T-PMTH-402 – Math. appliquées à l'info.
Chapitre 6 - Les nombres entiers

Jean-Sébastien Lerat
Jean-Sebastien.Lerat@heh.be

Haute École en Hainaut

2019-2020

Plan

Plan

Définition

Division

Soient $a, b \in \mathbb{Z}, a \neq 0$. a divise par b s'il existe $c \in \mathbb{Z}$ tel que $b = a \times c$.
Le fait que a divise b est noté $a|b$.
b est donc un multiple de a.

Exemple de division

$3|12$ car $c = 4(12 = 3 \times 4)$
$2|7$

Théorèmes

Soient $a, b, c \in \mathbb{Z}, a \neq 0$

Si $a|b$ est $a|c$ alors $a|(b+c)$ Par définition, puisque $a|b$, (resp. c) $\exists n$ (resp. m), $b = a \times n$ (resp. $c = a \times m$).
Montrons que $a|(b+c)$, c'est-à-dire $\exists k$ tel que $(b+c) = k \times a$.
Prenons $k = n + m$ ce qui donne bien $a \times (n+m) = a \times n + a \times m = (b+c)$.

Si $a|b$ et $a|c$ alors $a|(b \times c)$ *Preuve similaire*

Si $a|b$ et $b|c$ alors $a|c, b \neq 0$ *Preuve similaire*

Algorithme d'Euclide

Algorithme d'Euclide

Soient $a \in \mathbb{Z}$, $d \in \mathbb{N}, d > 0$. Il existe deux uniques entiers q et r tel que :
$a = d \times q + r$ et $0 \leq r < d$

Exemple

$a = 22, d = 5$
$22 = 5 * 4 + 2$

Algorithme d'Euclide – Unicité

Preuve par l'absurde.

Supposons qu'il existe q_1, q_2, r_1, r_2.tel que

$$\begin{cases} a = d \times q_1 + r_1 & 0 \leq r_1 < d \\ a = d \times q_2 + r_2 & 0 \leq r_2 < d \end{cases}$$

$$\begin{aligned} \Rightarrow d \times q_1 + r_1 &= d \times q_2 + r_2 \\ d \times q_1 - d \times q_2 &= r_2 - r_1 \\ d \times (q_1 - q_2) &= r_2 - r_1 \end{aligned}$$

Or $-d < r_2 - r_1 < d$ car $0 \leq r_i < d$.
$\Leftrightarrow -d < d \times (q_1 - q_2) < d$ car $= r_2 - r_1$
$\Leftrightarrow 0 \leq |d \times (q_1 - q_2)| < |d|$
$\Leftrightarrow 0 \leq |(q_1 - q_2)| < 1$ car $d \in \mathbb{N}, d > 0$
Or $q_1, q_2 \in \mathbb{N}$ donc $q_1 - q_2 = 0 \Rightarrow r_2 - r_1 = 0$.
$\Rightarrow r_1 = r_2$ et $q_1 = q_2$

Algorithme d'Euclide – Existence

Case de base (a=0) : prenons $q = r = 0, a = d \times q + r = 0$ et

$$0 \leq r < \underbrace{d}_{\text{peu importe sa valeur tant que } >0}$$

Case général (a) : on suppose que $\forall a\prime < a, a\prime = d\prime \times q\prime + r\prime, \qquad r\prime < d\prime$

Si $a < d$ alors $q = 0$ et $r = a$. On a bien que $a = d \times \underbrace{q}_{0} + \underbrace{r}_{a}$

Si $a \geq d$ Il faut montrer que a est de la forme $a = d \times q + r$. Soit un nombre $d > 0$, par hypothèse, il existe $a - d = q\prime \times d + r\prime$.

$\Rightarrow a = q\prime \times d + r\prime + d$

$\Leftrightarrow a = \underbrace{(q\prime + 1)}_{q} \times d + r\prime$

Plan

Arithmétique modulo

Modulo

Soient $a, b \in \mathbb{Z}, n \in \mathbb{N}$. On dit que a modulo n est le reste b de la division entière de a par b que nous noterons $a \equiv_n b \Leftrightarrow n|(a-b)$.

