Questions de divisibilité

Arithmétique et cryptographie

SUPINFO

Sommaire

1. Divisibilité et division Euclidienne.

1. Divisibilité et division Euclidienne.

Rappel sur les ensembles d'entiers

- L'ensemble des **entiers naturels**, constitué donc des entiers positifs $\{0,1,2,3,\ldots\}$, est noté $\mathbb{N}$. Ce même ensemble privé de l'élément 0 est noté $\mathbb{N}^*$.

- L'ensemble des **entiers relatifs**, constitué donc de tous les entiers $\{\ldots,-2,-1,0,1,2,\ldots\}$ est noté $\mathbb{Z}$. Ce même ensemble privé de l'élément 0 est noté $\mathbb{Z}^*$.

1. Divisibilité et division Euclidienne.

Multiples et diviseurs : principe

- On va s’intéresser dans un premier au temps aux divisions entre entiers qui “tombent juste“.
- Il est clair par exemple que 4 divise 12 mais ne divise pas 13.
- On va formaliser cela.

1. Divisibilité et division Euclidienne.

Multiples et diviseurs : définition

- Soient a,b éléments de $\mathbb{Z}$.

- S'il existe un entier relatif q tel que $a = b \times q$, on dit que :

  - b **divise** a
  - b est un **diviseur** de a
  - a est un **multiple** de b

- On note alors $b|a$.

1. Divisibilité et division Euclidienne.

Multiples et diviseurs : exemples

- 6 est un diviseur de 18 car $18 = 6 \times 3$. Autre formulation, 18 est un multiple de 6.

- $-13|221$ car $221 = (-13) \times (-17)$.

- Pour tout entier relatif a, $a + 1$ divise $a^2 - 1$. On a en effet l'égalité bien connue $a^2 - 1 = (a + 1) \times (a - 1)$.

1. Divisibilité et division Euclidienne.

Multiples et diviseurs : remarques

- L'ensemble des multiples de 0 est $\{0\}$ et l'ensemble de ses diviseurs est $\mathbb{Z}$.
- L'ensemble des multiples de 1 est $\mathbb{Z}$ et l'ensemble de ses diviseurs est $\{-1;1\}$.
- L'ensemble des multiples d'un entier relatif a est souvent noté $a\mathbb{Z}$.

1. Divisibilité et division Euclidienne.

Multiples et diviseurs : propriété

- Soient a,b éléments de $\mathbb{Z}$.
- Si $b|a$ alors $0 < |b| \leq |a|$.
- L'ensemble des diviseurs d'un nombre entier est donc fini.

1. Divisibilité et division Euclidienne.

Multiples et diviseurs : démonstration de la propriété précédente

- D'après les hypothèses, il existe un entier relatif q tel que $a = bq$.
- On a alors $|b| = \frac{|a|}{|q|}$.
- Or q étant un entier relatif non nul, on a nécessairement $|q| \geq 1$. D'où $\frac{1}{|q|} \leq 1$, ce qui prouve le résultat.
- L'ensemble des diviseurs d'un entier a est alors fini, car ces diviseurs sont nécessairement compris entre $-|a|$ et $|a|$.

1. Divisibilité et division Euclidienne.

Multiples et diviseurs : propriété

- Soient a,b éléments de $\mathbb{Z}^*$.

- On a l'équivalence

$$(a|b \text{ et } b|a) \Leftrightarrow (a = b \text{ ou } a = -b)$$

1. Divisibilité et division Euclidienne.

Multiples et diviseurs : propriétés

- Soient a,b,c éléments de $\mathbb{Z}$.
- Si $a|b$ et $b|c$, alors $a|c$. Cela signifie que la relation de divisibilité est **transitive**.
- Si $a|b$, alors pour tout entier relatif k, on a $ka|kb$.
- Si $a|b$ et $a|c$, alors pour tous entiers relatifs k et k', on a $a|(kb + k'c)$.

1. Divisibilité et division Euclidienne.

Multiples et diviseurs : éléments de démonstration des propriétés précédentes

- Prouvons par exemple la propriété de transitivité.

- D'après les hypothèses, il existe q et q' tels que $b = aq$ et $c = bq'$.

- On alors $c = aqq'$, ce qui signifie bien que $a|c$.

