UFR Sciences
M2 Calcul Formel

2021–2022
Martin WEIMANN

Examen Calcul Formel 2021-2022

Durée 4h00. Dans chaque exercice, les questions précédées de *(Maxima)* sont à faire dans un fichier maxima que vous déposerez sur ecampus à la fin de l'examen. Les autres questions sont à résoudre sur papier. Une note pour chaque rendu. La clarté, la justification des réponses et la présentation des copies seront prises en compte. Notes de CM et TP autorisées.

Exercice 1 (calculs de pgcd)

1. Soit $n \in \mathbb{Z}$. Déterminer le pgcd de n^2+2n+3 et n^2+n+9 en fonction des valeurs de n.
2. *(Maxima)* Vérifier votre résultat en considérant $n=12$, $n=23$ et $n=57$ et $n=100$.
3. Soient n, a, b trois entiers positifs. Démontrer que $\mathrm{pgcd}(n^a-1, n^b-1) = n^{\mathrm{pgcd}(a,b)}-1$.
4. *(Maxima)* Vérifier votre résultat en considérant $n=12$, $a=20$ et $b=32$.

Correction. 1. Soit $d = \mathrm{pgcd}(n^2, n^2+n+29)$, $d>0$. On a $n^2+2n+3 = (n^2+n+9)+(n-6)$ donc $d = \mathrm{pgcd}(n^2+n+9, n-6)$. On a $n^2+n+9 = n(n-6)+7n+9$ donc $d = \mathrm{pgcd}(n-6, 7n+9)$. On a $7n+9 = 7(n-6)+51$ donc $d = \mathrm{pgcd}(n-6, 51)$. Or $51 = 3\times 17$, avec 3 et 17 premiers. Donc $d=51$ si $n = 0 \mod 3$ et $n = 6 \mod 17$, $d=3$ si $n=0 \mod 3$ et $n \neq 6 \mod 17$, $d=17$ si $n\neq 0 \mod 3$ et $n=6 \mod 17$ et $d=1$ sinon.

2.

```
P:n^2+2*n+3$ Q:n^2+n+9$
gcd(ev(P,n=12),ev(Q,n=12));
gcd(ev(P,n=23),ev(Q,n=23));
gcd(ev(P,n=57),ev(Q,n=57));
gcd(ev(P,n=100),ev(Q,n=100));
```

3. Soit $a = qb+r$ la division euclidienne de a par b (suppose $a>b$). Puisque $g = \mathrm{pgcd}(a,b) = \mathrm{pgcd}(b,r)$ s'obtient par divisions euclidiennes successives, il suffit (par induction) de montrer que $\mathrm{pgcd}(n^a-1, n^b-1) = \mathrm{pgcd}(n^b-1, n^r-1)$. Il suffit donc de montrer que $n^a-1 = k(n^b-1)+n^r-1$ pour un $k\in\mathbb{N}$ i.e. $n^a \equiv n^r \mod n^b-1$. On a $n^a = n^{qb+r} = (n^b)^q n^r = (n^b-1+1)^q n^r \equiv n^r \mod n^b-1$. D'où le résultat.

4.

```
gcd(12^(20)-1,12^(32)-1);
12^(gcd(20,32))-1;
```

Exercice 2 (restes chinois multiples)

1. Soient $n_1, \ldots, n_k \in \mathbb{N}$ des entiers deux à deux premiers entre eux. Rappeler (en justifiant vos calculs) comment déterminer les solutions $x\in\mathbb{Z}$ du système

$$\begin{cases} x &= a_1 \mod n_1 \\ x &= a_2 \mod n_2 \\ &\vdots \\ x &= a_k \mod n_k \end{cases}.$$

2. *(Maxima)* Résoudre le problème suivant : il y a entre 2000 et 5000 étudiants dans une université. Lorsque ces étudiants sont répartis en classe de 12, il en reste 8 sans places, en classe de 13, il en reste 5 sans places et en classe de 17, il en reste 9 sans place. Combien y a-t-il d'étudiants ?