Exemple

$a = 7, n = 3, b = 1$

$7 \bmod 3 = 1$

Congruence

Congruence

Soient $a, b \in \mathbb{Z}, n \in \mathbb{N}$. On dit que a est congru à b modulo n noté $a \equiv_n b \Leftrightarrow n|(b-a)$, a est de la forme $a = b + k \times n$.

Exemple

$12 \equiv_5 2$
$12 \equiv_5 27$

Note : $a \bmod n \equiv_n a$

Propriétés

- Soit $n \in \mathbb{N}, n > 0$. $a \equiv_n b$ si et seulement si $\exists k \in \mathbb{Z}, a = b + k \times n$
- Soit $a \equiv_n b$ et $c \equiv_n d$:
  - $a + c \equiv_n b + d$
  - $a \times c \equiv_n b \times d$

Application

Génération de nombres pseudo-aléatoires

On choisit a, n, c, x_0

$x_{n+1} = (a \times x_n + c) \bmod n$

$n \sim 2^{31} - 1$

Cryptographie

f : fonction de chiffrement

g : fonction de déchiffrement

$g(f(message)) = message$

Chiffre de César

FKLIIUH GH FHVDU

$f(\text{symbole}) = code_{ASCII}(\text{symbole}) - 3$

$g(code) = symbole_{ASCII}(code + 3)$

Plan

Nombre premier

Définition

Soit $p \in \mathbb{N}, p \geq 2$. On dit que p est premier si et seulement si les seuls diviseurs sont 1 et p.

Exemple

2, 3, 5, 7, 11, 13, ...

Théorème fondamental de l'arithmétique

Théorème fondamental de l'arithmétique

Soit $n \geq 2$, n se décompose de manière *unique* en produit de nombres premiers.

Exemple

$6 = 2 \times 3$

Cas de base $(n = 2)$: 2 est le produit de 2.

Cas général $(n > 2)$:

Si n est premier $n = n$

si n n'est pas premier alors $\exists p, p|n \Rightarrow n = p \times q$.

$p < n$ et $q < n$, or par hypothèse d'induction forte, $\forall k < n$, k est décomposable en produit de nombres premiers.

$\Rightarrow p \times q$ est décomposable en facteurs premiers.

$\Rightarrow n$ est décomposable en facteurs premiers.

Définitions

Plus grand commun diviseur (PGCD)

Soient $a, b \in \mathbb{Z}, a \neq 0 \vee b \neq 0$. Le PGCD de a et b, noté $pgcd(a, b)$, est le plus grand nombre naturel $d \in \mathbb{N}$ tel que $d|a$ et $d|b$.

Note : $pgcd(p_1, p_2) = 1$ lorsque p_1, p_2 sont premiers entre eux.
Note : $pgcd(a, 0) = pgcd(0, a) = a$. Par convention $pgcd(0, 0) = 0$

Plus petit commun multiple (PPCM)

Soient $a, b \in \mathbb{Z}, a \neq 0 \vee b \neq 0$. Le PPCM de a et b, noté $ppcm(a, b)$, est le plus petit entier d tel que $a|d$ et $b|d$.

Exemples

$pgcd(24, 36) = 12$
$ppcm(2, 3) = 6$

Algorithme

Soient $a, b \in \mathbb{N}, a > 0, b > 0$, a est de la forme $a = b \times q + r$. Donc $r = a - b \times q$ $(a > b)$.