- Les autres résultats se démontrent de la même façon, en écrivant les hypothèses et en les exploitant directement

1. Divisibilité et division Euclidienne.

Quelques critères de divisibilité

- Un entier est divisible par 2 s’il se termine par 0, 2, 4, 6 ou 8.

- Un entier est divisible par 3 (*resp*. 9) si la somme de ses chiffres est divisible par 3 (*resp*. 9).

- Un entier est divisible par 5 s’il se termine par 0 ou 5.

1. Divisibilité et division Euclidienne.

Division Euclidienne : principe

- Quand une division entre des entiers ne tombe pas juste, cela signifie qu'il y a un **reste**.

- Par exemple 4 ne divise pas 13, on obtient un reste de 1.

- On va formaliser cela.

1. Divisibilité et division Euclidienne.

Division Euclidienne : théorème et définition

- Soit a élément de $\mathbb{Z}$, et b élément de $\mathbb{N}^*$.
- Il existe un unique couple d'entiers relatifs (q,r) vérifiant

$$a = bq + r \quad et \quad 0 \leq r < b$$

- On appelle alors a le **dividende**, b le **diviseur**, q le **quotient** et r le **reste** dans la division Euclidienne de a par b.

1. Divisibilité et division Euclidienne.

Division Euclidienne : algorithme de la descente de Fermat

- En pratique, pour déterminer le quotient et le reste, on distingue deux cas :
  - Si a est positif on lui retranche des multiples de plus en plus grands de b jusqu'à obtenir un reste strictement inférieur à b. Le quotient est alors le nombre de multiples de b retranchés.
  - Si a est négatif on lui additionne des multiples de plus en plus grands de b jusqu'à obtenir un reste strictement positif. Le quotient est alors l'opposé du nombre de multiples de b additionnés.

1. Divisibilité et division Euclidienne.

Division Euclidienne : algorithme de la descente de Fermat

```python
def descenteFermat(a, b):
    q, r = 0, a
    while r >= b:
        q += 1
        r -= b
    while r < 0:
        q -= 1
        r += b
    return q, r
```

1. Divisibilité et division Euclidienne.

Division Euclidienne : exemple

- Voici les divisions Euclidiennes de 27 et -27 par 12

$$27 = 12 \times 2 + 3 \quad \text{et} \quad -27 = 12 \times (-3) + 9$$

- À noter qu'un reste étant toujours positif, en aucun la division Euclidienne de -27 par 12 est

$$-27 = 12 \times (-2) + (-3)$$

- Ce que l'on aurait pu naïvement penser connaissant la division Euclidienne de 27 par 12.

1. Divisibilité et division Euclidienne.

Division Euclidienne : lien avec la divisibilité

- Soit a élément de $\mathbb{Z}$, et b élément de $\mathbb{N}^*$.

- Alors $b|a$ si et seulement si le reste de la division Euclidienne de a par b est égal à 0.

1. Divisibilité et division Euclidienne.

Test de divisibilité

```
def divisiblePar(a,b):
    q, r = descenteFermat(a,b)
    return r==0
```

1. Divisibilité et division Euclidienne.

Liste des diviseurs d’un entier

```
def listeDiviseurs(a):
    a = -a if a < 0 else a
    L = []
    for b in range(1,a+1):
        if divisiblePar(a,b):
            L.extend([b,-b])
    return L
```

1. Divisibilité et division Euclidienne.

Raisonnement par disjonction des cas : principe

- Après division euclidienne d'un entier relatif a par un entier naturel non nul b, les valeurs possibles des restes sont $0,1,2,\ldots,b-1$.

- Ainsi a peut s'écrire $bk, bk+1, bk+2, \ldots, bk+(b-1)$, avec k élément de $\mathbb{Z}$.

- Dans un problème de divisibilité par b, on pourra donc traiter chacun des b cas possibles.

1. Divisibilité et division Euclidienne.

Raisonnement par disjonction des cas : exemple

- Dans un problème de divisibilité par 2, on pourra écrire tout entier a sous la forme $2k$ ou $2k + 1$ avec k élément de $\mathbb{Z}$.

- Dans un problème de divisibilité par 3, on pourra cette fois écrire tout entier a sous la forme $3k$ ou $3k + 1$ ou $3k + 2$ avec k élément de $\mathbb{Z}$.

