Mathématiques

-

Arithmétique

Frédéric Menan

fmenan@cesi.fr

11/2024

Table des matières

1 DIVISION EUCLIDIENNE 3

2 PGCD ET PPCM 4

2.1 PROPRIETES DU PGCD 4

2.2 RECHERCHE DU PGCD : ALGORITHME D'EUCLIDE 4

3 DECOMPOSITION D'UN NOMBRE ENTIER EN FACTEURS PREMIERS 6

3.1 DEFINITIONS : NOMBRE COMPOSE, NOMBRE PREMIER, NOMBRES PREMIERS JUMEAUX, NOMBRE PREMIER DE MERSENNE, NOMBRE PREMIER DE FERMAT, NOMBRES PREMIERS ENTRE EUX 6

3.2 DECOMPOSITION D'UN ENTIER EN PRODUIT DE NOMBRES PREMIERS 6

3.3 RECHERCHE DU PGCD AVEC LA DECOMPOSITION EN FACTEURS PREMIERS 8

3.4 RECHERCHE DU PPCM 8

4 IDENTITE DE BEZOUT (OU EQUATION DE BEZOUT) 10

***5* CONGRUENCE MODULO N 11**

6 PRINCIPE GENERAL DU CODAGE RSA 13

6.1 PREPARATION DES CLES PUBLIQUE ET PRIVEE (PAR ALICE) 13

6.2 CHIFFREMENT DU MESSAGE (PAR BRUNO) 13

6.3 DECHIFFREMENT DU MESSAGE (PAR ALICE) 13

6.4 FICHE METHODE POUR LE CODAGE RSA : ALGORITHME D'EUCLIDE ETENDU 14

6.5 FICHE METHODE POUR LE CODAGE RSA : ALGORITHME D'EXPONENTIATION RAPIDE 16

7 ARITHMETIQUE : JOUER AVEC LES ENTIERS ET LES JEUX DE TYPE NIM 17

7.1 EXISTE-T-IL TOUJOURS UNE STRATEGIE ? 17

8 EXERCICES 20

9 REFERENCES BIBLIOGRAPHIQUES 30

9.1 REFERENCES HISTORIQUES, NOTIONS DIVERSES 31

1 Division euclidienne

A deux entiers naturels appelés dividende et diviseur, la division euclidienne associe deux autres entiers appelés quotient et reste. Ainsi, soient deux entiers naturels a (dividende) et b (diviseur) tels que b ≠ 0, on écrit de façon unique

$$a = b.q + r$$

L'entier naturel q est appelé quotient et l'entier naturel r est appelé le reste et r<b.

Exemple 1

$$29 = 7 * 4 + 1$$

29 : dividende ; 7 : diviseur ; 4 : quotient ; 1 : reste

On parle de la division euclidienne de 29 par 7.

Figure 1. EUCLIDE, mathématicien grec (http://www.univ-irem.fr/spip.php?article1263)

Quand r=0, on dit que b est un diviseur de a (ou que a est un multiple de b). On note alors $b|a$.

Cette relation, appelée divisibilité, est une relation d'ordre sur $\mathbb{N}^* = \{1,2,3, \ldots\}$. 1 alors est le plus petit élément de $\mathbb{N}^*$.

Théorème

Soient a, b et c trois entiers. Si c divise a et si c divise b, alors c divise tout nombre de la forme u.a + v.b avec u et v dans $\mathbb{Z}$ est divisible par c.

2 PGCD et PPCM

Le plus grand commun diviseur de deux nombres entiers a et b non nuls est le plus grand entier qui divise a et b. Il est noté PGCD(a,b). On le note aussi $a \wedge b$.

Le plus petit multiple commun, de deux entiers non nuls a et b est le plus petit entier strictement positif qui soit multiple de ces deux nombres. Il est noté PPCM(a,b). On le note aussi $a \vee b$.

2.1 Propriétés du PGCD

$$a \wedge b = b \wedge a$$

$$a \wedge 1 = 1$$

$$a \wedge a = a$$

$a \wedge b = b$ si et seulement si $b|a$

Théorème

Soient a, b, et c trois entiers naturels non nuls.

La multiplication est distributive par rapport au PGCD

$$c(a \wedge b) = ca \wedge cb$$

Si c est un diviseur commun à a et b, alors

$$\left(\frac{a}{c}\right) \wedge \left(\frac{b}{c}\right) = \frac{a \wedge b}{c}$$

Si c est un diviseur commun à a et b, pour que $c = a \wedge b$, il faut et il suffit que

$$\left(\frac{a}{c}\right) \wedge \left(\frac{b}{c}\right) = 1$$

Lemme de Gauss

Si $a \wedge b = 1$ et si a divise bc, alors a divise c.

Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$.

Si $a \wedge b = 1$, alors $a \wedge bc = a \wedge c$

Théorème

Soient a et b deux entiers naturels non nuls. Alors pour tous entiers naturels non nuls c et d, $a \wedge b$ divise $ac \wedge bd$

2.2 Recherche du PGCD : algorithme d'Euclide

Il permet de déterminer le PGCD de deux nombres.

Mise en évidence

On montre ci-dessous la recherche du PGCD de 791 et 336 par l'algorithme d'Euclide. Cet algorithme est une suite de divisions Euclidiennes. On trouve que 7 est le PGCD de 791 et 336.

$$\begin{aligned} 791 &= 336\times 2+119 \\ 336 &= 119\times 2+98 \\ 119 &= 98\times 1+21 \\ 98 &= 21\times 4+14 \\ 21 &= 14\times 1+7 \\ 14 &= 7\times 2+0 \end{aligned}$$

Mais comment-est on parvenu à ce résultat ?

Appelons c un diviseur commun à 791 et 336.

Si c est un diviseur commun à a et b, alors il divise 791-2×336, c'est-à-dire 119 (voir §1).

Comme c divise 336 et 119, il divise aussi 336-119×2=98.

Comme c divise 119 et 98, il divise aussi 119-98×1=21….etc.

