DÉPARTEMENT DE MATHÉMATIQUES UNIVERSITÉ DE MONTPELLIER

Arithmétique
Feuille n° 4 Théorème d'Euler, algorithme RSA et révisions

Théorème d'Euler et algorithme RSA

Exercice 1 :

Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}/78\mathbb{Z}$?

Exercice 2 : Fait en cours

Le but de cet exercice est de se familiariser avec une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978.

1. Calculer le reste dans la division euclidienne par 55 de 8^{23}.

2. Après avoir justifié son existence, calculer l'inverse modulaire de 23 modulo 40.

On souhaite maintenant appliquer le protocole RSA. On choisit $p = 5$, $q = 11$ et $c = 23$. Un message M de $\mathbb{Z}/N\mathbb{Z}$ sera chiffré en envoyant $M^c[N]$ et un message chiffré W sera déchiffré en calculant $W^d[N]$ où d est l'inverse modulaire de c modulo $\varphi(N)$.

3. Calculer $N = pq$ et $n = \varphi(N)$ pour les valeurs de p et q choisies.

4. c est-il premier avec n ?

5. Un émetteur veut chiffrer le nombre 8 : quelle est la valeur du message chiffré ?

6. Le récepteur reçoit le nombre 17 et veut le déchiffrer : à quel nombre en clair correspond-il ?

Exercice 3 :

On reprend dans cet exercice les notations de l'exercice précédent (et du cours). On considère les valeurs $p = 53$, $q = 11$ et $c = 2$.

1. Calculer la clé publique, c'est-à-dire (N, c).

2. Calculer la clé privée, c'est-à-dire d associée.

3. Bob veut envoyer le message "219" : quelle est la valeur du message chiffré ?

4. Vérifier que la valeur déchiffrée calculée par Alice correspond au message que Bob voulait envoyer.

Exercice 4 : RSA avec deux facteurs trop proches, source : Anca Nitulescu

Supposons que l'entier N soit le produit de deux nombres premiers p et q proches (on peut supposer $p > q$). On pose $t = \frac{p+q}{2}$ et $s = \frac{p-q}{2}$. Montrez que :

1. L'entier s est petit

2. $N = t^2 - s^2$

3. t est légèrement supérieur à la racine carrée de N.

On peut utiliser ces informations pour factoriser N. Grâce à l'algorithme suivant :

Algorithme de Fermat
$t \leftarrow \lceil \sqrt{N} \rceil$
$z = 2$
Tant que z n'est pas un carré :

1. $t \leftarrow t + 1$
2. $z \leftarrow t^2 - N$

Retourner $p = t + \sqrt{z}$

4. Appliquer cet algorithme pour factoriser 899, 110417 puis 364957402.

5. Trouver la clé secrète d correspondant à $N = 51983$ et $c = 17$

Révisions : Annales de 2024

Exercice 5 : (6 points)

Une année "normale" comporte 365 jours. Toutes les années
- multiples de 400
- ou multiples de 4 mais pas de 100

sont bissextiles : elles comportent 366 jours (avec un 29 février rajouté).
Cette année, le premier janvier (2024 donc) est tombé un lundi.

1. L'année 2024 est-elle bissextile ?

2. Combien y aura-t-il de mardi cette année 2024 ?

3. Quel jour de la semaine (lundi, mardi, mercredi, jeudi, vendredi, samedi ou dimanche) tombera le premier janvier 2025 ?

4. Le 1er mai 2024 sera un mercredi. En quelle année sera le prochain mercredi 1er mai ? et celui d'après ?

5. Déterminer les années multiple de 4 mais pas bissextiles entre 2024 et 2222 (il y en a 2).

6. Quel jour sera le 1er mai 2222 ?

Exercice 6 : (2 points)

Combien vaut 2023^{2024} [15] ?
Indication : on pourra commencer par calculer un représentant judicieux de la classe de 2023 *modulo* 15.

