ALICE & BOB

Initiation à la Cryptologie

Université de Limoges

IREM Institut de Recherche sur l'Enseignement des Mathématiques

http://www.irem.unilim.fr/

2017/2019

I/ Première partie : Les nombres premiers

Nombres premiers entre eux

On dit que deux nombres entiers a et b sont premiers entre eux si leur $PGCD$ est 1 :

> « a et b sont premiers entre eux si $PGCD(a;b) = 1$ »

Par exemple 5 et 12 sont premiers entre-eux car $PGCD(5;12) = 1$; 28 et 49 ne le sont pas car $PGCD(28;49) = 7$.

Nombres premiers

On appelle « nombre premier » tout entier naturel p ayant exactement deux diviseurs, lui-même et 1.

> « p est premier si pour tout $m \in \mathbb{N}, m < p, PGCD(p;m) = 1$ »

Ainsi, 20 qui est divisible par 1, 2, 4, 5, 10 et 20 n'est pas un nombre premier ; 17 qui n'est divisible que par 1 et 17 est un nombre premier.

Procédure de recherche de nombres premiers

Vérifier si un nombre entier N est un nombre premier se nomme « test de primalité ». Il en existe plusieurs sortes, plus ou moins complexes, plus ou moins rapides...
Pour un élève de lycée ou de collège, la façon la plus simple - mais sans doute la moins efficace aussi - consiste à effectuer la division euclidienne du nombre N par tous les entiers successifs de 1 à $\sqrt{N}$ et de vérifier pour chaque calcul si le reste obtenu est nul ou non.

Propriété : Divisibilité par m [1]

La divisibilité d'un nombre N par le nombre m peut s'exprimer de différentes façons.
« Un entier naturel n est divisible par m si et seulement si :

- le reste de la division euclidienne de N par m est nul,
- $N \equiv 0 \pmod{m}$ (N *est congru à* 0 *modulo* m),
- la partie décimale du quotient $\frac{N}{m}$ est nulle,
- la partie entière du quotient $\frac{N}{m}$ est égale au quotient $\frac{N}{m}$. »

Activité : Nombres premiers entre-eux [1]

Établissez la liste ordonnée L_n de tous les nombres strictement inférieurs à n et premiers avec n lorsque $n = 12$, $n = 19$ et $n = 35$ (*) :

1. $L_{12} = \{$ ..... $\}$
2. $L_{19} = \{$ ..... $\}$
3. $L_{35} = \{$ ..... $\}$

Activité : Trouver des nombres premiers [2]

Établissez une liste ordonnée de tous les nombres premiers (†) de 1 à 100 : .....

(*). La plupart des calculatrices de lycée possèdent une fonction de calcul du $PGCD$ de deux nombres entiers.
(†). L'annexe de ce document propose un algorithme de recherche

Activité : Test de primalité 3

Les nombres suivants sont-ils premiers ?

331 1789 1973 2017 2099 207030040050 5^{99} 2017^{2018} 592159 4233683

.....

.....

.....

.....

Activité : Factoriser un nombre entier 4

Écrivez chaque nombre n comme un produit de deux nombres entiers p et q différents de 1 et n.

factoriser $n = 51$	**factoriser** $n = 8633$	**factoriser** $n = 60491$
$51 =$ $\times$	$8633 =$ $\times$	$60491 =$ $\times$

II/ Seconde partie : L'exponentiation modulaire

Petit théorème de Fermat

Soit $a \in \mathbb{N}$ et p un nombre premier non diviseur de a,

$$a^{p-1} \equiv 1 \pmod{p}$$

Théorème d'Euler

Soit p et q deux nombres premiers, on pose $n = pq$. Pour tout entier naturel a premier avec n,

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

Activité : Trouver le reste d'une division euclidienne lorsque le dividende est un grand nombre 5

1. Calculez $2^8 \pmod{11}$ .....

.....

2. Calculez $3^{25} \pmod{29}$ .....

.....

$2^8 \pmod{11}$	$3^{25} \pmod{29}$

Activité : Trouver un exposant modulaire 6

1. Déterminez k tel que $2^k \equiv 6 \pmod{11}$ .....

.....

.....

2. Déterminez k tel que $3^k \equiv 26 \pmod{29}$ .....

.....

.....

solution de $2^k \equiv 6 \pmod{11}$	**solution de** $3^k \equiv 26 \pmod{29}$
$k =$	$k =$

III/ Troisième partie : Le codage RSA

Activité : Se fabriquer une clef publique de chiffrement

7

Vous allez produire une clef publique de chiffrement que vous mettrez en évidence sur votre plan de travail.

1. Choisissez deux nombres premiers p et q et calculez le produit $n = pq$:

p	q	n

2. Calculez $\varphi(n) = (p-1) \times (q-1) =$.....

$\varphi(n)$

Ce nombre appelé « indicatrice d'Euler », représente le nombre de nombres premiers avec n ; c'est à dire le nombre d'entiers dont le plus grand diviseur commun (PGCD) avec n est 1.

