

Arithmétique

Les entiers

Entiers et opérations de base

Maple travaille avec des entiers non limités en taille et sait effectuer sur ces entiers les opérations algébriques classiques dans \mathbb{Z} : somme, différence, produit, puissance, factorielle

```
> 123456789987654321*74185223963587942358;  
9158669615059777284626146395377628918
```

```
> 100!;  
93326215443944152681699238856266700490715968264381621468592963895217599993229915608941463976156518286253697920\  
8272237582511852109168640000000000000000000000000
```

```
> 2^128;
340282366920938463463374607431768211456
```

□ D'autre part, les fonctions `iquo` et `irem` donnent accès au quotient et au reste de la division euclidienne:

```
> iquo(1598472635738642,14789632);
```

```
> irem(1598472635738642,14789632);
```

10027538

Divisibilité

□ Les fonctions `igcd` et `ilcm` calculent le pgcd et le ppcm de deux entiers

```
> igcd(3^24-1,3^36-1);
```

```
> ilcm(3^24-1,3^36-1);
```

79766593171507806331040

□ La fonction `igcdex` renvoie (par effet de bord), en plus du pgcd, un couple de Bézout:

```
> igcdex(2^11-1,2^10-1,u,v);
```

```
> u*(2^11-1)+v*(2^10-1);
```

La fonction divisors du package numtheory, que l'on peut utiliser directement à l'aide de la syntaxe numtheory[divisors], calcule l'ensemble des diviseurs d'un nombre

```
> numtheory[divisors](2^12-1);
```

{ 13, 9, 5, 7, 15, 3, 21, 35, 39, 45, 63, 65, 91, 105, 117, 1, 195, 585, 455, 273, 819, 315, 4095, 1365 }

La fonction phi du package numtheory, que l'on peut utiliser directement à l'aide de la syntaxe numtheory[phi], calcule l'indicateur d'Euler d'un nombre

```
> numtheory[phi](2^9-1);
```

432

Factorisation, nombres premiers

La fonction ifactor calcule la décomposition en nombres premiers d'un nombre entier

```
> ifactor(2^12-1);
```

$(3)^2 (5) (7) (13)$

La fonction isprime teste si un nombre est premier (en fait il s'agit là d'un test probabiliste qui donne une quasi certitude que le nombre est premier)

```
> isprime(104729);
```

true

```
> isprime(2^11-1);
```

false

La fonction ithprime renvoie le i-ième nombre premier, alors que la fonction nextprime renvoie le nombre premier suivant un nombre donné

```
> ithprime(1997);
```

17377

```
> nextprime(1997);
```

1999

Z/nZ

Calcul algébrique dans Z/nZ

Le calcul modulo n s'effectue très facilement: il suffit de faire suivre chaque opération de l'expression ? mod n.

```
> 2^100 mod 37;
```

12

```
> 123456789*654987321 mod 256;
```

173

```
> 10^(-1) mod 31;
```

28

Puissances dans Z/nZ

Les trois fonctions msqrt, mroot, imagunit du package numtheory, que l'on peut utiliser directement à l'aide de la syntaxe complète numtheory[msqrt], numtheory[mroot], numtheory[imagunit] calculent respectivement la racine carrée de x modulo n, la racine m-ième d'un

```

[ nombre x modulo n ou une racine carrée de -1 modulo n (ces objets n'existent pas forcément)
[ > numtheory[msqrt](2,79);
[                                     9
[
[ > numtheory[mroot](2,5,79);
[                                     19
[
[ > numtheory[imagunit](85);
[                                     72
[
[ La fonction legendre du package numtheory, que l'on peut utiliser directement à l'aide de la syntaxe numtheory[legendre], calcule le symbole
[ de legendre  $\frac{p}{q}$  ; celui ci vaut 1 si p est un carré modulo q, -1 si p n'est pas un carré modulo q et 0 si q divise p
[
[ > numtheory[legendre](31,79);
[                                     1
[
[ > numtheory[msqrt](31,79);
[                                     30
[
[ > numtheory[legendre](29,79);
[                                     -1
[
[ > numtheory[msqrt](29,79);
[                                     FAIL
[                                      $\frac{(p-1)(q-1)}{4}$ 
[ La formule de réciprocité quadratique garantit que  $\frac{p}{q} \frac{q}{p} = (-1)^{\frac{(p-1)(q-1)}{4}}$  si p et q sont premiers:
[
[ > numtheory[legendre](31,79)*numtheory[legendre](79,31)=(-1)^(78*30/4);
[                                     -1 = -1
[
[ La fonction order du package numtheory, que l'on peut utiliser directement à l'aide de la syntaxe numtheory[order], calcule l'ordre d'un
[ élément x premier avec n dans le groupe multiplicatif des éléments inversibles de  $\mathbb{Z}/n\mathbb{Z}$ 
[ > numtheory[order](2,79);
[                                     39
[
[ c'est bien un diviseur de 78 qui est l'ordre du groupe multiplicatif des éléments inversibles de  $\mathbb{Z}/79\mathbb{Z}$ ; vérifions qu'il convient bien
[ > 2^39 mod 79;
[                                     1
[
[ Quant à la fonction primroot du package numtheory, que l'on peut utiliser directement à l'aide de la syntaxe numtheory[primroot], elle renvoie
[ un générateur du groupe multiplicatif des éléments inversibles de  $\mathbb{Z}/n\mathbb{Z}$  (on peut montrer que ce groupe est cyclique si n est premier).
[ > numtheory[primroot](79);
[                                     3
[
[ > sort([seq(3^i mod 79,i=0..77)]);

```

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39,
40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76,
77, 78]

Il y sont bien tous!

Cours de mathématiques

par Denis Monasse

Ed. Vuibert

Table des matières

- Plan général
- Algèbre générale
- Algèbre linéaire
- Réduction des endomorphismes
- Topologie des espaces métriques
- Espaces vectoriels normés
- Comparaison des fonctions
- Suites et séries numériques
- Fonctions d'une variable réelle
- Intégration
- Suites et séries de fonctions

- Séries entières
- Formes quadratiques
- Formes hermitiennes
- Séries de Fourier
- Calcul différentiel
- Equations différentielles
- Espaces affines
- Courbes
- Surfaces
- Intégrales multiples
- Index