Par récurrence, on montrerait alors que c divise tous les restes des divisions Euclidiennes. Donc c divise 7. Donc $c \leq 7$.

De bas en haut, on voit que 7 divise 14. Donc il divise 14×1+7=21. Donc il divise 21×4+14=98….etc. Par conséquent, 7, le dernier reste non nul de la suite de divisions Euclidiennes, divise 791 et 336.

On vient de voir que 7 est un diviseur commun à 791 et 336. On vient aussi de voir que tout diviseur commun à 791 et 336 divise 7. De fait, 7 est le PGCD de 791 et 336.

Théorème

La mise en évidence de l'algorithme d'Euclide nous amène à intuiter un résultat qui pourrait se démontrer en démontrant « formellement » l'algorithme d'Euclide : les diviseurs communs à deux nombres sont tous les diviseurs de leur PGCD.

3 Décomposition d'un nombre entier en facteurs premiers

La décomposition d'un nombre entier en facteurs premiers est un outil puissant pour approfondir et démontrer de nouvelles propriétés concernant le PGCD et le PPCM.

Elle permet aussi de retrouver le PGCD et le PPCM de deux entiers.

3.1 Définitions : nombre composé, nombre premier, nombres premiers jumeaux, nombre premier de Mersenne, nombre premier de Fermat, nombres premiers entre eux

Un nombre premier est un entier naturel strictement supérieur à 1 et divisible seulement par lui-même ou par 1.

Un nombre qui n'est pas premier est dit composé.

Les nombres premiers consécutifs, soit ceux qui se trouvent à une distance numérique de 2, sont appelés nombres premiers jumeaux (exemple 17 et 19).

Un nombre premier de Mersenne est un nombre premier qui, si on lui ajoute 1, donne une puissance de 2. Exemple : 7 est premier. 7+1=8 est une puissance de 2.

Un nombre premier de Fermat est un nombre premier de la forme $2^{2^n} + 1$ avec n entier naturel.

Deux entiers naturels non nuls a et b sont dits premiers entre eux si leur seul diviseur commun

est 1. Par exemple, 4 et 7 sont premiers entre eux, mais 4 et 6 ne le sont pas car 2 est un diviseur commun.

Théorème

Il existe une infinité de nombres premiers (on trouvera la preuve de ce théorème dans les exercices en ligne).

Les vingt-cinq nombres premiers inférieurs à 100 sont :
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, et 97.

Théorème

Le plus petit diviseur strictement supérieur à 1 d'un entier strictement supérieur à 1 est un nombre premier (on trouvera la preuve de ce théorème dans les exercices en ligne).

3.2 Décomposition d'un entier en produit de nombres premiers

Théorème

Tout entier naturel supérieur ou égal à 2 est soit un nombre premier, soit un produit de nombre premiers.

Le théorème précédent signifie qu'on peut écrire tout entier naturel supérieur ou égal à 2 comme un produit de puissances de nombres premiers. Décomposer un entier naturel en produit de facteurs premiers, c'est ainsi écrire ce nombre comme le produit de nombres premiers.

Exemple 2

A l'aide des nombres premiers 2, 3 et 5 on écrit 60 comme $60 = 2^2 \times 3 \times 5$.

La décomposition en facteurs premiers d'un nombre n s'écrit

$$n = 2^{v_2(n)}.3^{v_3(n)}.5^{v_5(n)}.7^{v_7(n)}.11^{v_{11}(n)} \ldots.$$

Les exposants $v_p(n)$ sont nuls sauf pour un nombre fini d'entre eux.

Théorème fondamental de l'arithmétique

Tout entier strictement positif peut se décomposer, de façon unique, en produit de facteurs premiers.

Remarque

b est un diviseur de a équivaut à $v_p(b) \leq v_p(a)$ pour tout p

Démarche de décomposition en facteurs premiers

Soit n un entier que l'on veut factoriser, c'est-à-dire décomposer en facteurs premiers.

Étape 1 : trouver le plus petit entier autre que 1 qui divise n

Étape 2 : diviser n par ce facteur premier et trouver le plus petit entier autre que 1 qui divise le résultat, tant que le résultat est strictement supérieur à 1

Exemple 3

60	2
30	2
15	3
5	5
1	

Finalement, $60 = 2^2 * 3 * 5$

Remarques

$$v_p(a \wedge b) = \inf(v_p(a), v_p(b))$$

$$v_p(a \vee b) = \sup(v_p(a), v_p(b))$$

Exemple 4

$$a = 2^3.3^4.5^2.7^3.11^1$$

$$b = 2^2.3^2.5^1.7^4.11^1.13$$

$$a \wedge b = 2^2.3^2.5^1.7^3.11^1$$

Définition

On dit que les nombres a et b sont premiers entre eux quand a∧b=1.

Théorème

Si $\delta = a \wedge b$, alors les nombres a/δ et b/δ sont premiers entre eux.

Si δ est un diviseur commun à a et b, et si les nombres a/δ et b/δ sont premiers entre eux, alors $\delta = a \wedge b$.

Théorème

Quand un nombre premier divise un produit de nombres entiers, il divise au moins un des facteurs.

3.3 Recherche du PGCD avec la décomposition en facteurs premiers

Le PGCD de plusieurs entiers peut aussi se retrouver en les décomposant en facteurs premiers.

Soient

$$a = 2^2 \times 3^3 \times 5^4 \times 7 = 472500$$

$$b = 2^2 \times 3^2 \times 5 \times 7^2 = 8820$$

Alors le PGCD de a et b est $2^2 \times 3^2 \times 5 \times 7 = 1260$

On voit que

$$v_p(PGCD) = inf\left[v_p(a), v_p(b)\right]$$

3.4 Recherche du PPCM

Théorème

$$ab = (a \wedge b)(a \vee b)$$

Exemple 5

La décomposition en facteurs premiers nous est d'un grand secours. Considérons $a = 36$ et $b = 56$.

$$a = 2^2 \times 3^2$$

$$b = 2^3 \times 7$$

Considérons le nombre $2^3 \times 3^2 \times 7 = 504$

On constate aisément que ce nombre est un multiple commun à a et b.