Correction. 1. Soit $n = n_1 \cdots n_k$ et $\hat{n}_i = n/n_i$. Donc $\hat{n}_i$ est premier avec n_i. On calcule une relation de Bezout $u_i n_i + v_i \hat{n}_i = 1$. Les solutions du système sont $x = (\sum_i v_i \hat{n}_i a_i) + kn$, $k \in \mathbb{Z}$.

2.

```
n1:12$ n2:13$ n3:17$  n:n1*n2*n3$ n1hat:n/n1$ n2hat:n/n2$ n3hat:n/n3$
[u1,v1,d1]:gcdex(n1,n1hat);
[u2,v2,d2]:gcdex(n2,n2hat);
[u3,v3,d3]:gcdex(n3,n3hat);
x:mod(8*v1*n1hat+5*v2*n2hat+9*v3*n3hat,n);
On trouve $x=1760\mod n$. La seule solution dans $[2000,5000]$ est $4412$.
```

Exercice 3 (racines carrées modulo N)

1. Soit N un produit de k nombres premiers deux à deux distincts. Montrer à l'aide du théorème des restes chinois que l'équation $x^2 = 1$ dans $\mathbb{Z}/N\mathbb{Z}$ admet exactement 2^k solutions distinctes.
2. *(Maxima)* Résoudre l'équation $x^2 = 1$ dans $\mathbb{Z}/4301\mathbb{Z}$.

Correction. 1. On écrit $N = p_1 \cdots p_k$. On a un iso $\mathbb{Z}/N\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \cdots \mathbb{Z}/p_k\mathbb{Z}$, donc résoudre équation $mod N$ revient à résoudre les équations $mod p_i$ pour chaque i. Il y a exactement deux solutions $r_i \in \{\pm 1 \mod p_i\}$ dans le corps $\mathbb{Z}/p_i\mathbb{Z}$ et chacun des 2^k k-uplets $(r_1, \ldots, r_k)$ se relève en une unique solution $r \mod N$. On a donc 2^k solutions solutions distinctes. Attention, comme me l'a fait remarquer l'un d'entre vous, il faut supposer N impair. En effet, l'équation $x^2 = 1 \mod 2$ a une seule solution (double).

2.

```
 ifactors(4301);
 On trouve 4301 = 11* 17* 23. Les facteurs premiers de 4301 ont multiplicité 1, donc on doit trouver 8 
résoud avec les restes chinois les 8 systèmes d'équations
x = +- 1 mod 11
x= +-1 mod 17
x= +-1 mod 23
(en copiant les lignes de commandes de l'exo 2 avec les nouvelles valeurs de
n1,n2,n3).

[u1,v1,d1]:gcdex(n1,n1hat)$
[u2,v2,d2]:gcdex(n2,n2hat)$
[u3,v3,d3]:gcdex(n3,n3hat)$
L:[]$
x:mod(v1*n1hat+v2*n2hat+v3*n3hat,n)$
L:append(L,[x])$
x:mod(v1*n1hat+v2*n2hat-v3*n3hat,n)$
L:append(L,[x])$
x:mod(v1*n1hat-v2*n2hat+v3*n3hat,n)$
L:append(L,[x])$
x:mod(-v1*n1hat+v2*n2hat+v3*n3hat,n)$
L:append(L,[x])$
x:mod(v1*n1hat-v2*n2hat-v3*n3hat,n)$
L:append(L,[x])$
x:mod(-v1*n1hat+v2*n2hat-v3*n3hat,n)$
L:append(L,[x])$
x:mod(-v1*n1hat-v2*n2hat+v3*n3hat,n)$
L:append(L,[x])$
```

```
x:mod(-v1*n1hat-v2*n2hat-v3*n3hat,n)$
L:append(L,[x])$
L;
On trouve finalement que les solutions de x^2=1 mod 4301 sont
[1,1310,254,2738,1563,4047,2991,4300].
```

Exercice 4 (opérations sur complexes) On représente un nombre complexe $z \in \mathbb{C}$ sous sa forme algébrique $z = a + ib$, avec $a, b \in \mathbb{R}$.