Exercice 7 : (3 points)

Soit n un entier naturel. Montrer que

1. Montrer que $4^n + 15n - 1$ est un multiple de 9

2. Montrer que $4^n + 2^n + 1$ est divisible par 7

3. ChatGPT prétend que $3^{2n+1} + 2^{n+2}$ est un multiple de 7 pour tout entier positif n : a-t-il raison ? (justifier votre réponse)

Exercice 8 : (3 points)

Le professeur Moustache regarde les photos de l'anniversaire de sa collègue Alice dont il ignore l'âge. Les amies d'Alice avaient préparé deux gâteaux. Sur le premier, l'âge d'Alice est représenté en système décimal par des bougies vertes pour les dizaines et des bougies blanches pour les unités. Sur le second, l'âge est écrit en base 12 avec des bougies roses et jaunes, les jaunes représentant les unités et les roses les douzaines. Mais les photos que montrent Alice sont en noir et blanc ! Le professeur Moustache voit 9 bougies identiques sur le premier gâteau et 10 sur le second. Pouvez-vous l'aider à trouver l'âge d'Alice ?

Exercice 9 : (8 points)

Le but de cet exercice est d'évaluer votre maîtrise d'une méthode de chiffrement à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman, qui ont inventé cette méthode de chiffrement en 1977 et l'ont publiée en 1978. On choisit $p = 7$, $q = 11$ et un c. On a alors $N = 77$. Un message M de $\mathbb{Z}/N\mathbb{Z}$ sera chiffré en envoyant $M^c[N]$ et un message chiffré W sera déchiffré en calculant $W^d[N]$ où d est l'inverse modulaire de c modulo $\varphi(N)$.

1. Calculer $n = \varphi(N)$ et $\varphi(n)$.

2. Sachant que c doit être inversible modulo n, combien y a-t-il de valeurs de c possible ?

Bob hésite entre 4 valeurs de c possibles : 7, 13, 17 et 23. Il aimerait choisir celle qui permet un décodage le plus facile possible.

3. Après avoir justifié son existence, calculer l'inverse modulaire de 7 modulo n.

4. Quel est l'inverse modulaire de 17 modulo n ?

5. Vérifier que les inverses modulaires de 13 et 23 modulo n sont respectivement 37 et 47.

Bob décide de choisir $c = 7$ et note d son inverse modulaire calculé il y a deux questions.

6. Montrer que pour tout entier W, $W^d \equiv W[7]$ et que $W^d \equiv W^3[11]$.

7. En déduire un polynôme en W de degré 3 qui permet de calculer $W^d[77]$.

8. En combien d'opérations au minimum Alice peut-elle calculer $W^7[77]$ pour un entier W quelconque ?

Révisions : Annales de 2023

a) Nombres entiers naturels

Exercice 10 :

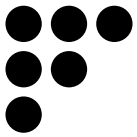
(le premier exercice proposé l'année dernière n'est plus au programme de cette année).

Exercice 11 :

Montrer par récurrence que $9^n - 5^n$ est divisible par 4 pour tout entier $n \in \mathbb{N}$.

Exercice 12 :

Les flamands voyagent disposés régulièrement en triangles. Déterminer le nombre de ces oiseaux lorsque l'on connaît le nombre de files. Par exemple, dans la figure ci-contre, les oiseaux sont représentés par les cercles noirs, il y a trois files et ils sont six au total.
Vous prouverez votre résultat par récurrence sur le nombre de files.



b) Division euclidienne

Exercice 13 :

On divise un entier positif a par 45. On trouve que le reste est égal au carré du quotient.
Pouvez-vous déterminer l'entier a ? Est-il unique ?

Exercice 14 :

Soient n, a, b trois entiers naturels. On suppose que q est le quotient de la division euclidienne de n par a et q' est le quotient de la division euclidienne de q par b. Est-il possible de déterminer en fonction de ces données :

1. Le quotient de la division euclidienne de n par b ?
2. Le quotient de la division euclidienne de n par ab ?
3. Le quotient de la division euclidienne de a par b ?

