Université de Metz
Département de Mathématiques

Année universitaire 2015-2016.

L3 Calcul formel

Feuille de TD n° 1

Exercice 1

Soient p un nombre premier, n et m des entiers tels que $0 < n < m$.

1) Déterminer le reste de la DE de $p^m - 1$ par $p^n - 1$.

2) En déduire que $pgcd(p^m - 1, p^n - 1) = p^{pgcd(m,n)} - 1$.

Exercice 2 (Examen 1999-2000)

1) Soient a, b, $m \neq 0$ des entiers. Formuler et démontrer une condition nécessaire et suffisante pour que la congruence

$$ax \equiv b \mod m$$

admette une solution. Décrire une méthode pour trouver une solution. Examiner la question de l'unicité des solutions.

2) Résoudre les congruences

$$23699x \equiv 1 \mod 253921,$$

$$22646x \equiv 26 \mod 70616.$$

Exercice 3

Soient $n \in \mathbb{N}^*$ et $s_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ la surjection canonique. On note $U(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

1. Vérifier que $(U(\mathbb{Z}/n\mathbb{Z}), .)$ est un groupe.

2. Démontrer que $s_n(x)$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si p.g.c.d$(x, n) = 1$.En déduire que le cardinal $\varphi(n)$ de $U(\mathbb{Z}/n\mathbb{Z})$ est égal au nombre des entiers q tels que

$$0 \leq q \leq n, \quad \text{p.g.c.d } (n, q) = 1$$

3. Démontrer que $U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z}) = U(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$. En déduire, en utilisant le théorème chinois, que si p.g.c.d $(n, m) = 1$, $\varphi(mn) = \varphi(n).\varphi(m)$.

4. Démontrer que $\varphi(n) = n. \prod_{\substack{\text{p premier} \\ \text{p|n}}} \left(1 - \frac{1}{p}\right)$.

5. Si a et n sont deux entiers premiers entre eux, démontrer que $a^{\varphi(n)} \equiv 1 \mod n$. Ce résultat est connu sous le nom de *théorème d'Euler*.

Application : calculer 63^{21} modulo 23 , 1990^{7279} modulo 7 et 1990^{7203} modulo 143 .

Exercice 4 (Examen Janvier 2014)

Donner les trois derniers chiffres en base 10 du nombre 2013^{399}.

Exercice 5 (Examen Janvier 2014)

1. A l'aide de l'algorithme de Garner, résoudre le système de congruences
   (on donnera une solution particulière puis l'ensemble de toutes les solutions)

$$\begin{cases} x \equiv -2 \mod 11 \\ x \equiv 2 \mod 17 \\ x \equiv -6 \mod 19 \\ x \equiv 14 \mod 31 \end{cases}$$

2. Quelle est la plus petite valeur positive de x ? Justifier.

Exercice 6 Les pirates et le cuisinier chinois (Mars 2010)

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

Exercice 7 (Janvier 2015)

A l'aide de l'algorithme de Garner, résoudre le système de congruences simultanées suivant :

$$\begin{cases} 5x \equiv 4 \mod 3 \\ 3x \equiv 1 \mod 5 \\ 6x \equiv -9 \mod 33 \\ 5x \equiv 10 \mod 35 \end{cases}$$

Exercice 8 (Janvier 2015)

Résoudre le système suivant :

$$\begin{cases} 3x + 4y \equiv 5 \mod 13 \\ 2x + 5y \equiv 7 \mod 13 \end{cases}$$