Prenons un autre multiple commun à a et b, appelons le m. La décomposition de m en facteurs premiers sera de la forme $m = p.2^2 \times 3^2$ car m est multiple de a, et $m = q.2^3 \times 7$ car m est multiple de b, avec p et q nombres entiers.

Mais la décomposition en facteurs premiers est unique ! m sera donc de la forme $m = k.2^3 \times 3^2 \times 7$ avec k entier.

L'exposant 3 pour le facteur 2 est sup($v_2(a)$; $v_2(b)$), l'exposant 2 pour le facteur 3 est sup($v_3(a)$; $v_3(b)$), l'exposant 1 pour le facteur 7 est sup($v_7(a)$; $v_7(b)$).

Le plus petit multiple commun m est bien sûr pour k=1. On retrouve $2^3 \times 3^2 \times 7 = 504$. Finalement, PPCM(36 ;56)=504.

Utilisation

En utilisant la formule $ab = (a \wedge b)(a \vee b)$, on peut aisément, après détermination du PGCD(a ;b) par l'algorithme d'Euclide ou la décomposition en facteurs premiers, retrouver PPCM(a ;b).

Exemple 6

On montre que 453∧ $267 = 3$. Alors

$$453 \vee 267 = \frac{453 \times 267}{3} = 40317$$

Théorème

Soient a_1, a_2, a_n des éléments de $\mathbb{N}^*$. Soit $a_1 \vee a_2 \vee \ldots \vee a_n$ le PPCM des ces entiers. Alors

$$v_p(a_1 \vee a_2 \vee \ldots \vee a_n) = sup\left[v_p(a_1), v_p(a_2), \ldots, v_p(a_n)\right]$$

De plus, les multiples communs à ces entiers sont tous des multiples de leur PPCM.

Si les entiers a_i sont premiers entre eux deux à deux, alors leur PPCM est égal à leur produit.

4 Identité de Bezout (ou équation de Bezout)

Si a et b sont des entiers naturels alors il existe deux entiers p et q vérifiant

$$a.p + q.b = PGCD(a;b)$$

L'algorithme d'Euclide et le lemme de Gauss peuvent fournir l'ensemble des solutions (p,q) de cette équation (hors programme de ce cours).

Figure 2. Étienne Bézout (1730 – 1783) (https://mathshistory.st-andrews.ac.uk/Biographies/Bezout/pictdisplay/)

5 Congruence modulo n

Définition

Soit n un entier naturel. Deux entiers relatifs a et b sont dits congrus modulo n si leur différence est divisible par n, c'est-à-dire si il existe un entier k tel que

$$a = b + k.n$$

On dit alors que « a est congru à b modulo n » ou que « a et b sont congrus modulo n » et on note

$$a \equiv b \ mod \ n$$

Remarque importante

La définition revient aussi à dire : deux entiers a et b sont « congrus modulo n » si le reste de la division euclidienne de a par n est égal à celui de la division de b par n.

Exemple 7

$$13 = 9 + 1 * 4$$

$$9 = 2 * 4 + 1$$

$$13 = 3 * 4 + 1$$

13 et 9 sont congrus modulo 4.

Remarque

On dit aussi que $a \equiv b \ mod \ n$ quand n divise a-b.

Dans l'exemple précédent, 4 divise bien 13-9.

Propriétés

Soient a_1, a_2, b_1, b_2 des entiers relatifs. Soit n un entier naturel

Si $a_1 \equiv a_2 \ mod \ n$ et $b_1 \equiv b_2 \ mod \ n$ alors

$$a_1 + b_1 \equiv a_2 + b_2 \ mod \ n$$

$$a_1 . b_1 \equiv a_2 . b_2 \ mod \ n$$

Petit théorème de Fermat

Si p est un nombre premier, alors pour n'importe quel entier relatif a

$$a^p \equiv a \ mod \ p$$

Figure 3. Pierre de Fermat (XVIIème siècle) (https://www.fermat-science.com/pierre-fermat/)

Corollaire

Si p ne divise pas a, alors

$$a^{p-1} \equiv 1 \, mod \, p$$

Petit théorème de Fermat « amélioré »

Soient p et q deux nombres premiers distincts et soit n=p.q.

Pour tout entier relatif a tel que PGCD(a,n)=1, alors

$$a^{(p-1)(q-1)} \equiv 1 \, mod \, n$$

Remarque

L'hypothèse PGCD(a,n)=1 revient à dire que p et q ne divisent pas a

Exemple et démonstration

https://www.youtube.com/watch?v=M7vOxKVLsVY

Définition

Soit x un entier. Un entier x' tel que $x.x' \equiv 1 \, mod \, n$ est dit inverse de x modulo n.

Si un tel entier existe, on dit que x est inversible modulo n.

6 Principe général du codage RSA

Bruno veut envoyer un message secret à Alice.

6.1 Préparation des clés publique et privée (par Alice)

- Choix de deux nombres premiers p et q
- Calcul de n=p.q
- Calcul de ϕ(n)=(p-1).(q-1)

- Choix d'un exposant e tel que PGCD(e, ϕ(n))=1
- Calcul de d, inverse de e modulo ϕ(n) par l'algorithme d'Euclide étendu (voir fiche méthode)

$$d \times e \equiv 1 \; mod \; \varphi(n)$$

Clé publique d'Alice : n et e Clé privée d'Alice : d

6.2 Chiffrement du message (par Bruno)

Bruno veut envoyer un message à Alice. Il doit en faire un ou plusieurs entiers compris entre 0 et n-1. Il récupère la clé publique d'Alice. Les étapes sont ensuite :

- Calcul du message chiffré $x \equiv m^e \; mod \; n$ par l'algorithme d'exponentiation rapide (voir fiche méthode)
- Transmission du message x à Alice

6.3 Déchiffrement du message (par Alice)

- Calcul de $m \equiv x^d \; mod \; n$ par l'algorithme d'exponentiation rapide

Exemple 8

On choisit p=5 et q=17.