3. Choisissez un nombre c premier avec $\varphi(n)$.
Il suffit de vérifier avec la calculatrice que $PGCD(c;\varphi(n)) = 1$ (on note aussi $c \wedge \varphi(n) = 1$).

c

4. Votre clef publique est prête, c'est le couple $(c;n)$ que vous pouvez afficher pour vos camarades : ils l'utiliseront pour vous faire parvenir des messages chiffrés.

$(c;n)$

Activité : Se fabriquer une clef privée de déchiffrement (avec l'aide des professeurs)

8

Vous allez produire une clef privée qui va vous permettre de déchiffrer les messages qui vous parviendront.

1. Calculez l'inverse modulaire d de c modulo $\varphi(n)$; c'est à dire le nombre d tel que :

$$c \times d \equiv 1 \pmod{\varphi(n)} \quad \text{ou encore} \quad d \equiv c^{-1} \pmod{\varphi(n)}$$

d

2. Votre clef privée est prête, c'est le couple $(d;n)$ que vous devez impérativement conserver secret.

$(d;n)$

Activité : Chiffrer un message

9

Vous allez maintenant chiffrer un message court (5/10 lettres) que vous transmettrez au groupe de votre choix. Pour cela, on utilisera la table de codage alpha-numérique suivante :

A = 01	B = 02	C = 03	D = 04	E = 05	F = 06	G = 07	H = 08	I = 09	J = 10	K = 11	L = 12	M = 13
N = 14	O = 15	P = 16	Q = 17	R = 18	S = 19	T = 20	U = 21	V = 22	W = 23	X = 24	Y = 25	Z = 26

1. Notez la clef publique $(c';n')$ de chiffrement du groupe de votre choix :

$(c';n')$ clé publique du groupe destinataire du message

2. Écrivez en clair le message que vous souhaitez faire parvenir au groupe puis procédez à son codage : chaque lettre (dans la réalité, ce sont des groupes de lettres) est associé à un nombre M_i.
Dans ce cas, votre message n'est fait que de nombres entre 01 et 26.

message en clair

message codé

3. Chiffrez chaque nombre M_i obtenu par l'exponentiation modulaire suivante :

$$C_i = M_i^{c'} \pmod{n'}$$

message chiffré à envoyer

4. Remettez à son destinataire le message chiffré que vous avez obtenu. Ce message peut même être rendu public car seul le destinataire sera en mesure de le déchiffrer.

Activité : Déchiffrer un message

10

Vous avez reçu un message ? Vous n'aurez aucun mal à le déchiffrer avec votre clé privée $(d;n)$ de déchiffrement.

1. Notez soigneusement le message chiffré reçu :

message chiffré reçu

2. Chaque groupe de deux chiffres du message reçu correspond à une lettre chiffrée avec votre clé publique. Déchiffrez chacune d'elles en appliquant la formule ci-dessous puis procédez à la transcription du message en lettres :

$$M_i = C_i^d \pmod{n}$$

message déchiffré

message en clair

3. Remerciez votre correspondant par un message chiffré.

IV/ Annexes

Un algorithme de recherche de nombres premiers

L'algorithme suivant permet la recherche de nombres premiers dans un intervalle choisi par l'utilisateur. Celui-renseigne la borne inférieure `min` et la borne supérieure `max` ; le reste du travail est effectué lors de la boucle itérative « `Pour` ».
Lors de chaque itération, on teste si le nombre `N` est divisible par tous les entiers `n` qui sont inférieurs ou égaux à la racine carrée de `N` (boucle `tant que`). Si aucun des entiers `n` n'est diviseur de `N` alors le test de primalité est positif.
Bien que simple, la méthode est malheureusement coûteuse en temps car elle effectue des calculs inutiles : en effet, si `N` n'est pas divisible par un entier `n`, alors `N` n'est divisible par aucun des multiples de `n`...

Recherche de nombres premiers dans un intervalle $[\min; \max]$

```
1  saisir min
2  saisir max
3  pour N allant de min à max faire
4      D ← 2
5      P ← 1
6      tant que D ≤ √N et P = 1 faire
7          si partie entière de (N ÷ D) = N ÷ D alors
8              P ← 0
9          sinon
10             D ← D + 1
11     si P = 1 alors
12         afficher N
```

Un algorithme d'exponentiation modulaire

L'algorithme suivant permet la recherche du reste de la division euclidienne d'une nombre `B` à l'exposant `E` par un entier `M`.
L'avantage principal de cet algorithme est qu'il permet de traiter de très grands nombres sans devoir réellement les calculer. Magique !

Calcul de R dans $B^E \equiv R \pmod{M}$

```
1  saisir B
2  saisir E
3  saisir M
4  R ← B mod M pour I allant de 2 à E faire
5      R ← (R × B) mod M
6  afficher R
```

N.B. : Certaines calculatrices possèdent déjà cette fonction sans qu'il soit nécessaire de les programmer.