1. Montrer que l'on peut multiplier deux nombres complexes en utilisant 3 multiplications réelles (on ne s'intéresse pas aux additions ou soustractions).
2. *(Maxima)* Ecrire un tel programme de multiplication des complexes et calculer le temps requis pour effectuer 10000 produits $(a + ib)(c + id)$ avec a, b, c, d aléatoires dans $[-1000, 1000]$. Comparer avec maxima (sans oublier `expand` pour effectuer les produits).

Correction. 1. On a les formules $(a + bi)(c + di) = (ac - bd) + (ad + bc)i =: x + iy$. Il faut a priori 4 multiplications réelles. Notons $u = (a+b)(c+d)$, $v = ac$, $w = bd$. On a alors $x = v - w$ et $y = u - v - w$. Il faut donc seulement 3 multiplications selon cette méthode.

2.

```
ProduitComplexe(a,b,c,d):=block( [u,v,w],
    u:(a+b)*(c+d),
    v:a*c,
    w:b*d,
    return(v-w+(u-v-w)*%i)
    )$

t:elapsed_run_time()$
for i:1 thru 10000 do
    (a:random(2000)-1000,
     b: random(2000)-1000,
     c: random(2000)-1000,
     d: random(2000)-1000,
     ProduitComplexe(a,b,c,d)
)$
elapsed_run_time()-t;

t:elapsed_run_time()$
for i:1 thru 10000 do
    (a:random(2000)-1000,
     b: random(2000)-1000,
     c: random(2000)-1000,
     d: random(2000)-1000,
     expand((a+b*%i)*(c+d*%i))
)$
elapsed_run_time()-t;
```

TSVP !

Exercice 5 (corps finis) On considère le polynôme $Q = X^9 - X + 1 \in \mathbb{F}_3[X]$.

1. Montrer que Q n'a pas de racines dans $\mathbb{F}_3$ et $\mathbb{F}_9$.
2. Montrer que $\mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(X^3 - X - 1)$.
3. Montrer que toute racine $\alpha \in \mathbb{F}_{27}$ du polynôme $X^3 - X - 1$ est une racine de Q.
4. Justifier que tout $x \in \mathbb{F}_{27}$ s'écrit de manière unique $x = a\alpha^2 + b\alpha + c$ avec $a, b, c \in \mathbb{F}_3$. En déduire toutes les racines de Q dans $\mathbb{F}_{27}$.
5. Factoriser Q dans $\mathbb{F}_3[X]$.
6. *(Maxima)* Fabriquer un polynôme aléatoire unitaire $P \in \mathbb{F}_3[X]$ de degré 9 et déterminer ses racines dans $\mathbb{F}_{27}$. Combien de racines en moyenne sur 100 tirages ?

Correction. 1. Soit $z \in \mathbb{F}_9$. On a donc $z^9 = z$ et $Q(z) = 1 \neq 0$. Donc Q n'a pas de racines dans $\mathbb{F}_9$ (ni a fortiori dans $\mathbb{F}_3$).

2. On remarque que $P := X^3 - X - 1$ n'a pas de racines dans $\mathbb{F}_3$. Etant de degré 3, il est nécessairement irréductible (sinon, il aurait un facteur de degré 1, donc une racine dans $\mathbb{F}_3$). Ainsi, $\mathbb{F}_3[X]/(X^3 - X - 1)$ est un corps, de cardinal $3^3 = 27$. Comme deux corps finis de même cardinal sont isomorphes, le résultat suit.

3. Si $\alpha^3 = \alpha + 1$, alors $\alpha^9 = \alpha^3 + 1 = \alpha + 2 = \alpha - 1$ (la première égalité par $\mathbb{F}_3$-linéarité du Frobenius).

