18 ♦◊◊ Bezout

Identité de Bezout
Soient a et b deux entiers relatifs et d leur PGCD alors il existe deux entiers u et v tels que :

$$au + bv = d$$

L'algorithme d'Euclide permet de calculer le pgcd de deux entiers naturels a et b tels que $a > b$.

Il consiste à réitérer les manipulations suivantes :

1. Effectuer la division euclidienne de a par b. Soit r le reste.
2. Remplacer a par b et b par r. On a $b > r$ d'après la définition de la division euclidienne.

Le pgcd est le dernier reste non nul.

Exemple d'application : calcul d'inverse modulaire

Déterminez d tel que $7d = 1 \mod 360$. (revient à calculer l'inverse de $7 \mod 360$).

$$\begin{array}{ccc} 360 & = & 51 \times 7 + 3 \\ 7 & = & 2 \times 3 + 1 \end{array}$$

puis "on remonte" :

$$\begin{array}{ccl} 1 & = & 7 - 2 \times 3 \mod 360 \\ 1 & = & 7 - 2 \times (360 - 51 \times 7) \mod 360 \\ 1 & = & 7 + 102 \times 7 \mod 360 \\ 1 & = & 7 \times (1 + 102) \mod 360 \\ 1 & = & 7 \times 103 \mod 360 \end{array}$$

D'où $d = 103$.

Entraînez-vous en déterminant d_1 et d_2 tels que : $17d_1 = 1 \mod 120$ puis $19d_2 = 1 \mod 520$

19 ♦◊◊ Calcul modulaire

Calculer de tête :

1. $2^{256} \mod 128$
2. $529^{436} \mod 66$
3. $1023^{4096} \mod 1024$

20 ♦◊◊ Square and Multiply

En utilisant l'algorithme *square and multiply*, montrer que :

$$41^{37} \mod 527 = 113; \qquad 5^7 \mod 403 = 346; \qquad 128^{17} \mod 407 = 50;$$

$$84^{113} \mod 143 = 2; \qquad 207^{219} \mod 583 = 192.$$

21 ♦♦◊ TP pari-gp square and multiply

Télécharger la dernière version de pari-gp ici : `http://bit.ly/28OgFEk`

Toujours créer un fichier `toto.txt` dans le même dossier que l'exécutable et lire ce fichier avec la commande `\r toto.txt`

Pour chercher une fonction faire `?name` pour avoir une aide sur la fonction, par exemple `?gcd`. Vous pouvez aussi utiliser la complétion automatique pour avoir la liste des fonctions.

Les deux algorithmes suivants prennent en entrée un entier positif m et un entier positif e.

```
{
a1(m,e)=
C=1;
for(i=1,e,C=C*m);
return(C);
}
{
a2(m,e)=
if(e==1,return(m));
if((e%2)==0,
return(a2(m,e/2)^2)
,return(a2(m,(e-1)/2)^2*m)
);
}
```

- Qu'est ce que ces algorithmes retournent ?
- Vérifiez vos résultats précédents à l'aide de ces deux fonctions.
- Laquelle est la plus efficace et pourquoi ?

CLEF PUBLIQUE

22 ♦♦◊ Théorème des restes chinois

Comment résoudre le système de congruences suivant :

$$\left\{\begin{array}{lllll} x & = & r_1 & \mod m_1 \\ x & = & r_2 & \mod m_2 \\ & & & \dots \\ x & = & r_k & \mod m_k \end{array}\right. \qquad ?$$

C'est le théorème des restes chinois qui nous fournit la réponse :

Soit k nombres entiers naturels $m_1, m_2, ..., m_k$, premiers entre eux deux à deux, et k entiers $r_1, r_2, ..., r_k$.

Le système de congruences

$$\left\{\begin{array}{llll} x & = & r_1 & \mod m_1 \\ x & = & r_2 & \mod m_2 \\ & & & \dots \\ x & = & r_k & \mod m_k \end{array}\right.$$

admet une unique solution modulo $M = m_1 m_2 ... m_k$.

La méthode permettant de construire une solution de ce système est fournit ci-dessous.