On a donc n=85 et ϕ(n)=64.

On choisit e tel que PGCD(e, ϕ(n))=1. Prenons e=5. On vérifie aisément que PGCD(5, 64)=1.

Il faut calculer d, inverse de e=5 modulo ϕ(n)=64, c'est-à-dire d tel que $d \times e \equiv 1 \; mod \; \varphi(n)$. Pour de grands nombres, on utilisera l'algorithme d'Euclide étendu.

5×13+64×(-1)=1 donc $5 \times 13 \equiv 1 \; mod \; 64$ donc l'inverse de 5 modulo 64, c'est-à-dire l'inverse de e modulo ϕ(n) est d=13.

On veut envoyer le message **m=10**. Calcul de $x \equiv m^e \; mod \; n \equiv 10^5 \; mod \; 85$

On a

$$10^2 = 100 \equiv 15 \; mod \; 85$$

$$10^4 = 10^2 . 10^2 \equiv 15^2 \equiv 225 \equiv 55 \; mod \; 85$$

$$10^5 = 10^4.10 \equiv 55 \times 10 \equiv 550 \equiv 40\ mod\ 85$$

Le message chiffré sera x=40.

Pour déchiffrer le message, il faut calculer $40^{13}\ mod\ 85$

$$40^2 = 1600 \equiv 70\ mod\ 85$$

$$40^4 = 40^2.40^2 \equiv 70^2 \equiv 4900 \equiv 55\ mod\ 85$$

$$40^8 = 40^4.40^4 \equiv 55^2 \equiv 3025 \equiv 50\ mod\ 85$$

Finalement,

$$40^{13} = 40^8.40^4.40 \equiv 50 \times 55 \times 40 \equiv 10\ mod\ 85$$

On retrouve **m=10**, le message de Bruno.

Remarque

RSA repose sur le lemme suivant :

Soit d l'inverse de e modulo ϕ(n) avec n=p.q et p≠q. Si $x \equiv m^e\ mod\ n$, alors $m \equiv x^d\ mod\ n$

Le message chiffré par la clé publique peut donc être retrouvé avec sa clé privée.

6.4 FICHE Méthode pour le codage RSA : Algorithme d'Euclide étendu

Connaissant des entiers a et n, cet algorithme permet de calculer l'inverse de a modulo n.

En effet, on montre que l'entier a est inversible modulo n si et seulement si PGCD(a,n)=1.

Or si PGCD(a,n)=1 et si on parvient à calculer u et v tels que $au + nv = 1$, alors l'inverse de a modulo n est l'entier u, puisque si $au + nv = 1$, alors au=1-nv donc $au \equiv 1\ mod\ n$.

L'algorithme d'Euclide étendu fournit les coefficients de Bézout tels que a.u+b.v=PGCD(a,b).

On peut donc s'en servir pour calculer l'inverse de a modulo n. Autrement dit, trouver un inverse de a modulo n revient à calculer les coefficients de Bezout associés à la paire (a,n).

Principe

https://www.youtube.com/watch?v=M7vOxKVLsVY

Exemple 9

On cherche u et v tels que 4553.u + 629.v = 1

Soient

$$x_0 = 1\ ;\ x_1 = 0\ ;\ y_0 = 0\ ;\ y_1 = 1$$

Pour i=2,

7 est le quotient de la division euclidienne de 4553 par 629.

$$x_2 = x_0 + 7.x_1 = 1$$

$$y_2 = y_0 - 7.y_1 = -7$$

Idem pour i=3, i=4…….

A la fin, on a bien $130 \times 4553 - 941 \times 629 = 1$

quotients		xi	yi
	4553	1	0
	629	0	1
7	150	1	-7
4	29	-4	29
5	5	21	-152
5	4	-109	789
1	1	130	-941

Référence intéressante : sous SCILAB (www.pedagogie.ac-nantes.fr)

```
// Algorithme d'Euclide étendu
// ----------------------------
// fonction qui renvoie le quotient de deux entiers
function q=iquo(a, b)
k=0;
d=a;
while d>=0
k=k+1;
d=d-b;
end
q=k-1;
endfunction
// ---------------------------
// algorithme d'Euclide étendu
a=input("entrer l''entier a : ");
b=input("entrer l''entier b : ");
// ---------------------------
A=[a,1,0];
B=[b,0,1];
q=iquo(A(1,1),B(1,1));
C=A-q.*B;
while C(1,1)<>0
A=B;
B=C;
q=iquo(A(1,1),B(1,1));
C=A-q.*B;
end
// affichage de d=PGCD(a,b), u et v
// tels que au+bv=d
disp(B);
```

6.5 FICHE Méthode pour le codage RSA : Algorithme d'exponentiation rapide

https://www.youtube.com/watch?v=M7vOxKVLsVY

Cet algorithme permet de calcul rapidement a^k mod n

Exemple 10

Calcul de 5^{11} mod 14

D'abord, notons que 11 = 8+2+1 donc $5^{11} = 5^8 + 5^2 + 5^1$

On a

$$5 \equiv 5 \; mod \; 14$$

$$5^2 \equiv 25 \equiv 11 \; mod \; 14$$

$$5^4 = 5^2 \times 5^2 \equiv 11 \times 11 \equiv 121 \equiv 9 \; mod \; 14$$

$$5^8 = 5^4 \times 5^4 \equiv 9 \times 9 \equiv 81 \equiv 11 \; mod \; 14$$

Par conséquent

$$5^{11} = 5^8 \times 5^2 \times 5^1 \equiv 11 \times 11 \times 5 \equiv 602 \equiv 3 \; mod \; 14$$

7 Arithmétique : jouer avec les entiers et les jeux de type NIM

Considérons le jeu ci-dessous.