1. Divisibilité et division Euclidienne.

2. Plus Grand Commun Diviseur.

2. Plus Grand Commun Diviseur.

PGCD : principe

- Le **PGCD**, **P**lus **G**rand **C**ommun **D**iviseur, de deux entiers relatifs est une notion que l'on manipule depuis toujours, parfois même inconsciemment.

- Par exemple, lorsque l'on réduit une fraction à sa forme dite irréductible, on divise numérateur et dénominateur par leur PGCD

$$\frac{90}{120} = \frac{3 \times 30}{4 \times 30} = \frac{3}{4}$$

2. Plus Grand Commun Diviseur.

PGCD : définition

- Soient a,b éléments de $\mathbb{Z}^*$.

- On appelle Plus Grand Commun Diviseur de a et b l'unique naturel d vérifiant à la fois

  1. $d|a$ et $d|b$.
  2. Si c est un entier naturel tel que $c|a$ et $c|b$ alors $c \leq d$.

- On le notera $d = \mathrm{PGCD}\,(a,b)$ ou $d = a \wedge b$.

2. Plus Grand Commun Diviseur.

PGCD : détermination empirique

- On va calculer “à la main“ le PGCD de 18 et 48.

- On commence par chercher les diviseurs de ces deux entiers :

  - Les diviseurs de 18 dans $\mathbb{N}$ sont $1,2,3,6,9$ et 18.
    Les diviseurs de 48 dans $\mathbb{N}$ sont $1,2,3,4,6,8,12,16,24$ et 48.

- Les diviseurs communs de 18 et 48 dans $\mathbb{N}$ sont donc $1,2,3$ et 6.

- Le plus grand d'entre eux, et ainsi le PGCD de 18 et 48, est donc 6.

2. Plus Grand Commun Diviseur.

Lemme d'Euclide : énoncé

- Soient a,b,q,r éléments de $\mathbb{Z}^*$.
- Si

$$a = bq + r$$

- Alors

$$\mathrm{PGCD}\,(a,b) = \mathrm{PGCD}\,(b,r)$$

2. Plus Grand Commun Diviseur.

Lemme d'Euclide : démonstration

- Si c est un diviseur commun de a et b, puisque $r = a - bq$, il sera nécessairement également un diviseur de r.

- De même, si c est un diviseur commun de b et r, il sera aussi un diviseur de a.

- L'ensemble des diviseurs communs de a et b est donc égal à l'ensemble des diviseurs communs de b et r. Q.E.D.

2. Plus Grand Commun Diviseur.

Algorithme d'Euclide

- Problème : trouver le PGCD de deux entiers naturels a et b.

- Résolution :

  1. Si b est non nul, diviser a par b. On note r le reste de cette division euclidienne.
  2. Remplacer a par b et b par r.
  3. Recommencer tant que cela est possible à partir de l'étape 1.
  4. Le PGCD est alors la dernière valeur non nulle de r.

2. Plus Grand Commun Diviseur.

Algorithme d'Euclide : exemple

- Calcul du PGCD de 142 et 38

$$\begin{array}{ccc} 142 & = & 38 \times 3 + 28 \\ 38 & = & 28 \times 1 + 10 \\ 28 & = & 10 \times 2 + 8 \\ 10 & = & 8 \times 1 + 2 \\ 8 & = & 2 \times 4 + 0 \end{array}$$

- On a donc

$$\mathrm{PGCD}\,(142{,}38) = 2$$

2. Plus Grand Commun Diviseur.

Algorithme d'Euclide : implémentation itérative

```
def PGCD(a,b):
    while b != 0:
        a, b = b, a%b
    return a
```

2. Plus Grand Commun Diviseur.

Algorithme d’Euclide : implémentation récursive

```
def PGCD(a,b):
    if b == 0:
        return a
    else:
        return PGCD(b,a%b)
```

2. Plus Grand Commun Diviseur.

PGCD : propriétés

- Soient a,b éléments de $\mathbb{Z}^*$.
- Les diviseurs communs à a et b sont les diviseurs de $\mathrm{PGCD}\,(a,b)$.
- Si k est un entier relatif non nul, on a $\mathrm{PGCD}\,(ka,kb) = |k| \times \mathrm{PGCD}\,(a,b)$.
- Si $d = \mathrm{PGCD}\,(a,b)$ et si a',b' sont des entiers naturels tels que $a = da'$ et $b = db'$, alors $\mathrm{PGCD}\,(a',b') = 1$.

