 sont premiers entre eux.

Commençons par chercher une solution particulière de l'équation $21\,x + 17\,y = 1$. Sans avoir besoin d'utiliser l'algorithme d'Euclide élargi, on constate (en prenant les premiers multiples de 21 et ceux de 17) qu'une solution est $x_0 = -4$, $y_0 = 5$.

Une solution particulière de l'équation $21\,x + 17\,y = 49$ est $x_0 = -4\times 49 = -196$, $y_0 = 5\times 49 = 245$.

La solution générale de l'équation est :

$$\begin{cases} x = -196 + 17k \\ y = 245 - 21k \end{cases}$$

Faisons ressortir une solution qui est la plus proche de 0 possible : on trouve $x_0 = 8$, $y_0 = -7$ en faisant $k = 12$. [6] Finalement on peut écrire la solution générale sous la forme :

$$\begin{cases} x = 8 + 17k \\ y = -7 - 21k \end{cases}$$

[6] On s'est arrangé pour que x devienne positif, en ajoutant à -196 un certain nombre de fois 17. Mais dans ce cas, y est négatif. On aurait pu aussi bien rendre y positif le plus petit possible, en enlevant à 245 un certain nombre de fois 21 : on aurait obtenu la deuxième solution la plus proche de 0 possible, soit $x = -9$, $y = 14$.

5) On considère l'équation 21 x + 17 y = N avec N entier > 0. Quelle est la plus petite valeur de N pour laquelle cette équation admet une solution positive : x > 0 et y > 0.

Les plus petites valeurs possibles de x et y sont 1 et 1. On trouve alors $N = 38$. Remarquons que lorsque $N > 38$, on n'est pas pour autant assuré d'avoir une solution positive, le cas où $N = 49$ étant un exemple où x et y sont toujours de signe contraire. Mais pour N « suffisamment » grand, on est sûr d'avoir des solutions positives (penser aux points solutions qui sont régulièrement espacés sur une droite de pente négative, avec une ordonnée à l'origine suffisamment grande).

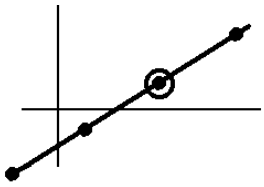
6) En s'aidant de la méthode de résolution du 4° , faire un programme qui donne toutes les solutions de l'équation a x + b y = c, avec a, b et c positifs.

```
a=903; b=731; c=2107;        /* un exemple pour a, b, c  */
printf("Résolution de %dx+%dy=%d",a,b,c);
r0=a;r1=b; while (r1!=0) { r2=r0%r1; r0=r1; r1=r2;}  /* calcul du pgcd g par l'algorithme d'Euclide */
g=r0; printf("\n\nLe pgcd de %d et %d est %d",a,b,g);
if (c%g !=0) printf("\n\nPas de solutions");
else                                   /* cas où il y a une infinité de solutions */
  {aa=a/g; bb=b/g; cc=c/g;     /* on divise a, b, c  par  g  */
     /*  cherchons une solution de aa . x + bb . y = 1 par l'algorithme d'Euclide élargi  */
   r0=aa;r1=bb;x0=1;x1=0;y0=0;y1=1;
   while (r1!=0) {q=r0/r1; r2=r0%r1;x2=x0-x1*q;y2=y0-y1*q;
            r0=r1; r1=r2;x0=x1;x1=x2;y0=y1;y1=y2; }
   x0=cc*x0;  y0=cc*y0;    /* une solution particulière de aa . x + bb . y =  cc  */
   while (x0<0) {x0+=bb; y0-=aa;}              /* on s'arrange pour avoir une solution */
   while (x0>=bb) {x0-=bb; y0+=aa;}            /* avec    0 ≤ x < bb     */
            printf("\n\nUne infinité de solutions: \nx=%d + k*%d \ny=%d - k*%d", x0,bb,y0,aa);
  }
```

7) Résoudre 17 x – 21 y = 1000.

Commençons par chercher une solution particulière à l'équation $17x - 21y = 1$. En s'aidant de la question 4°, on trouve $x_0 = 5$, $y_0 = 4$ (remarquons que si une solution de $ax + by = c$ est x_0 , y_0, une solution de $ax - by = c$ est x_0 , $-y_0$). Une solution particulière de $17x - 21y = 1000$ est $x_0 = 5000$, $y_0 = 4000$. D'où la solution générale :

$x = 5000 + 21k$, $y = 4000 + 17k$. Mais on préfère faire ressortir une solution particulière positive la plus petite possible, comme indiqué sur le dessin suivant :



C'est y qu'il faut choisir positif le plus petit possible. Cela s'obtient ici en enlevant à 4000 un certain nombre de fois 17, de façon que y reste ≥ 0 mais inférieur à 17.