4. Tout $x \in \mathbb{F}_{27}$ s'écrit de manière unique $x = a\alpha^2 + b\alpha + c$ avec $a, b, c \in \mathbb{F}_3$ d'après 2. Donc $x^9 = a\alpha^{18} + b\alpha^9 + c\alpha$ avec $\alpha^9 = \alpha - 1$ et donc $\alpha^{18} = \alpha^2 + \alpha + 1$, de sorte que $x^9 - x + 1 = a\alpha + a - b + 1$. Donc x racine de Q ssi $a = 0$ et $b = 1$ soit $x = \alpha, \alpha + 1, \alpha - 1$.

5. D'après 3., on sait que le polynôme minimal P de α divise Q. Donc $Q = PR$, avec $R \in \mathbb{F}_3[X]$ de degré 6. Or R n'a pas de racines dans $\mathbb{F}_3$ et $\mathbb{F}_9$ (d'après 1.), ni dans $\mathbb{F}_{27}$ (d'après 3. et 4.). Donc R n'admet aucun facteur irréductible de degré $1, 2, 3$ puisque tout polynôme irréductible de degré k a une racine dans $\mathbb{F}_{3^k}$ (en fait toutes ses racines y sont). Donc R est irréductible. Une division euclidienne de Q par P permet de calculer $R = X^6 + X^4 + X^3 + X^2 - X - 1$.

6.

```
RandomPol(d,p):=block([],
    return (X^d+sum(random(3)*X^(i-1),i,1,d)))$

Racines(P):=block([L,res],
    modulus:3,
    L:[],
    for a:0 thru 2 do
        for b:0 thru 2 do
            for c:0 thru 2 do
                (res:remainder(ev(P,X=a*t^2+b*t+c),t^3-t-1),
                if res=0 then L:append(L,[a*t^2+b*t+c])),
    modulus:false,
    return (L)
    )$

TestNbreRacines(N):=block([compt,P],
    compt:0,
    for i:1 thru N do
        (P:RandomPol(9,3),
         compt:compt+length(Racines(P))),
    return (compt/N)
    )$

TestNbreRacines(100);

On trouve environ 2 racines dans F_27 en moyenne.
```

Exercice 6 (récurrences linéaires à coefficients constants) Une récurrence linéaire d'ordre d à coefficients constants est définie par

$$a_{n+d} = c_0 a_n + \cdots + c_{d-1} a_{n+d-1} \tag{1}$$

avec $c_i \in K$ (K un corps fixé), les valeurs initiales $a_0, \ldots, a_{d-1}$ étant fixées.

1. Déterminer une matrice M telle que

   $$(a_{n+1}, \ldots, a_{n+d}) = (a_n, \ldots, a_{n+d-1}).M$$

   Comment appelle-t-on ce type de matrice ?

2. En déduire que l'on a pour tout $n \in \mathbb{N}$ la relation

   $$(a_n, a_{n+1}, a_{n+d-1}) = (a_0, \ldots, a_{d-1}).M^n$$

3. *(Maxima)* Déduire un programme basé sur l'exponentiation rapide des matrices qui calcule le n-ème terme de la suite de Tribonacci $T_0 = 0, T_1 = T_2 = 1, T_{n+3} = T_n + T_{n+1} + T_{n+2}$. Que vaut T_{20} ?

4. Exprimer en fonction de n et d la complexité du calcul de a_n avec l'exponentiation rapide des matrices (on supposera que l'on utilise la multiplication naïve des matrices).

5. On veut améliorer la dépendance en d de la complexité du calcul de a_n en profitant de la structure de la matrice M. On introduit pour cela le *polynôme caractéristique*

   $$P = X^d - c_{d-1} X^{d-1} - \cdots - c_0$$

   associé à la récurrence linéaire (1).

   (a) Montrer que M coïncide avec la matrice de multiplication par X dans l'algèbre $K[X]/(P)$ munie de la base canonique $(1, X, \ldots, X^{d-1})$.

   (b) En déduire que pour tout $n \in \mathbb{N}$, la première colonne C_n de M^n représente les coordonnées de $X^n \mod P$ dans la base $(1, \ldots, X^{d-1})$.

   (c) Justifier que pour tout $n \in \mathbb{N}$, on a $a_n = (a_0, a_1, \ldots, a_{d-1}).C_n$.

