

UNIVERSITÉ PARIS DIDEROT - PARIS 7
Année 2008-2009, Licence 2, MI4
Groupes et arithmétique

Examen du 25/06/09 (durée : 3 heures)

Document autorisé : résumé de cours manuscrit sur une page recto-verso de format A4 (21×29,7).

La calculatrice est autorisée.

On demande de rédiger les détails de calcul.

I

1. Expliquer pourquoi 12 est inversible dans $\mathbb{Z}/25\mathbb{Z}$ et calculer son inverse.
2. Résoudre l'équation

$$12x \equiv 7 \text{ modulo } 25 .$$

3. Résoudre dans $\mathbb{Z}$ le système de congruences suivant.

$$\begin{cases} 12x \equiv 7 \text{ modulo } 25 \\ x \equiv 2 \text{ modulo } 21 \end{cases}$$

II

1. Donner la liste complète des éléments du groupe multiplicatif $\mathcal{U}(\mathbb{Z}/20\mathbb{Z})$.
2. Montrer que le groupe $(\mathcal{U}(\mathbb{Z}/20\mathbb{Z}), \times)$ n'est pas cyclique. (On pourra au choix utiliser le théorème chinois, ou calculer l'ordre de chaque élément.)
3. Calculer le reste de la division euclidienne de 383^{127} par 20.

III

1. Factoriser 6601.
2. Est-ce que 6601 est un nombre de Carmichael ?

Pour $k \in \mathbb{N}^*$, on pose :

$$a_k = 6k + 1 , \quad b_k = 12k + 1 , \quad c_k = 18k + 1 , \quad N_k = a_k b_k c_k .$$

3. Montrer que si les trois nombres a_k , b_k et c_k sont premiers, alors N_k est un nombre de Carmichael.
4. Montrer que N_6 est un nombre de Carmichael.

IV

On note F_n le n -ième nombre de Fermat : $F_n = 2^{2^n} + 1$.

1. Calculer F_2 et F_3 . Sont-ils premiers ?
2. Calculer les symboles de Legendre $\left(\frac{F_1}{3}\right)$ et $\left(\frac{F_2}{3}\right)$, puis $\left(\frac{F_n}{3}\right)$ pour $n \geq 1$.
3. Pour $n \geq 1$, utiliser la formule de réciprocité pour calculer le symbole de Legendre $\left(\frac{3}{F_n}\right)$ lorsque F_n est premier.
4. Démontrer que si F_n , $n \geq 1$, est premier alors $3^{\frac{F_n-1}{2}}$ est égal à -1 modulo F_n .
5. Calculer F_4 . Expliquer comment calculer efficacement $3^{\frac{F_4-1}{2}}$ modulo F_4 , et donner la réponse en utilisant le résultat du premier script ci-dessous.
6. Quel est l'ordre de 3 dans la groupe $\mathcal{U}(\mathbb{Z}/F_4\mathbb{Z})$? En déduire que F_4 est premier.
7. Est-ce que F_5 est premier ?

```
p=3
for k in range(16):
    print k, ' ', p
    p=(p^2)%(2^(2^4)+1)
```

```
0  3
1  9
2  81
3  6561
4  54449
5  61869
6  19139
7  15028
8  282
9  13987
10 8224
11 65529
12 64
13 4096
14 65281
15 65536
```

```
p=3
for k in range(32):
    print k, ' ', p
    p=(p^2)%(2^(2^5)+1)
```

```
0  3
1  9
2  81
3  6561
4  43046721
5  3793201458
6  1461798105
7  852385491
8  547249794
9  1194573931
10 2171923848
11 3995994998
12 2840704206
13 1980848889
14 2331116839
15 2121054614
16 2259349256
17 1861782498
18 1513400831
19 2897320357
20 367100590
21 2192730157
22 2050943431
23 2206192234
24 2861695674
25 2995335231
26 3422723814
27 3416557920
28 3938027619
29 2357699199
30 1676826986
31 10324303
```