On trouve finalement comme solution générale :

$$\begin{cases} x = 65 + 21k \\ y = 5 + 17k \end{cases}$$

8) Faire le programme qui permet de résoudre une équation de la forme :
ax – by = c avec a, b et c positifs.

Il suffit d'apporter de petites modifications au programme du 6°.

```
a=17; b=21; c=1000;
r0=a;r1=b; while (r1!=0) {q=r0/r1; r2=r0%r1; r0=r1; r1=r2;}
g=r0; printf("\n\nLe pgcd de %d et %d est %d",a,b,g);
```

```
if (c%g !=0) printf("\n\nPas de solutions");
else
  {aa=a/g; bb=b/g; cc=c/g;
   r0=aa;r1=bb;x0=1;x1=0;y0=0;y1=1;
   while (r1!=0) {q=r0/r1; r2=r0%r1;x2=x0-x1*q;y2=y0-y1*q;
              r0=r1; r1=r2;x0=x1;x1=x2;y0=y1;y1=y2; }
   x0=cc*x0; y0= - cc*y0;    /* première modification sur y0 */
   printf("\n(%d %d)",x0,y0);
   while (y0<0) {y0+=aa;x0+=bb;}  /* deuxième modification */
   while (y0>=aa) {x0-=bb; y0-=aa;}
   printf("\n\nUne infinité de solutions: \nx=%d + k*%d \ny=%d + k*%d",x0,bb,y0,aa);
  }
```

9.4. Equation du second degré

a) Déterminer les nombres x et y entiers naturels vérifiant $x^2 - y^2 = 1$.

L'équation s'écrit $(x - y)(x + y) = 1$. Puisqu'il s'agit d'entiers, et que $x + y$ est positif (le cas $(-1)(-1) = 1$ est exclu), cela impose que $x + y = 1$ et aussi $x - y = 1$, d'où la solution unique $x = 1$, $y = 0$.

b) Déterminer les nombres x et y entiers naturels vérifiant $x^2 - y^2 = p$, *p étant un nombre premier.*

L'équation s'écrit $(x - y)(x + y) = p$. La seule possibilité de factorisation est $1\ p = p$ ou $p\ 1 = p$, le cas $(-1)(-p)$ étant exclu. Et comme $x + y$ est supérieur à $x - y$, la seule possibilité est :

$x + y = p$ et $x - y = 1$, d'où $2x = p + 1$.

Si $p = 2$, il n'y a aucune solution, la division de 3 par 2 ne tombant pas juste.
Si p est > 2, il est toujours impair, d'où $x = (p + 1)/2$, $y = (p - 1)/2$.

9.5. Suites de nombres entiers

On considère les deux suites (x_n) *et* (y_n) *définies, pour tout n entier naturel, par les relations de récurrence et les conditions initiales :*

$x_{n+1} = 2\,x_n - 1$ *et* $x_0 = 3$
$y_{n+1} = 2\,y_n + 3$ *et* $y_0 = 1$

A- Etude de (x_n)

1) Calculer x_3 *et* x_4*. Quel est le pgcd de* x_3 *et* x_4 *?*

Remarquons que tous les termes de la suite (x_n) sont des nombres entiers naturels, par récurrence évidente. De la définition de (x_n), on déduit $x_1 = 5$, $x_2 = 9$, $x_3 = 17$, $x_4 = 33$. Puisque x_3 est seulement divisible par 1 et par 17 et que x_4 ne contient pas 17 comme nombre premier dans sa décomposition, le pgcd de x_3 et x_4 est 1. Les nombres x_3 et x_4 sont premiers entre eux.

2) x_n *et* x_{n+1} *sont-ils premiers entre eux pour tout n ?*

La relation de récurrence s'écrit $2x_n - x_{n+1} = 1$. Grâce à la propriété de Bezout, avec 1 et 2 premiers entre eux, il en découle que x_n et x_{n+1} sont premiers entre eux, quel que soit n.

3) En prenant la fonction f telle que $f(x) = 2x - 1$*, ce qui permet d'écrire* $u_{n+1} = f(u_n)$*, déterminer le point fixe unique L de f, c'est-à-dire la solution L de l'équation* $f(x) = x$.

L'équation $f(x) = x$ s'écrit $x = 2x - 1$, d'où la solution unique $x = 1$. Il existe un point fixe unique $L = 1$ tel que $L = 2L - 1$.

