

Contrôle du 7 octobre 2011 durée 1h30

Sans document.

Les réponses aux questions théoriques doivent être rédigées rigoureusement.

Les réponses aux questions utilisant Maple doivent comporter les commandes tapées, leurs résultats et vos commentaires.

– Exercice 1 (1 point) Rédaction

La qualité de la rédaction vaut 1 point.

– Exercice 2 (4 points) Equations diophantiennes linéaires

Résoudre dans \mathbf{Z} les équations :

- $241662x + 372160y = 669308$
- $105411x + 392506y = 160517$

On demande toutes les solutions et la suite de calculs pour les obtenir.

Explicitez le lien entre vos solutions et celles de la commande **isolve** de Maple.

– Solution

Equation $241662x + 372160y = 669308$

On calcule une relation de Bézout entre 241662 et 372160 :

```
[ > igcdex(241662,372160,'u','v');u;v;
      2
     -85889
     55772
```

Le pgcd vaut 2 et divise 669308, il y a donc des solutions qui sont :

```
[ > sols:={x=u*669308/2+k*372160/2,y=v*669308/2-k*241662/2};
      sols:={x=-28743097406+186080k,y=18664322888-120831k}
```

Une vérification :

```
[ > subs(sols,241662*x+372160*y);
      669308
```

Une autre vérification :

```
[ > isolve(241662*x+372160*y=669308);
      {x=-64126-186080_N1,y=41642+120831_N1}
```

On remarque qu'on a les mêmes coefficients pour k (au signe près) mais que Maple n'utilise pas la même solution initiale à raison, il part d'une solution bien plus petite. Comment la retrouver ?

On va chercher k pour que y soit le plus petit possible :

```
[ > iquo(18664322888,120831);
      154466
[ > subs(k=154466,sols);
      {x=-64126,y=41642}
```

On retrouve bien la solution de Maple.

Equation $105411x + 392506y = 160517$

On calcule une relation de Bézout entre 105411 et 392506 :

```
[ > igcdex(105411, 392506, 'u', 'v') ;  
                                         857
```

Le pgcd ne divise pas 160517 :

```
[ > irem(160517, 857) ;  
                                         258
```

Il n'y a donc pas de solution

```
[ > isolve(105411*x+392506*y=160517) ;
```

ce que confirme Maple.

Exercice 3 (5 points) Equations modulaires

Résoudre dans $\mathbf{Z}/n\mathbf{Z}$ les équations :

- $257784x = 232773 \pmod{879615}$

- $98031x = 111872 \pmod{365026}$

On demande toutes les solutions et la suite de calculs pour les obtenir.

Vérifiez avec la commande **msolve** de Maple.

Solution

Equation $257784x = 232773 \pmod{879615}$

On résoud l'équation $257784x + 879615y = 232773$ mais on ne s'intéresse qu'aux valeurs de x distinctes modulo 879615.

```
[ > igcdex(257784, 879615, 'u') ;  
                                         3
```

Le pgcd vaut 3 et divise bien le second membre :

```
[ > irem(232773, 3) ;  
                                         0
```

Les solutions dans \mathbf{Z} sont :

```
[ > x=u*232773/3+k*879615/3 ;  
                                          $x = 11082477712 + 293205k$ 
```

La solution initiale n'étant pas très agréable on en calcule une meilleure (ça n'est pas obligatoire)

```
[ > irem(11082477712, 293205) ;  
                                         208327
```

Les solutions modulo 879615 sont obtenues en partant de cette solution initiale et en faisant varier k de 0 au pgcd - 1.

```
[ > seq(208327+293205*k, k=0..3-1) ;  
                                         208327, 501532, 794737
```

On compare à Maple :

```
[ > msolve(257784*x=232773, 879615) ;  
                                         {x = 501532}, {x = 794737}, {x = 208327}
```

Equation $98031x = 111872 \pmod{365026}$

De même on cherche les solutions de $98031x + 365026y = 111872$

```
[ > igcdex(98031, 365026, 'u') ;  
                                         797
```

Le pgcd ne divise pas le second membre :

```
[ > irem(111872,797);
```

292

Il n'y a donc pas de solution, ce que confirme Maple :

```
[ > msolve(98031*x=111872,365026);
```

Exercice 4 (10 points) Test de primalité

- Montrer que si n est un nombre premier impair alors l'équation $x^2 = 1 \pmod n$ a pour seules solutions $x = 1 \pmod n$ ou $x = (-1) \pmod n$.
- Soit n un nombre premier impair et a un entier compris entre 1 et $n-1$, montrer que $a^{\binom{n-1}{2}}$ est égal à 1 ou -1 modulo n .
- Ecrire une procédure `TestPremier(n,a)` qui effectue le test ci-dessus et rend **true** si n est peut-être premier, **false** sinon.
- Donner tous les n non premiers entre 1000 et 2000 pour lesquels ce test répond **true** avec $a = 6$.

Solution

- Si x est solution de $x^2 = 1 \pmod n$ alors n divise $x^2 - 1 = (x-1)(x+1)$ or n est premier donc n divise $x-1$, c'est à dire $x = 1 \pmod n$, ou n divise $x+1$, c'est à dire $x = (-1) \pmod n$.
- Si n est un nombre premier et a un entier compris entre 1 et $n-1$ alors $a^{(n-1)} = 1 \pmod n$ (Théorème de Fermat), si de plus n est impair $\frac{n-1}{2}$ est un entier et $a^{\binom{n-1}{2}}$ est de carré 1 donc égal à 1 ou -1 modulo n .
- Pour éviter le double calcul on met le résultat de $a^{\binom{n-1}{2}} \pmod n$ dans une variable c . On peut remarquer l'utilisation de l'opérateur `&^` pour le calcul de la puissance modulaire et que cette procédure n'est pas bien définie si n est pair.

```
[ > TestPremier:=proc(n,a)
  local c;
  c:=a&^((n-1)/2) mod n;
  c=1 or c=n-1
end;
```

- On fait une boucle qui ne teste que les impairs :

```
[ > l:=NULL;
  for n from 1001 by 2 to 2000 do
    if (not isprime(n)) and TestPremier(n,6) then l:=l,n fi
  od;
  l;

  l:=
  1111, 1261, 1333, 1729
[ > ifactor(1111),ifactor(1261),ifactor(1333),ifactor(1729);
```

┌ ┌ ┌ (11) (101), (13) (97), (31) (43), (7) (13) (19)
└ └ └ On a 4 nombres non premiers pour lesquels le test répond vrai.