2. Plus Grand Commun Diviseur.

PGCD : exemple d'application des propriétés précédentes

- On a vu dans un exemple précédent que $\mathrm{PGCD}(142,38) = 2$, donc :
  - Les diviseurs communs de 142 et 38 sont les diviseurs de 2, *i.e.* $-2,-1,1$ et 2.
  - On a $\mathrm{PGCD}(71,19) = 1$.

2. Plus Grand Commun Diviseur.

Entiers premiers entre eux : définition

- Deux entiers naturels non nuls sont dits **premiers entre eux** si leur PGCD est égal à 1.

- Autrement dit, deux entiers naturels non nuls sont dits **premiers entre eux** si leurs seuls diviseurs communs sont -1 et 1.

1

2. Plus Grand Commun Diviseur.

Entiers premiers entre eux : exemple

- $\mathrm{PGCD}\,(142{,}38) = 2$ donc 142 et 38 ne sont pas premiers entre eux.

- $\mathrm{PGCD}\,(71{,}19) = 1$ donc 71 et 19 sont premiers entre eux.

2. Plus Grand Commun Diviseur.

3. Théorème de Bézout.

3. Théorème de Bézout.

Identité de Bézout

- Soient a,b éléments de $\mathbb{Z}^*$. Soit $d = \mathrm{PGCD}\,(a,b)$.

- Il existe deux entiers relatifs u et v premiers entre eux tels que

$$au + bv = d$$

- Ces deux entiers appelés **coefficient de Bézout** ne sont pas uniques.

3. Théorème de Bézout.

Détermination pratique des coefficients de Bézout : principe

1. On effectue l'algorithme d'Euclide.

2. On part de la dernière ligne où le reste est non nul, *i.e.* de la ligne donnant le PGCD, et on exprime successivement chacun des restes à l'aide de la ligne qui l'a produit. On obtient à la fin les coefficients u et v.

3. Théorème de Bézout.

Détermination pratique des coefficients de Bézout : exemple

- Rappelons le calcul du PGCD de 142 et 38

$$\begin{array}{ccc} 142 & = & 38 \times 3 + 28 \\ 38 & = & 28 \times 1 + 10 \\ 28 & = & 10 \times 2 + 8 \\ 10 & = & 8 \times 1 + 2 \\ 8 & = & 2 \times 4 + 0 \end{array}$$

- On commence par exprimer le dernier reste non nul, à savoir 2

$$2 = 10 - 8 \times 1$$

3. Théorème de Bézout.

Détermination pratique des coefficients de Bézout : exemple

- On remplace alors le reste précédent, à savoir 8

$$2 = 10 - (28 - 10 \times 2) \times 1$$

- On factorise

$$2 = 28 \times (-1) + 10 \times 3$$

- On remplace de nouveau le reste précédent, qui est 10

$$2 = 28 \times (-1) + (38 - 28 \times 1) \times 3$$

3. Théorème de Bézout.

Détermination pratique des coefficients de Bézout : exemple

- On factorise de nouveau

$$2 = 38 \times 3 + 28 \times (-4)$$

- On recommence avec le reste précédent (qui sera le dernier), à savoir 28

$$2 = 38 \times 3 + (142 - 38 \times 3) \times (-4)$$

- Dernière factorisation et obtention des coefficients de Bézout

$$2 = 142 \times (-4) + 38 \times 15$$

3. Théorème de Bézout.

Théorème de Bézout : énoncé

- Soient a,b éléments de $\mathbb{Z}^*$.

- Les entiers a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tels que

$$au + bv = 1$$

3. Théorème de Bézout.

Théorème de Bézout : démonstration

- Si a et b sont premiers entre eux cela signifie que leur PCDG est égal à 1. L'existence des entiers relatifs u et v tels que $au + bv = 1$ provient alors directement de l'identité de Bézout.

- Réciproquement, s'il existe deux entiers relatifs u et v tels que $au + bv = 1$, les diviseurs communs de a et b nécessairement des diviseurs de 1. Ce qui prouve bien que a et b sont premiers entre eux.