4) En introduisant la suite (v_n) telle que $v_n = x_n - L$, montrer que (v_n) est une suite géométrique, dont on déterminera les caractéristiques. Puis donner la forme explicite de v_n et en déduire celle de x_n.

Retranchons membre à membre les deux égalités $x_{n+1} = 2\,x_n - 1$ et $L = 2L - 1$. On obtient $x_{n+1} - L = 2x_n - L$, soit $v_{n+1} = 2\,v_n$. La suite (v_n) est une suite géométrique de raison 2 et de terme initial $v_0=2$. On en déduit sa forme explicite $v_n = 2 \times 2^n$, $v_n = 2^n + 1$, puis celle de u_n : $u_n = 2^{n+1} + 1$.

B- Etude de (y_n)

1) Montrer que $2x_n - y_n = 5$.

Faisons un raisonnement par récurrence pour montrer la formule $2x_n - y_n = 5$.

- C'est vrai au départ : on a bien $2x_0 - y_0 = 6 - 1 = 5$.
- Supposons la formule vraie à un certain rang *n*, et montrons que cela reste vrai au rang suivant : $2x_{n+1} - y_{n+1} = 2(2x_n - 1) - (2y_n + 3) = 4x_n - 2\,y_n - 5 = 2(2x_n - y_n) - 5 = 2 \times 5 - 5 = 5$.

En faisant marcher la récurrence, la formule est vraie pour tout *n*.

2) Exprimer y_n en fonction de n.

Puisque $y_n = 2x_n - 5$ grâce à ce qui précède, et que $x_n = 2^{n+1} + 1$, il vient : $y_n = 2^{n+2} - 3$.

C- Pgcd g_n de x_n et y_n

1) En utilisant la formule du B-1, montrer que g_n est soit 1 soit 5.

Puisque g_n est un diviseur de x_n et de y_n, il divise aussi $2x_n - y_n$, et par suite g_n divise 5. Il ne peut donc être que 1 ou 5.

2) Donner la suite des restes r_n de la division de 2^n par 5 suivant les valeurs de n.

La division de la suite des puissances de 2 à partir de $2^0 = 1$ donne comme restes successifs 1, 2, 4, 3, 1, 2, 4, 3, … ce qui donne une suite périodique dont la période est 1, 2, 4, 3. Pour montrer que c'est vrai pour tout *n*, il suffit de prouver que 2^{n+4} donne le même reste que 2^n lorsqu'on fait leur division par 5. Comme $2^{n+4} = 2^n \times 16$, et que 16 donne un reste égal à 1, cela montre que les restes de 2^n et 2^{n+4} sont les mêmes. Plus précisément : $r_{4k} = 1$, $r_{4k+1} = 2$, $r_{4k+2} = 4$, $r_{4k+3} = 3$, pour tout *k*.

3) En déduire pour quelles valeurs de n les nombres x_n et y_n sont premiers entre eux.

Puisque $x_n = 2^{n+1} + 1$, avec $2^{n+1} = 5q + r_{n+1}$, on a $x_n = 5q + r_{n+1} + 1$, d'où la suite périodique des restes successifs : 3, 0, 4, 2, 3, 0, 4, 2, …. lorsqu'on divise x_n par 5.

De même $y_n = 2^{n+2} - 3 = 5q + r_{n+2} - 3$, d'où la suite des restes successifs 1, 0, 3, 4, 1, 0, 3, 4, … On constate que les nombres x_n et y_n sont tous deux multiples de 5 si et seulement si *n* est de la forme $n = 1 + 4k$. C'est le seul cas où leur pgcd vaut 5. Dans tous les autres cas, il ne peut être que 1. Lorsque la division de *n* par 4 donne un reste autre que 1, les deux nombres sont premiers entre eux.

9.6. Résolution d'équations de Diophante

Programmer la résolution d'équations de la forme $a\,x + b\,y = c$ et $a\,x - b\,y = c$, avec a, b, c positifs. Donner les résultats obtenus pour :

- *$147\,x + 258\,y = 369$*
- *$101\,x + 37\,y = 3819$*
- *$999\,x - 49\,y = 369$*
- *$999\,x - 49\,y = 5000$*

Grâce aux programmes créés précédemment, on trouve :

- pour 147 x + 258 y = 369, x = 85 + 86 k, y = – 47 – 49 k
- pour 101 x + 37 y = 3819, x = 14 + 37 k, y = 65 – 101 k
- pour 999 x – 49 y = 369, x = 22 + 49 k, y = 441 + 999 k
- pour 999 x – 49 y = 5000, x = 13 + 49 k, y = 163 + 999 k

9.7. Caisses de lingots d'or

Des lingots d'or sont seulement disponibles par caisses de 5 lingots ou par caisses de 11. Une société a besoin d'exactement N lingots, avec N entier positif. Pour cela elle doit acheter un certain nombre x (≥ 0) de caisses de 5 et un certain nombre y de caisses de 11, de façon à obtenir un compte rond. On veut connaître les solutions (x , y) et leur nombre selon les valeurs prises par N.