Soit d **diviseur de** a **et** $b \Rightarrow d|a$ **et** $d|b$.
$\Rightarrow a = d \times x$ et $b = d \times y$.
$b \times q = d \times y \times q$ est divisible par d.
$$\Rightarrow \underbrace{a - b \times q}_{=r} = d \times x - \underbrace{d \times y \times q}_{=b \times q}$$
$\Leftrightarrow r = d \times (x - y \times q)$ est divisible par d (multiple).
$\Leftrightarrow r$ est divisible par d.
De manière similaire, si $d|b$ et $d|r$ alors $d|b \times q + r$ (récursion).

d est diviseur commun de a et b si et seulement si d est diviseur commun de b et $r \Rightarrow pgcd(a, b) = pgcd(b, r)$

Corollaire $pgcd(a, b) = pgcd(b, a \bmod b)$

Plan

Changement de base

Représentation des nombres dans $\mathbb{N}$

Soit $b, n \in \mathbb{N}, b \geq 2$. n peut être écrit de manière unique tel que

$$n = \sum_{i=0}^{k} a_i \times b^k$$

où $a_i \in [0, b-1]$

Exemple d'écriture

Base $b = 10$ $925_{10} = 9 \times 10^2 + 2 \times 10^1 + 5 \times 10^0$

Base $b = 2$ $101_2 = 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$

Base $b = 16$ $AF_{16} = \underbrace{A}_{10} \times 16^1 + \underbrace{F}_{15} \times 16^1 6^0$

Chiffrement

Chiffrement

Un Chiffrement est un système qui définit comment chiffrer et déchiffrer un message. C'est-à-dire comment rendre un message inintelligible (incompréhensible) et comment rendre le message inintelligible en message intelligible.

Chiffrement symétrique

Un **chiffrement symétrique** va utiliser une seule clef (« mot de passe ») afin de chiffrer et déchiffrer un message à l'aide d'une fonction de chiffrement f et une fonction g de déchiffrement :

$$g(f(message, clef), clef) = message$$

Chiffrement asymétrique

Un **chiffrement asymétrique** va utiliser deux clefs appelées *clef publique* p et *clef privée* s. Les fonctions de chiffrement f et de déchiffrement g s'utilisent de la manière suivante :

$$g(f(message, s), p) = message$$

RSA

Chiffrement RSA

Le **chiffrement RSA** [a] est un algorithme de chiffrement asymétrique où :

La clef publique (n, e)

La clef privée (n, d)

La fonction de chiffrement $f(\mathit{message}_{\text{clair}}) = \mathit{message}_{\text{clair}}^{e} \bmod n$

La fonction de déchiffrement $g(\mathit{message}_{\text{chiffré}}) = \mathit{message}_{\text{chiffré}}^{d} \bmod n$

a. Le nom vient de ses inventeurs : *Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman*.

Générer une clef RSA :

1. Choisir deux nombres premiers distincts p et q
2. Calculer le module de chiffrement $n = pq$
3. Calculer l'indicatrice d'Euler $\phi(n) = (p-1)(q-1)$, i.e. combien de nombres premiers avec n.
4. Choisir un nombre entier $e < \phi(n)$ premier (avec $\phi(n)$)
5. Calculer le nombre entier $d = e^{-1} \bmod \phi(n)$

Solidité du RSA

Comment se fait-il que cet algorithme permet de communiquer de manière sécurisée ?

Il faut que le calcule de $m^e \bmod n$ soit rapide et qu'il soit impossible (ou difficile) de retrouver (calculer) d sur base de (n, e).

Or $d = e^{-1} \bmod \phi(n)$ et $\phi(n) = (p-1)(q-1)$.
$\Rightarrow d = e^{-1} \bmod (p-1)(q-1)$
Il faut que la recherche de p et q soit impossible/difficile.

Expansion modulo

Expansion modulo

L'expansion modulo d'un nombre b est le calcul de $b^n \bmod m$.