Posons $M_i = \frac{M}{m_i}$ pour $i = 1, 2, ..., k$. On a donc pgcd$(M_i, m_i) = 1$ et on peut ainsi trouver d'après l'identité de Bezout deux entiers u_i et v_i tel que $M_i u_i + m_i v_i = 1$.

On a alors : $u_1 M_1 r_1 + u_2 M_2 r_2 + ... + u_k M_k r_k = r_i \mod m_i$ pour $i = 1, 2, ..., k$

Par conséquent le nombre $x = u_1 M_1 r_1 + u_2 M_2 r_2 + ... + u_k M_k r_k$ est solution du système.

De plus si y est une autre solution de celui-ci, alors m_i divise $x - y$ pour chaque $i = 1, 2, ..., k$. Ainsi $x - y$ est divisible par M. Le système admet donc une seule solution modulo M.

Autrement dit, les solutions du système sont de la forme

$$x = u_1 M_1 r_1 + u_2 M_2 r_2 + ... + u_k M_k r_k + nM$$

avec n entier.

Application :

Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur.

Ils décident de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait trois pièces. Mais les pirates se querellent et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Survient alors un naufrage et seuls 6 pirates, le cuisinier et le trésor sont sauvés et le partage laisserait 5 pièces d'or à ce dernier.

Quelle est alors la fortune minimale que peut espérer ce dernier s'il décide d'empoisonner le reste des pirates ?

CLEF PUBLIQUE

23 ♦♦◇ Autour des nombres premiers

1. Pour quelles valeurs du nombre entier n le nombre $n^2-8n+15$ est-il premier ?
   Même question pour n^2+4n+3.
2. Pour quelles valeurs de n et m (entiers) le nombre $2n^2+5mn+3m^2$ est-il premier ?
3. Trouver 1 000 entiers naturels consécutifs, tous composés (non premiers).
4. - **Théorème :** Soit n un entier naturel. Si n est un nombre premier, alors pour tout entier a premier avec n, on a $a^{n-1}=1 \mod n$ (c'est-à-dire n divise $a^{n-1}-1$).
   - **Remarque :** Le théorème de Fermat peut être utilisé pour montrer qu'un entier n'est pas premier : si il existe un entier a premier avec n tel que $a^{n-1} \neq 1 \mod n$ alors n n'est pas premier.
   - **Application :** L'entier 37901 est-il premier ?

24 ♦♦♦ Test de primalité de Miller-Rabin

Soit p un nombre premier impair que l'on écrit sous la forme $p=2^s\times d+1$. Soit $a\in\{1,\dots,p-1\}$. On définit une suite récurrente (b_i) en posant : $b_i=a^{d\times 2^i}$.

1. Montrer que dans $\mathbb{Z}/p\mathbb{Z}$, l'équation $x^2=1$ entraine $x=1$ ou $x=-1$.
2. Montrer que $b_s\equiv 1 \mod p$.
3. On suppose que b_0 n'est pas congru à 1 modulo p.
   Montrer l'existence de $i\in\{0,\dots,s-1\}$ tel que $b_i\equiv -1 \mod p$.
4. En déduire un test de non-primalité d'un entier.

25 ♦♦♦ Algorithme $p-1$ de Pollard

Le but est de trouver un facteur non trivial de $n=19\,048\,567$. On prend $B=19$ et $a=3$.

1. Vérifier que pgcd$(a,n)=1$.
2. Déterminer, pour chaque nombre premier $\leqslant 19$, sa plus grande puissance qui soit $\leqslant n$.
   Soit Q le ppcm de toutes ces puissances, et p un *hypothétique* fecteur premier de n tel que $p-1$ soit 19-friable [a].
3. Montrer que $p-1$ divise Q.
4. En déduire que p divise a^Q-1 (on pourra utiliser le petit théorème de Fermat).
5. En déduire que $\gcd(a^Q-1,n)(=\gcd((a^Q-1) \mod n,n))$ est différent de 1.
6. On admet le calcul intermédiaire $a^Q \mod n=554\,56$. En déduire numériquement un facteur non-trivial de n.

a. C'est-à-dire que tous les facteurs premiers sont inférieurs à 19.

CLEF PUBLIQUE