On pose 20 jetons sur la table et chaque joueur peut en retirer un ou deux à tour de rôle. Celui qui retire le dernier pion gagne. Vous préférez jouer en premier ou en second ?

On voit que le premier joueur peut toujours gagner en prenant 2 jetons au départ et en laissant toujours sur la table un multiple de 3.

Un raisonnement qui part de la fin du jeu pour remonter aux choix qui doivent être faits dès le début est dit « induction à rebours ».

Généralisation

Soient M pions sur la table. A chaque tour, on doit retirer de 1 à n jetons. Bien sûr, n<M.

Le joueur qui retire le dernier pion a gagné.

Si le reste de la division euclidienne de M par n+1 vaut 0, alors le premier joueur démarre avec un multiple de n+1. Il existe alors une stratégie gagnante pour le second joueur qui doit se contenter de laisser sur la table un multiple de n+1.

Si le reste de la division euclidienne de M par n+1 est r (donc 0<r<n+1), il existe alors une stratégie gagnante pour le premier joueur qui devra retirer au premier tour r pions, afin de laisser sur la table un multiple de n+1.

Cette généralisation permet de connaitre la stratégie (jouer en premier ou second, et comment jouer) pour 3469 pions et la possibilité d'en retirer entre 1 et 57 !

Bien évidemment, si celui qui retire le dernier pion, la stratégie s'inverse.

7.1 Existe-t-il toujours une stratégie ?

Considérons le jeu ci-dessous.

On dispose au départ de 20 pions. Chacun son tour, chaque joueur peut en prendre 1, 3 ou 5.

Celui qui prend le dernier jeton remporte la partie. Qui a une chance de gagner ? Quelle est la stratégie à adopter ?

D'abord, montrons que

- Si p est un entier pair et q un entier impair, alors p-q est impair
- Si p et q sont des entiers impairs, alors p-q est pair

Démonstration : Si p est pair, alors il existe un entier a tel que p=2a. Si q est impair, alors il existe un entier b tel que q=2b+1. Par conséquent, p-q=2a-2b-1=2(a-b)-1 est impair. Sur le même raisonnement, on montre le second résultat.

Revenons au jeu.

Le premier joueur fera la soustraction d'un nombre pair (20) par un nombre impair. Il va donc laisser un nombre impair de pions. Le second joueur va faire impair – impair et donc laisser un nombre pair de pions. Le premier joueur va refaire la soustraction d'un nombre pair par un nombre impair et laisser un nombre impair de pions. Finalement, le premier joueur va toujours laisser un nombre impair de pions sur la table et le second joueur va toujours laisser un nombre pair de pions sur la table. 0 est pair donc le second joueur gagne toujours.

On voit qu'il n'y a pas de place au hasard, ni de place à la stratégie, pour aucun des joueurs : le second joueur gagne toujours. Le gagnant est connu à l'avance, quels que soient leurs choix de prendre 1, 3 ou 5 pions.

On parle de pseudo-jeux.

A noter qu'aucune stratégie n'est possible mais le joueur gagnant dépend du nombre initial de pions sur la table. En effet

- Si le nombre initial de pions est impair et que l'on retire un nombre de pions impair, le premier joueur gagnera toutes les parties.
- Si le nombre initial de pions est pair et que l'on retire un nombre de pions impair, le second joueur gagnera toutes les parties.

Remarque : élargissement vers les jeux dynamiques

Chaque joueur joue chacun son tour.

On montre que

- si chaque joueur dispose à tout instant de toutes les informations lui permettant de décider de son prochain coup
- si les deux joueurs décident de leur coup tour à tour
- si aucun élément aléatoire n'intervient dans le jeu
- si chaque partie se termine, avec un nombre de coups finis, par la victoire d'un des deux joueurs

alors il existe une stratégie gagnante pour le premier ou le second joueur.

Identification des stratégies gagnantes

- Heuristique
- Étude des cas particuliers
- La réflexion à rebours (voir jeu de Nim)
- Symétrie
- Parité (voir le pseudo-jeu étudié)

Commandes SCILAB et EXCEL

SCILAB

Pour l'aide sur une fonction, taper help fonction directement dans SCILAB

- factor()
- diviseurs()
- premier() pour savoir si n est un nombre premier

- numero_premier() retourne le nombre premier numéro n, avec n entier positif ou nul, dans la suite des nombres premiers.
- pgcd(m,n) retourne le plus grand commun diviseur de m et n avec m et n entiers.
- ppcm(m,n) retourne le plus petit commun multiple de m et n avec m et n entiers.
- liste_premiers(n) : retourne la suite des nombres premiers inférieurs à n avec n entier positif ou nul.
- impair()
- pair()
- quotient()
- reste(m,n) retourne le reste de la division Euclidienne de m par n.

8 Exercices

8.1.1 Division Euclidienne

Effectuer la division euclidienne de 213 par 8

Correction

213 8

-16 26
53
-48
5

$$213 = 8 \times 26 + 5$$

8.1.2 Division Euclidienne

On sait que 72347=336*213+779

En déduire, sans faire la division du nombre 72347, le reste de la division de 72347 par 336

Indice : le reste d'une division euclidienne doit être inférieur au quotient

Réponse

Par 336 : reste = 107

779=2*336+107

72347=336*213+2*336+107=336*215+107

8.1.3 Division Euclidienne

On sait que 72347=336*213+779

En déduire, sans faire la division du nombre 72347, le reste de la division de 72347 par 213

Indice : le reste d'une division euclidienne doit être inférieur au quotient

Réponse :

Par 213 : reste = 140

72347=336*213+779=213*339+140

8.1.4 PGCD et décomposition en facteurs premiers

En utilisant la décomposition en facteurs premiers, calculer le PGCD de 31500, 420, 300

Indice : pour deux entiers a et b $v\_p\ (PGCD) = inf[v\_p\ (a), v\_p\ (b)]$

Réponse

31500=2^2*3^2*5^3*7

420=2^2*3*5*7

300=2^2*3*5^2

Donc PGCD=2^2*3*5=60

8.1.5 Propriétés des entiers

Pour tout entier naturel n : n(n+1)(n+2)(n+3) est divisible par 24

1/ vrai

2/ faux

Indice : pour 4 nombres consécutifs il y a toujours un diviseur de 2, un diviseur de 3, un diviseur de 4 ?