Remarrques :

1. $(ab) \bmod m = [(a \bmod m)(b \bmod m)]] \bmod m$
2. $b^n = \prod_{i=0}^{n} b = \begin{cases} (b^{\frac{n}{2}})^2 & \text{si } n \text{ est pair} \\ b(b^{\frac{n-1}{2}})^2 & \text{si } n \text{ est impair} \end{cases}$

Un algorithme efficace va donc calculer à chaque étape $base^2 \bmod m$ tel que

$$base = \underbrace{\overbrace{b^{\lfloor \frac{n}{2} \rfloor}}^{\text{Remarque 2}} \bmod m}_{\text{Remarque 1}}$$

Inverse modulo

Inverse modulo

L'inverse de a modulo n est un nombre u tel que

$$u = a^{-1} \bmod n$$

$\Leftrightarrow ua \equiv_n 1$
$\Rightarrow \exists v \in \mathbb{Z},\ 1 - au = nv$
$\Leftrightarrow 1 = nv + au$

Comment calculer $d = e^{-1} \bmod \phi(n)$?

Selon le théorème d'Euler si e est premier avec n ($\Leftrightarrow pgcd(e, n) = 1$),

$$\begin{aligned} e^{\phi(n)} &\equiv_n 1 \\ e \times e^{\phi(n)-1} &\equiv_n 1 \\ e^{\phi(n)-1} &\equiv_n \frac{1}{e} \\ e^{\phi(n)-1} &\equiv_n e^{-1} \\ e^{(p-1)(q-1)-1} &\equiv_n e^{-1} = d \end{aligned}$$

Plan

Exercices – 1/3

1. Prouvez que si $a \in \mathbb{N}, a > 0$, alors 1 divise a et a divise 0.
2. Soient $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$, prouvez que si $a|b$ et $b|a$ alors $a = b$ ou $a = -b$.
3. Déterminez le quotient et le reste de 111 divisé par 11 ; 123 par 7 ; 777 divisé par 21 ; 1434 divisé par 13 et 1025 divisé par 15.
4. Calculez $7 \bmod 5$; $789 \bmod 5672$; $77 \bmod 11$; $55 \bmod 7$; $72 \bmod 13$
5. Soient $a, b, n, m \in \mathbb{N}$ tels que $n \geq 2, m \geq 2 et n|m$. Prouvez que si $a \equiv_m b$ alors $a \equiv_n b$.
6. Soit $n \in \mathbb{N}$. Prouvez que si n est impair alors $n^2 \equiv_2 1$.
7. Soient $a, b, c, d \in \mathbb{Z}, m \in \mathbb{N}, m > 0$. Prouvez que si $a \equiv_m b$ et $c \equiv_m d$ alors $(a + c) \equiv_m (b + d)$ et $(ac) \equiv_m (bd)$.
8. Déduire de l'exercice précédent que :
   - $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
   - $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$
9. Prouvez que les deux égalités suivantes sont fausses :
   - $(a + b) \bmod m = (a \bmod m) + (b \bmod m)$
   - $(ab) \bmod m = (a \bmod m)(b \bmod m)$

Solutions – 1/3

1. $1|a \Leftrightarrow a = 1 * b \Leftrightarrow \frac{a}{1} = b \Rightarrow b = a$
   $a|0 \Leftrightarrow 0 = a * b \Leftrightarrow \frac{0}{a} = b \Rightarrow b = 0$, $\frac{0}{a}$ existe car $a > 0$
2. $(a|b \Leftrightarrow b = a * c, b|a \Leftrightarrow a = b * d) \Rightarrow a = d = \frac{1}{c}$ avec $c, d \in \mathbb{Z}$
   Si a, b de mêmes signes (resp. différent) alors c et d positifs (resp. négatifs) $\Rightarrow a = b$ ou $a = -b$
3. $111 = 11*10+1, 123 = 7*17+4, 1434 = 13*110+4, 1025 = 15*68+5$
4. $7 \equiv_5 2,789 \equiv_{5672} 789,77 \equiv_{11} 0,55 \equiv_7 6,72 \equiv_{13} 7$
5. On sait que $m = n * k, k \in \mathbb{N}, a = m * l + b \Rightarrow a = n * k * l + b, a$ s'exprime bien sous la forme $a = n * p + b$, n le diviseur et b le reste
6. n est impaire $\Leftrightarrow n = 2 * k + 1$,
   $n^2 = (2 * k + 1)^2 = 4k^2 + 4k + 1 = 2 * (2k^2 + 2k) + 1 \Rightarrow n^2 \equiv_2 1$
7. $a + c = (m * k + b) + (m * l + d) = m * lk + (b + d)$
   $a * c = (m * k + b) * (m * l + d) = m * (mkl + ld + bl) + (b * d)$
8. $(a + b) \equiv_m (m * k + b + b) \equiv_m 2b \bmod m \Leftrightarrow$
   $((a \bmod m) + (b \bmod m)) \bmod m = (b + b) \bmod m = 2b \bmod m$
   $(a + b) \equiv_m b * (m * k + b) = m * bk + b^2 \equiv_m b^2 \bmod m \Leftrightarrow$
   $((a \bmod m)(b \bmod m)) \bmod m = b^2 \bmod m$
9. $a = 8, m = 5, b = 3, k = 1 : 8 + 3 \not\equiv_5 3 + 2 \Leftrightarrow 1 \neq 5$,
   $8 * 3 \not\equiv_5 3 * 2 \Leftrightarrow 4 \neq 6$