Exercice 15 :

Soit n un entier naturel. On considère les deux entiers a et b définis par :

$$a = 2n^2 + 7n + 21 \text{ et } b = 2n + 2.$$

Vous devez dire si l'affirmation suivante est vraie ou fausse : «*Pour tout entier naturel n, le quotient et le reste de la division euclidienne de a par b sont respectivement égaux à $n + 2$ et $n + 17$*».
Une réponse non justifiée ne sera pas prise en compte.

c) Numération

Exercice 16 :

Déterminer le nombre entier naturel n, qui s'écrit :

- $n = \overline{abca}^{11}$ dans le système de base 11 ;
- $n = \overline{bbac}^{7}$ dans le système de base 7

Vous devrez donner les valeurs de a, b, c ainsi que la valeur de n dans le système décimal.

Exercice 17 :

Soit b un entier supérieur à 2 et α et β deux entiers naturels vérifiant $\alpha + \beta = b + 1$.

1. Vous donnerez des exemples avec $b = 7$;
2. Montrer que $\alpha \times (b-1)$ et $\beta \times (b-1)$ s'écrivent avec les mêmes chiffres, pris en ordre inverse dans le système de numération de base b ;
3. En déduire que le double de $b-1$ et le carré de $b-1$ s'écrivent avec les mêmes chiffres pris en ordre inverse.

Exercice 18 :

On considère l'entier naturel A qui s'écrit $\overline{1x416}$ dans le système de numération de base sept, où x est un chiffre compris entre 0 et 6.

1. Déterminer x pour que :
   (a) A soit divisible par six ;
   (b) A soit divisible par cinq.
   En déduire qu'il existe x tel que A soit divisible par trente.
2. On donne à x la valeur zéro. Déterminer l'écriture décimale de A. Quel est le nombre de diviseurs positifs de A ? Quel est l'ensemble des diviseurs positifs de A qui sont premiers avec trois ?

Exercice 19 :

1. Résoudre dans $\mathbb{Z}^2$ l'équation
$$5x - 3y = 2.$$
2. Un entier naturel A s'écrit $\overline{55}$ en base x et $\overline{37}$ en base y.
Quelles sont les valeurs possibles de x et y ? Déterminer x et y sachant de plus qu'il existe un entier naturel B qui s'écrit $\overline{121}$ en base x et $\overline{59}$ en base y.
3. Écrire A et B en système décimal.

d) Congruences

Exercice 20 :

Soient a et b deux entiers naturels.

1. Démontrer que $a^2 + b^2$ est divisible par 7 si et seulement si les deux nombres a et b sont divisibles par 7.
2. Que devient le problème si on remplace 7 par 13 ? Le résoudre.

Exercice 21 :

Déterminer le reste de la division par 11 du nombre 7077^{377}.

Exercice 22 :

On considère le nombre entier $A = 18^{2023}$.

1. A est-il divisible par 9 ? Par 4 ? (Justifier les réponses)
2. Déterminer le reste de la division euclidienne de A par 7.

e) Diviseurs et multiples

Exercice 23 :

Déterminer tous les couples d'entiers naturels (x, y) vérifiant :
- $pgcd(x, y) = 18$;
- $x + y = 360$.

Exercice 24 :

Déterminer tous les couples d'entiers naturels (x, y) vérifiant :
- $ppcm(x, y) = 660$;
- $x + y = 286$.

Exercice 25 :

1. On considère dans $\mathbb{Z}^2$ l'équation :

$$11a + 7b = 2024 \tag{1}$$

   (a) Montrer que pour tout couple (a, b) solution de (1), b est divisible par 11.

   (b) En déduire l'ensemble des solutions de (1).

2. Déterminer tous les couples (p, q) d'entiers naturels non nuls, tels que

$$11m + 7d = 2024$$

   où m désigne le ppcm de p et de q, et d leur pgcd.

Exercice 26 :

On considère trois entiers naturels non nuls a, b, c. On suppose :
- $pgcd(a, b) = \delta$;
- $pgcd(b, c) = \delta'$.

Quel est le plus grand diviseur commun des trois nombres (a, b, c) ?
Sachant que $\delta = 12$, $\delta' = 18$ et que $a + b + c = 102$, déterminer toutes les valeurs possibles des trois nombres a, b, c.