1) *Trouver une valeur de N pour laquelle le problème n'a aucune solution.*

Le nombre de lingots est $N = 5x + 11y$. On voit aussitôt que la valeur minimale de N est 5, pour $x = 1$ et $y = 0$. On ne peut pas avoir moins.

Traitons d'ailleurs le cas où $N = 1$. Une solution particulière de l'équation $5x + 11y = 1$, où 5 et 11 sont premiers entre eux, est $x_0 = –2$, $y_0 = 1$. La solution générale est :
$x = –2 + 11k$, $y = 1 – 5k$, avec k dans $\boldsymbol{Z}$. Il n'existe aucune solution positive, comme on pouvait s'y attendre.

2) *Traiter le cas où $N = 5 \times 11 = 55$. Pourquoi est-on assuré d'avoir au moins une solution dès que $N \geq 55$? Traiter cette question géométriquement.*

L'équation $5x + 11y = 55$ admet exactement deux solutions : $x = 11$, $y = 0$, et $x = 0$, $y = 5$. En effet, sur la droite D d'équation $5x + 11y = 55$, ce sont les deux seuls points solutions, situés sur chacun des axes Ox et Oy (on sait que deux solutions successives, correspondant à deux points sur la droite, sont séparés par le vecteur (11, –5). Dès que l'on prend $5x + 11y = N$ avec $N > 55$, la droite correspondante est située au-dessus de la droite D, et comme deux points solutions sont séparés par le vecteur (11, –5), on est sûr qu'il y a au moins un point solution dans la zone positive (le quart de plan xOy).

3) *Traiter le cas où N = 101.*

On a vu qu'une solution particulière de l'équation $5x + 11y = 1$ est $x_0 = –2$, $y_0 = 1$. Une solution particulière de l'équation $5x + 11y = 101$ est $x_0 = –202$, $y_0 = 101$. La solution générale de cette équation est : $x = –202 + 11k$, $y = 101 – 5k$.

Parmi cette infinité de solutions, celles qui sont positives doivent être telles que $k \geq 202 / 11$, soit $k \geq 19$, et pour la deuxième équation $k \leq 101 / 5$, soit $k \leq 20$. Deux valeurs conviennent : $k = 19$ ou 20, d'où deux solutions : $x = 7$, $y = 6$, ou $x = 18$, $y = 1$.

4) *Faire le programme qui pour chaque valeur de N, par exemple entre 1 et 200, donne les solutions éventuelles et leur nombre. Dégager le nombre de valeurs de N pour lesquelles il n'y a aucune solution, et donner la plus grande d'entre elles.*[7]

```
a=5; b=11;
cumul=0;    /* cumul contiendra à la fin le nombre de cas sans solutions */
for(N=1; N<200; N++)
  { afficher N
```

[7] On pourra vérifier que la plus grande valeur de N ne donnant aucune solution est $Nmax = ab – a – b$, et que le nombre de cas sans solution est $(Nmax + 1)/2$. Pour la démonstration, consulter [AUD2014]

```
 r0=a;r1=b;x0=1;y0=0;x1=0;y1=1;   /* algorithme d'Euclide élargi  pour ax + by = 1 */
 while(r1!=0)
   {  q=r0/r1;r2=r0-q*r1;x2=x0-q*x1;y2=y0-q*y1;
      r0=r1;r1=r2; x0=x1;x1=x2; y0=y1;y1=y2;
   }
 x0=N*x0; y0=N*y0;   /* une solution particulière de ax + by = N  */
 nbsol=partieentiere(x0,b)+partieentiere(y0,a)+1; /* calcul théorique du nombre de solutions */
 compteur=0;    /* compteur sera le nombre de solutions obtenu expérimentalement */
 if (x0<0)
 do {x0+=b; y0-=a;  if (x0>=0 && y0>=0) {compteur ++; printf(" (%d %d)",x0,y0);} }
 while(y0>=0);
 else if (y0<0)
 do {x0-=b; y0+=a;   if (x0>=0 && y0>=0) {compteur ++; printf(" (%d %d)",x0,y0);} }
 while(x0>=0);
 if (compteur==0) cumul++;
 printf("   nombre de solutions= %d ",compteur);  if (compteur!=nbsol) printf("ERREUR");
 }
printf("\n\nNombre de cas où il n'y a pas de solutions= %d ",cumul);
}
```

Le programme donne 20 valeurs de *N* pour lesquelles il n'y a pas de solutions, la plus grande étant 39.