Exercices – 2/3

1. Soient $m, n \in \mathbb{Z}$ et p un nombre premier. Prouvez que si $p|mn$ alors $p|m$ ou $p|n$. Ce résultat est-il toujours vrai si p n'est pas premier ?
2. Déterminez lesquels de ces nombres sont premiers : $21, 71, 111$ et 143.
3. Décomposez les nombres suivants en facteurs premiers : $88, 124, 289$ et 402.
4. Calculez $pgcd(15, 36)$, $ppcm(21, 49)$, $pgcd(121, 125)$ et $ppcm(31, 81)$.
5. Prouvez que le produit de trois entiers consécutifs est toujours divisible par 6.
6. Écrire en notation binaire les nombres suivants : $7, 9, 11, 31$ et 65.
7. Écrire en notation hexadécimale les nombres suivants : $13, 31$ et 65.

Solutions – 2/3 – Partie 1

1. $m * n = p * q$ Tout nombre se décompose en un produit de nombres premiers. Soit $q = \prod_i q_i, m = \prod_j m_j, n = \prod_k n_k$ des produits de nombres premiers. $\Rightarrow m * n = \prod_j m_j * \prod_k n_k, p * q = p * \prod_i q_i$ $\Rightarrow \prod_j m_j * \prod_k n_k = p * \prod_i q_i$ La liste exaustive des nombres premiers de m et n qui sont aussi diviseurs se trouve dans la partie gauche de l'égalité. p s'y trouve donc forcément.
2. $3|21, 3|111, 11|143$ et 71 est premier
3. $88 = 2 \times 2 \times 2 \times 11, 124 = 2 \times 2 \times 31, 289 = 17 \times 17, 402 = 2 \times 3 \times 67$
4. $pgcd(15, 36) = 3, ppcm(21, 49) = 147, pgcd(121, 125) = 1$ et $ppcm(31, 81) = 2511$.

Solutions – 2/3 – Partie 2

1. Soit $n \in \mathbb{N}$, montrons que $6 | n * (n+1) * (n+2)$. $n^3 + 2n^2 + n$ doit être de la forme $6 * x$. En particulier $2 * 3 * x$.
   Divisible par 2 :
   si n est pair alors produit de nombres pairs est pair, sinon n^3 est impair, $2n^2$ est pair, n est impair ce qui donne un nombre pair.
   Divisible par 3 :
   Montrons que $n * (n+1) * (n+2)$ est divisible par 3. Soit n est divisible par trois, sinon c'est qui lui manque une ou deux unités. Donc forcément, $n+1$ ou $n+2$ sera divisible par 3 d'où leur produit qui est divisible par 3.
2. $7 =_2 111, 9 =_2 1001, 11 =_2 1011, 31 =_2 11111$ et $65 =_2 1000001$.
3. $13 =_{16} D, 31 =_{16} 1F$ et $65 =_{16} 41$.