Réponse : vrai.

On peut constater que pour 4 nombres consécutifs il y a toujours : un diviseur de 2, un diviseur de 3, un diviseur de 4 (tous distincts). Donc le produit de 4 nombres consécutifs est divisible par 2x3x4 = 24. On peut montrer la propriété de façon rigoureuse par récurrence.

8.1.6 Propriétés des entiers

Pour tout entier naturel n : n(n+1)(n+2)(n+3)(n+4) est divisible par 120

1/ vrai

2/ faux

Indice : pour 5 nombres consécutifs il y a toujours : un diviseur de 2, un diviseur de 3, un diviseur de 4, un diviseur de 5 ?

Réponse : vrai.

On peut constater que pour 5 nombres consécutifs il y a toujours : un diviseur de 2, un diviseur de 3, un diviseur de 4, un diviseur de 5 (tous distincts). Donc le produit de 5 nombres consécutifs est divisible par 2x3x4x5 = 120. On peut montrer la propriété de façon rigoureuse par récurrence.

8.1.7 Propriétés des nombres premiers

Tous les nombres premiers sont impairs.

1/ vrai

2/ faux

Indice : si on n'arrive pas à démontrer une proposition parce qu'on pense qu'on pense qu'elle est fausse, le contre-exemple est un très bon outil

Réponse : faux.

2 est premier et pair (mais c'est le seul nombre premier pair, tous les autres nombres premiers sont impairs !)

8.1.8 Propriétés des nombres premiers

Les deux seuls nombres premiers consécutifs sont 2 et 3.

1/ vrai

2/ faux

Indice : : on peut constater que pour tout entier $n > 2$, alors n est divisible par 2 ou $n+1$ divisible par 2.

Réponse : vrai

On peut constater que pour tout entier $n > 2$, alors n est divisible par 2 ou $n+1$ divisible par 2. Donc deux entiers consécutifs strictement supérieurs à 2 ne peuvent être tous les deux nombres premiers.

8.1.9 Propriétés des nombres premiers

Théorème

Si a et b sont des entiers premiers entre eux, alors $a+b$ et $a \times b$ sont premiers entre eux.

Preuve

Supposons que $a+b$ et $a \times b$ ne sont pas premiers entre eux. Il existe alors un nombre p divisant $a \times b$ et $a+b$. Si p divise $a \times b$, alors p divise au moins l'un des deux. Si p divise a, et si p divise $a+b$, alors p divise b. Donc p est un diviseur commun de a et b. Or a et b sont des entiers premiers entre eux donc ils n'ont pas de diviseur commun. Donc $a+b$ et $a \times b$ sont premiers entre eux.

Quel type de raisonnement a été appliqué ?

1/ Par l'absurde

2/ Par contraposée

3/ Par récurrence

4/ Au cas par cas

Indice : pour montrer la proposition P on a supposé « non P » et on a montré qu'on aboutit à une contradiction

Réponse : 1, par l'absurde

8.1.10 Décomposition d'un nombre entier en facteurs premiers

Décomposer 20 en produit de facteurs premiers

Avec la convention d'écriture : par exemple pour 12, on note 2.2.3

Indice : https://www.youtube.com/watch?v=6ZpaNKCpAGM

Réponse : 2.2.5

$$20 = 2^2 * 5$$

8.1.11 Décomposition d'un nombre entier en facteurs premiers

Décomposer 1050 en produit de facteurs premiers

Avec la convention d'écriture : par exemple pour 12, on note 2.2.3

Indice : https://www.youtube.com/watch?v=6ZpaNKCpAGM

Réponse : 2.3.5.5.7

$$1050 = 2 * 3 * 5^2 * 7$$

8.1.12 Les extraordinaires propriétés du nombre 60

Exercice inspiré du livre « L'énigme de Fermat » 2010 ISBN 978-84-1329-171-0

Les extraordinaires propriétés du nombre 60 pourraient expliquer l'utilisation précoce, répandue et tenace du système sexagésimal. Le système décimal s'est imposé, le système binaire est la base de l'informatique, et pourtant on compte encore les minutes et les secondes en base 60, et un tour fait 360°, multiple de 60.

https://fr.wikipedia.org/wiki/Syst%C3%A8me_sexag%C3%A9simal

Q1) 60 contient un grand nombre de diviseurs. Combien au total ?

Q2) Entre quels nombres premiers jumeaux le nombre 60 est-il situé ?

Q3) Le nombre 60 est la somme de 4 nombres premiers consécutifs. Lesquels ?

Q4) Le nombre 60 est la somme de 2 nombres premiers jumeaux. Lesquels ?

Q5) Le nombre 60 est le plus petit nombre que l'on peut obtenir à partir de n sommes différentes de deux nombres premiers. Déterminer n.

Indices

Q1/ lister ses diviseurs

Q2/ des nombres premiers consécutifs, soit ceux qui se trouvent à une distance numérique de 2, sont appelés nombres premiers jumeaux

Q3/ chercher les nombres premiers inférieurs à 60 et faire la somme de 4 d'entre eux qui sont consécutifs

Q4/ des nombres premiers consécutifs, soit ceux qui se trouvent à une distance numérique de 2, sont appelés nombres premiers jumeaux

Q5/ un peu de tâtonnement ! Un exemple : 60 = 7 + 53

Réponse

Q1/ 12

Q2/ 59 et 61

Q3/ 11, 13, 17, 19

Q4/ 29 et 31

Q5/ n=6

8.1.13 Exercice : équation diophantienne

Soit l'équation (1)

$$11x - 4y = 2$$

Déterminer l'ensemble des solutions de (1) dans $\mathbb{N}$

Correction

Solution particulière (x0 ;y0)=(2 ;5)

$$11x - 4y = 11x_0 - 4y_0$$

$$11.(x - x_0) = 4.(y - y_0)$$

$$y - y_0 = 11k$$

$$y = 11k + 5$$

$$11x - 4(11k + 5) = 2$$

$$11x = 44k + 22$$

$$x = 4k + 2$$

Solution générale :

$$x = 4k + 2$$

$$y = 11k + 5$$

8.1.14 Congruence, définitions

Soit un entier n > 0 et deux entiers a et b. Cocher les bonnes réponses.