3. Théorème de Bézout.

Théorème de Bézout : exemple d’application

- Pour tout entier naturel n, on peut affirmer que les entiers $a = 2n + 1$ et $b = 3n + 2$ sont premiers entre eux.

- En effet, on vérifie facilement que $-3a + 2b = 1$.

- Le résultat découle alors du théorème de Bézout.

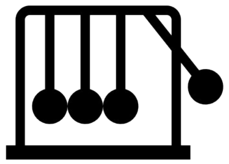
3. Théorème de Bézout.

4. Théorème de Gauss.

4. Théorème de Gauss.

Théorème de Gauss : énoncé

- Soient a,b,c éléments de $\mathbb{Z}^*$.
- Si $a|bc$ et si $\mathrm{PGCD}\,(a,b) = 1$, alors $a|c$.
- Autrement dit, si a divise le produit de b et c, et si a et b sont premiers entre eux, alors a divise c.



4. Théorème de Gauss.

Théorème de Gauss : démonstration

- D’après le théorème de Bézout, puisque a et b sont premiers entre eux, il existe deux entiers relatifs u et v tels que $au + bv = 1$.
- En multipliant cette égalité par c, on obtient $auc + bvc = c$.
- Or par hypothèse $a|bc$, donc $a|bvc$. Il est de plus évident que $a|auc$.
- Il en découle que $a|c$.

4. Théorème de Gauss.

Équation diophantienne : définition

- Une **équation diophantienne** est une équation polynomiale à coefficients entiers dont on cherche les solutions parmi les nombres entiers.

4. Théorème de Gauss.

Équation diophantienne : culture générale

- L’équation diophantienne la plus célèbre est celle posée par Pierre de Fermat

$$x^n + y^n = z^n$$

- Conjecture de Fermat : si $n > 2$ il n’existe pas d’entiers x,y,z vérifiant cette équation.

- Résultat démontré seulement en 1994 par Andrew Wiles.

4. Théorème de Gauss.

Équation diophantienne : cas simple

- On ne va s'intéresser ici qu'à certaines équations du premier degré à deux inconnues

$$ax = by$$

- On supposera de plus que $\mathrm{PGCD}\,(a,b) = 1$ ce qui n'est nullement restrictif puisque sinon il suffit de diviser l'équation par ce PGCD.

4. Théorème de Gauss.

Équation diophantienne : exemple

- On considère l'équation
$$12x = 7y$$

- On a nécessairement $7|12x$ mais comme $\mathrm{PGCD}\,(7,12) = 1$ le théorème de Gauss implique que $7|x$.

- Ainsi il existe un entier relatif k tel que $x = 7k$.

- L'équation devient alors
$$12 \times 7k = 7y$$

4. Théorème de Gauss.

Équation diophantienne : exemple

- Après simplification on obtient $y = 12k$.
- Une solution de cette équation sera donc nécessairement de la forme $x = 7k, y = 12k$ avec k entier relatif.
- Réciproquement il est clair que tout couple de cette forme est bien solution de l'équation.
- L'ensemble des solutions est donc

$$\{(7k, 12k), k \in \mathbb{Z}\}$$

4. Théorème de Gauss.

Corollaire du théorème de Gauss : énoncé

- Soient a,b,c éléments de $\mathbb{Z}^*$.
- Si $a|c$, $b|c$ et si $\mathrm{PGCD}\,(a,b) = 1$, alors $ab|c$.
- Autrement dit, si a et b divisent c, et si a et b sont premiers entre eux, alors le produit de a et b divise c.

4. Théorème de Gauss.

Corollaire du théorème de Gauss : démonstration

- Puisque par hypothèse a et b divisent c, il existe deux entiers relatifs x et y tels que $c = ax = by$.

- Ainsi $a|by$ et comme $\mathrm{PGCD}\,(a,b) = y$, le théorème de Gauss implique que $a|y$.

- Il existe donc un entier relatif k tel que $y = ka$.

- En remplaçant y par cette valeur dans l'expression de c, il vient $c = bka$.

- Ce qui prouve bien que $ab|c$.

4. Théorème de Gauss.

Critères de divisibilité

- Si un nombre entier est divisible par 2 et par 3, il est divisible par 6.

- Si un nombre entier est divisible par 5 et par 12, il est divisible par 60.

4. Théorème de Gauss.