5) *On admettra que le nombre de solutions positives ou nulles ($x \geq 0$ et $y \geq 0$) de l'équation $a\,x + b\,y = N$, avec a et b premiers entre eux, est $[x_0 / b] + [y_0 / a] + 1$, où (x_0, y_0) est une solution particulière (n'importe laquelle, et pas forcément positive) de l'équation, et où [X] désigne la partie entière de X. Vérifier par programme que cette formule est cohérente avec les résultats obtenus au 4°.*

Remarque sur la partie entière [X] de X *: il s'agit du nombre entier le plus proche de X et qui lui est inférieur ou égal. Par exemple [3]=3, [3,2] = 3 , [–3]= –3, [–3,3]= –4. Dans le cas présent on doit trouver la partie entière [n / d] d'une fraction d'entiers. Si n et d ont le même signe, il suffit de prendre le quotient euclidien dans la division de n par d. Mais si le quotient n/d est négatif, il convient de distinguer deux cas : soit la division tombe juste et on prend le quotient euclidien de n par d (par exemple [–6/3]= –2, soit elle ne tombe pas juste, et l'on prend le quotient entier tel qu'il est donné par l'ordinateur, par exemple le quotient de – 7 par 3 (soit – 2,33) est –2 , et on lui enlève 1, pour avoir la partie entière –3 dans l'exemple choisi. D'où la fonction ramenant la partie entière de n/d :*

```
int partieentiere (int n, int d)
{  if (n*d>=0) return n/d;
   else if (n%d==0) return n/d;
   else return n/d -1;
}
```

Le calcul théorique du nombre des solutions a été intégré dans le programme précédent, et l'on peut comparer le résultat théorique à celui expérimental donné par le programme.

9.8. Somme de carrés successifs égale à 7440

1) *Trouver deux nombres entiers naturels consécutifs tels que leur somme multipliée par leur produit donne comme résultat le nombre 7440. Pour cela ne pas procéder par essais successifs, sauf en désespoir de cause, mais agir ainsi :*

Appeler x et x+1 ces deux nombres, et après avoir décomposé 7440 en produit de nombres premiers, commencer par montrer que x ne peut pas être pair (s'il l'était montrer de quelle forme il serait et constater que c'est impossible), puis trouver la seule solution possible.

La somme des deux nombres étant $2x + 1$, et leur produit $x(x + 1)$, on obtient l'équation :
$x(x + 1)(2x + 1) = 7440$. La décomposition de 7440 en produit de nombre premiers est :

$7440 = 2^4 \times 3 \times 5 \times 31$.

Distinguons deux cas :

* x pair. Alors $x + 1$ et $2x + 1$ sont impairs, et x doit contenir $2^4 = 16$ au moins. Si $x = 16$, $x + 1 = 17$, mais 17 n'est pas présent dans 7440. Au delà de 16, la plus petite valeur de x est $16 \times 3 = 48$, mais dans ce cas le produit $x (x + 1) (2x + 1)$ dépasse largement 7440. Inutile d'essayer d'autres valeurs de x encore plus grandes. Il n'y a pas de solution pour x pair.

* x impair. Alors $x + 1$ est pair et $2x + 1$ impair. C'est $x + 1$ qui doit contenir 2^4 au moins. Si $x + 1 = 16$, $x = 15$ et $2x + 1 = 31$. On vient de trouver une solution. Si $x + 1$ contient plus que 16, alors le produit $x (x + 1) (2x + 1)$ dépasse largement 7440.

Il existe une seule solution : $x = 15$.

2) *Combien faut-il prendre de nombres entiers successifs à partir de 1 pour que la somme de leurs carrés (soit : $1^2 + 2^2 + 3^2 + \ldots + n^2$) soit égale à 1240 ? Pour cela il faudra se souvenir de la formule sur la somme des carrés et utiliser la question 1°.*

On sait que $1^2 + 2^2 + 3^2 + \ldots + n^2 = n (n + 1) (2n + 1) / 6$. On veut obtenir 1240, soit :
$n (n + 1) (2n + 1) = 7440$, d'où $n = 15$, et l'on a $1^2 + 2^2 + 3^2 + \ldots + 15^2 = 1240$.

Pour aller plus loin :

[AUD2014] P. Audibert, Algorithmes et théorie des nombres, Ellipses 2014.