Exercices – 3/3

1. Convertir les entiers suivants de l'hexadécimal au décimal : $A0B1$ et $F0A02$.
2. Convertir les entiers suivants de l'hexadécimal au binaire : $ABBA$ et $FACE$.
3. Convertir les entiers suivants du binaire en hexadécimal : 11111011 et 10011101.
4. Prouvez qu'un nombre entier est divisible par 3 si et seulement si la somme de ses digits en décimal est divisible par 3.
5. Trouvez l'inverse de 5 modulo 11 ainsi que l'inverse de 3 modulo 7.
6. Prouvez que $2^{240} \bmod 11 = 1$

Solutions – 3/3– Partie 2

1. $A0B1 =_{10} 41137$ et $F0A02_{10} = 985602$
2. $ABBA =_2 1010101110111010$ et $FACE =_2 1111101011001110$.
3. Convertir les entiers suivants du binaire en hexadécimal : $11111011 =_{16} FB$ et $10011101 =_{16} 9D$.
4. Soit un nombre $z \in \mathbb{Z}$ représenté sous forme décimale $z = \sum_{i=0} z_i \times 10^i$. Montrons que $3|z$ ssi $3|\sum_{i=0} z_i$. Cas 1 : $|sum_{i=0} z_i| < 10$ alors par exhaustivité (montrer toutes les combinaisons) z n'est divisique que dans le cas où $|sum_{i=0} z_i|$ est un multiple de 3. Cas 2 : $|sum_{i=0} z_i| \geq 10$, $z' = sum_{i=0} z_i$, on retombe dans le cas 1 en remplaçant z par z'.
5. L'inverse de 5 modulo $11 = 9$ et l'inverse de 3 modulo $7 = 5$.

Solutions – 3/3 – Partie 2 ($2^{240} \bmod 11 = 1$)

```
(b^2)^120
((b^2)^2)^60
(((b^2)^2)^2)^30
((((b^2)^2)^2)^2)^15
((((b^2)^2)^2)^2 mod 11)^15
((((b^2)^2)^2)^2 mod 11)^15
9^15 mod 11
(9 * (9^14 mod 11))  mod 11
(9 * ((9^2)^7 mod 11))  mod 11
(9 * (4^7 mod 11))  mod 11
(9 * (4* (4^6 mod 11) mod 11)  mod 11
(9 * (4* ((4^2 mod 11)^3 mod 11) mod 11)  mod 11
(9 * (4* (5^3 mod 11) mod 11)  mod 11
(9 * (4* (5^3 mod 11) mod 11)  mod 11
(9 * (4* 4 mod 11)  mod 11
9 * 5  mod 11
45 mod 11
1
```

Exercices – Python

1. Soient $a, d \in \mathbb{N}, d > 0$. Écrivez un algorithme qui calcule $a \; div \; b$ et $a \bmod b$. Prouvez la correction et la terminaison de votre algorithme.
2. Soient a et $b \in \mathbb{N}$, prouvez que $pgcd(a, b) = pgcd(b, a \bmod b)$. Utilisez ce résultat pour construire un algorithme qui calcule $pgcd(a, b)$. Prouvez la correction et la terminaison de votre algorithme. Utilisez votre algorithme pour obtenir $pgcd(1000, 5040)$, $pgcd(1001, 2345)$.
3. Écrire un algorithme qui teste si un nombre est premier. Prouvez la correction et la terminaison de votre algorithme.
4. Étant donnés $n, b \in \mathbb{N}$ avec $b \geq 2$, écrire un algorithme qui retourne la représentation de n en base b. Prouvez la correction et la terminaison de votre algorithme.
5. Voici la clef publique RSA ($e = 12373, n = 8204732881$) qui a permis de chiffrer le message suivant :

   $5920091197, 3617337899, 7436421556, 316637925, 5289362343, 726885161$

   Cassez-le !