   (d) *(Maxima)* Ecrire un programme basé sur l'exponentiation rapide dans $\mathbb{Q}[X]/(P)$ qui, étant donnés $c = [c_0, \ldots, c_{d-1}]$, $a = [a_0, \ldots, a_{d-1}]$ et $n \in \mathbb{N}$, calcule le n-ème terme a_n de la suite récurrente linéaire (1). Vérifier que votre programme fonctionne en calculant T_{20}.

   (e) En supposant que l'on utilise multiplication et division euclidienne rapides dans $\mathbb{Q}[X]$, estimer le nombre d'opérations dans $\mathbb{Q}$ utilisées par votre programme. Quelle méthode est préférable ?

Correction. 1. On remarque que M est la matrice compagnon

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{d-1} \end{pmatrix}$$

2. Immédiat par récurrence.
3.

```
PuissMat(M,n):=block([d],
    d:length(M),
    if n=0 then
        return(ident(d)),
    Mcarre:M.M,
    if mod(n,2)=0 then
        return(PuissMat(Mcarre,n/2)),
    return(M.PuissMat(Mcarre,(n-1)/2))
```

```
    )$

Trib(n):=block([M,L],
    M:matrix([0,0,1],[1,0,1],[0,1,1]),
    L:matrix([0,1,1]).PuissMat(M,n),
    return(L[1][1])
    )$

Trib(20);
On trouve T_{20}=66012.
```

4. L'exponentiation rapide conduit à $\log_2(n)$ multiplications de matrices de $\mathcal{M}_d(K)$, chaque multiplication en $O(d^3)$, et une multiplication matrice vecteur en $O(d^2)$. Au total $O(\log(n)d^3)$ opérations dans K.

5.a) Soit $m : K[X]/(P) \to K[X]/(P)$ la multiplication par X. On a donc $m(X^i \mod P) = X^{i+1} \mod P$ pour tout $i < d-1$ et $m(X^{d-1} \mod P) = X^d \mod P = c_0 + \cdots + c_{d-1}X^{d-1}$. D'où le résultat.

5.b) La matrice M^n représente la composée n-ième m^n de l'endomorphisme m, i.e. la multiplication par X^n. La première colonne C_n de M^n représente donc les coordonnées de $m^n(1) = X^n \mod P$ dans la base $(1, \ldots, X^{d-1})$.

5.c) Découle immédiatement de 2.

5.d)

```
PuissModP(Q,P,n):=block([Qcarre],
    if n=0 then
        return(1),
    Qcarre:remainder(Q^2,P),
    if mod(n,2)=0 then
        return(PuissModP(Qcarre,P, n/2)),
    return(remainder(Q*PuissModP(Qcarre,P,(n-1)/2),P))
    )$

niemeTerme(c,a,n):=block([d,P,C,res],
    d:length(a),
    P:X^d-sum(c[i+1]*X^i,i,0,d-1),
    C:PuissModP(X,P,n),
    res:sum(a[i+1]*coeff(C,X,i),i,0,d-1),
    return(res)
    )$

Trib2(n):=block([c,a],
    c:[1,1,1],
    a:[0,1,1],
    return(niemeTerme(c,a,n))
    )$

Trib2(20);

On retrouve bien T_{20}=66012.
```

5.e) Le calcul de $X^n \mod P$ coûte $\log(n)$ multiplications dans $K[X]/(P)$ avec l'exponentiation rapide, et chaque multiplication dans $K[X]/(P)$ coûte $\tilde{O}(\deg P) = \tilde{O}(d)$ opérations dans K (produit dans $K[X]$ en degré d puis calcul du reste de la division euclidienne par P). D'où $\tilde{O}(\log(n)d)$ opérations dans K pour le calcul de C_n. Le calcul de a_n nécessite ensuite $O(d)$ opérations dans K (produit scalaire). Au total : $\tilde{O}(\log(n)d)$ opérations dans K. On est passé d'une complexité cubique en d à une complexité linéaire en d.