1/ a et b sont dits congrus modulo n si leur différence est divisible par n

2/ a et b sont dits congrus modulo n si il existe un entier k tel que a=b+k.n

3/ a et b sont « congrus modulo n » si le reste de la division euclidienne de a par n est égal à celui de la division de b par n

4/ a et b sont dits congrus modulo n si n divise a-b

Réponse : 1 2 3 4

8.1.15 Congruence

Soient 4 entiers a_1,a_2,b_1,b_2 tels que $a_1 \equiv b_1 mod n$ et $a_2 \equiv b_2\ mod\ n$.

Cocher la ou les réponses justes.

1/ $a_1 - a_2 \equiv b_1 - b_2$

2/ $a_1 . a_2 \equiv b_1 . b_2$

Indice : est-ce que (a1-a2)-(b1-b2) et que (a1.a2)-(b1.b2) sont divisibles par n ?

Réponse : 1 et 2.

8.1.16 Arithmétique modulaire et matrices : le chiffrement de Hill

Remarque préliminaire : cet exercice suppose une connaissance sommaire des matrices (inverse d'une matrice, produit)

Lester S. Hill a proposé, dans les années 1920, un chiffrement de messages combinant arithmétique et calcul matriciel.

Son fonctionnement est le suivant :

Attribuons à chaque lettre de l'alphabet un nombre. On a aussi besoin d'attribuer un nombre au caractère vide ou « espace » que l'on nommera %

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	%
0	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

On définit une matrice A dont le déterminant vaut 1.

Par exemple,

$$A = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$$

On veut coder le message « FRED »

La correspondant numérique de « FRED » est, d'après le tableau : « 5 17 4 3 »

Remarque : si on avait voulu coder un message avec un nombre impair de caractères, par exemple « YES », on aurait codé le message « YES% » afin de réaliser les calculs matriciels.

Calculons alors

$$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 5 \\ 17 \end{pmatrix} = \begin{pmatrix} 61 \\ 100 \end{pmatrix}$$

Que faire de ce vecteur ? Ce vecteur est congru à un autre vecteur modulo 27

$$\begin{pmatrix} 61 \\ 100 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 19 \end{pmatrix} (mod\ 27)$$

car 61 et 7 sont congrus modulo 27 et 100 et 19 sont congrus modulo 27.

Par conséquent, les caractères FR seront codés par HT (7 correspond à H et 19 à T dans le tableau).

De même

$$\begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 17 \\ 27 \end{pmatrix}$$

17 et 27 trouvent déjà une correspondance dans le tableau : les caractères R%

Le message « FRED » sera codé par « HTR% »

Comment le déchiffrer ?

Calculons l'inverse de A

$$A^{-1} = \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}$$

Calculons

$$\begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}\begin{pmatrix} 7 \\ 19 \end{pmatrix} = \begin{pmatrix} -22 \\ 17 \end{pmatrix}$$

Or -22 est congru à 5 modulo 27 car -22=27×(-1)+5

On retrouve bien le vecteur $\begin{pmatrix} 5 \\ 17 \end{pmatrix}$ qui correspond aux lettres FR

De même,

$$\begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}\begin{pmatrix} 17 \\ 27 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$

On retrouve bien le vecteur $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$ qui correspond aux lettres ED.

Le message « HTR% » est donc bien le message original « FRED ».

Remarque : pour l'exemple, on a pris une matrice 2*2 et on a regroupé les caractères en paires. On aurait pu prendre une matrice 3*3 ou 4*4 pour augmenter la sécurité ! Trouver des matrices dont le déterminant vaut 1 est possible, et les ordinateurs actuels peuvent inverser d'immenses matrices sans souci.

Chiffrer le message « YES% » avec la matrice proposée dans l'exemple

Réponse : « GLGW »

8.1.17 Préparation au codage RSA : petit théorème de Fermat amélioré

Soient p=5 et q=7. Soit a un entier.

On a $a^{24} \equiv x \ mod \ 35$. Que vaut x ?

Indice : Petit théorème de Fermat amélioré

On peut remarquer que 35=p.q et 24=(p-1).q-1)

Réponse : x=1

35=7x5 et 24=(5-1).(7-1)

Petit théorème de Fermat amélioré : soit n=35=p.q. Alors

$$a^{(p-1)(q-1)} \equiv 1 \ mod \ n$$

8.1.18 Préparation au codage RSA : algorithme d'Euclide étendu

Par l'algorithme d'Euclide étendu, calculer u et v tels que 3365.u+549.v=1

Convention d'écriture : si u=73 et v=-87, écrire dans Moodle u=73v=-87

Indice : exemple sous EXCEL pour a=4553 et b=629

4553*130+629*(-941)=1

	4553	1	0
	629	0	1
7	150	1	-7
4	29	-4	29
5	5	21	-152
5	4	-109	789
1	1	130	-941

https://www.youtube.com/watch?v=M7vOxKVLsVY

Réponse : u=116 et v=-711

8.1.19 Préparation au codage RSA : exponentiation rapide

On veut calculer 5^{11} mod 14 par la méthode appelée exponentiation rapide.

Détails de la méthode :

En notant que 11=8+2+1, ce qui implique 511=58x52x51

En notant que les 5^(2^i) mod 14 donnent

5≡5 mod 14

5^2≡25≡11 mod 14

5^4=5^2×5^2≡11×11≡121≡9 mod 14

5^8=5^4×5^4≡9×9≡81≡11 mod 14

En déduire 5^{11} mod 14

Indice : penser à la propriété : si a1≡a2 mod n et b1≡b2 mod n alors

a1.b1≡a2.b2 mod n

Réponse : 3

5^11≡5^8×5^2×5^1≡11×11×5≡11×55≡11×13≡143≡3 mod 14

https://www.youtube.com/watch?v=M7vOxKVLsVY

8.1.20 Codage RSA

RSA a été créé en 1978 par Rivest, Shamir et Adleman (RSA) et se base sur les propriétés des nombres premiers.

Vidéos à visionner :

https://www.youtube.com/watch?v=M7vOxKVLsVY

https://www.youtube.com/watch?v=Xlal_d4zyfo

Bruno vous a envoyé le message x=37.

Avec les mêmes clés privées et publiques que dans la vidéo, déchiffrer le message de Bruno.

Réponse : m=12

8.1.21 20 pions, celui qui retire le dernier jeton gagne

On pose 20 jetons sur la table et chaque joueur peut en retirer un ou deux à tour de rôle. Celui qui retire le dernier jeton gagne.

Cocher les bonnes réponses

1/ Le premier joueur peut toujours gagner en prenant 2 jetons au départ et en laissant toujours sur la table un multiple de 3

2/ Le joueur qui laisse 2 jetons sur la table remporte la partie

3/ Le joueur qui laisse 3 jetons sur la table remporte la partie

4/ Le joueur qui laisse toujours un multiple de 5 sur la table remporte la partie

5/ Le joueur qui laisse toujours un multiple de 3 sur la table remporte la partie

6/ Le joueur qui laisse sur la place 12 jetons peut gagner la partie

7/ Même si le premier joueur connait la stratégie, le joueur qui joue en second peut remporter la partie

8/ Si le nombre initial de jetons est modifié et vaut n, le premier joueur doit diviser n par 3. Si le reste de la division est 2, il retire 2 jetons au premier coup. Si le reste de la division est 1, il retire 1 jeton au premier coup. Si le reste de la division est 0 et que le second joueur connait la stratégie gagnante, le premier joueur ne peut pas gagner.

Indice : c'est un jeu de type NIM

Réponse : 1, 3, 5, 6, 8

9 Références bibliographiques

[1] *Gauss: une révolution de la théorie des nombres*. Barcelone: RBA Coleccionables, 2018.

[2] Y. Brémont et P. Réocreux, *Mécanique du solide indéformable: calcul vectoriel, cinématique cours et exercices résolus classes préparatoires aux grandes écoles*. in Mécanique, no. 1. Paris: Ellipses, 1995.

[3] J. Deulofeu, *Dilemmes de prisonniers et stratégies dominantes: la théorie des jeux*. in Le monde est mathématique, no. 7. Paris: RBA France, 2013.

[4] J. Vélu, *Méthodes mathématiques pour l'informatique: cours et exercices corrigés*, 5è ed. in Info Sup. Malakoff: Dunod, 2019.

[5] J. Vélu, G. Avérous, I. Gilles, et F. Santi, *Mathématiques pour l'informatique: rappels de cours, méthodes, exercices et problèmes avec corrigés détaillés*. in Sciences sup. Paris: Dunod, 2008.

[6] V. Torra, *Du boulier à la révolution numérique: algorithmes et informatique*. in Le monde est mathématique, no. 13. Paris: RBA France, 2013.

[7] *Codage et cryptographie mathématiciens, espions et pirates informatiques*. Paris: RBA France, 2013.

[8] S. Belhaj et A. Ben Aïssa, *Mathématiques pour l'informatique: cours et exercices corrigés licence 1 & 2 informatique*. Paris: Vuibert, 2013.

[9] J. Buchmann, *Introduction à la cryptographie: cours et exercices corrigés*. Paris: Dunod, 2006.

[10] A. Billionnet, *Exercices et problèmes résolus de recherche opérationnelle. Tome 3, Programmation linéaire et extensions ; problèmes classiques*. Paris: Masson, 1991.

[11] V. Bonnet, « COURS DE MATHÉMATIQUES Terminale S ». 2011.

https://www.canal-u.tv/video/tele2sciences/chapitre_arithmetique_partie_1_division_euclidienne_et_pgcd.10082

http://www.maths-france.fr/Terminale/TerminaleS/Cours/20-arithmetique.pdf

Reconnaitre qu'un nombre est premier https://www.youtube.com/watch?v=JNssbGROVL8

Jeux de type NIM https://fr.wikipedia.org/wiki/Jeux_de_Nim

Codage RSA

https://www.canal-u.tv/video/tele2sciences/kezako_comment_crypte_t_on_les_donnees_sur_internet.8957

https://www.youtube.com/watch?v=M7vOxKVLsVY

https://www.youtube.com/watch?v=Xlal_d4zyfo

http://images.math.cnrs.fr/IMG/pdf/roulette-russe-idm.pdf

Euclide étendu sur SCILAB

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjkuOPS3dnrAhVSJBoKHb-8AbEQFjAAegQIBBAB&url=https%3A%2F%2Fwww.pedagogie.ac-nantes.fr%2Fmedias%2Ffichier%2Ftd1_1421784804167.pdf%3FID_FICHE%3D1420558704606%26INLINE%3DFALSE&usg=AOvVaw2YnjvzFWhukBDCO0zXl_it

Un peu de détente

https://www.canal-u.tv/video/ehess/magie_en_base_deux.52627

9.1 Références historiques, notions diverses

Euclide, De Fermat, Bezout, Euler, Gauss, L'os d'Ishango, Le dernier théorème de Fermat : 350 ans de recherche pour un seul théorème !, un fichier EXCEL vieux de 4000 ans : https://www.canal-u.tv/video/institut_fourier/emmanuel_peyre_des_nombres_au_hasard.38721