UNIVERSITÉ DE RENNES 1

ARI – L2 – ISTIC – Université de Rennes 1

Arithmétique — Examen du 11/05/2018

Durée : 2h.
Les documents (cours, TD, ...) et les appareils (calculatrice, téléphones, ...) ne sont ***pas*** *autorisés.*
Chaque réponse devra être soigneusement justifiée *(ne pas se contenter d'une suite de calculs sans explications).*
Le barème indiqué est donné à titre indicatif.

Exercice 1. *(2 points)*

a) Rappeler la définition d'un nombre premier.

b) Montrer qu'il existe une infinité de nombres premiers.

Exercice 2. *(5 points)*

a) Écrire en pseudo-code l'algorithme d'Euclide pour calculer le pgcd de deux entiers a et b dans $\mathbb{N}$.

b) En utilisant cet algorithme, calculer le pgcd de 5040 et 864.

c) Donner la décomposition en facteurs premiers de 5040.

d) Donner la décomposition en facteurs premiers de 864.

e) Expliquer comment retrouver le pgcd de 5040 et 864 en utilisant les décompositions en facteurs premiers.

f) Quelle est la décomposition en facteurs premiers du ppcm de 5040 et 864 ?

Exercice 3. *(7 points)*

(A) a) Soit $n \in \mathbb{N}$. Montrer que n est pair si et seulement si n^7 est pair.

b) Pour $n \in \mathbb{N}$, on note $f(n)$ le reste de la division euclidienne de n^7 par 3. Calculer $f(0), f(1), f(2)$.

c) En déduire $f(n)$ pour $n \in \mathbb{N}$. Que vaut $f(n) - n$ modulo 3 ?

d) À l'aide du petit théorème de Fermat et des questions précédentes, démontrez que 42 divise $n^7 - n$ pour tous $n \in \mathbb{N}$.

(B) a) Calculer les coefficients binomiaux $\binom{7}{k} = \frac{7!}{k!(7-k)!}$ pour les entiers k variant de 0 à 7. Lesquels sont divisibles par 7 ?

b) De façon générale, montrer que si p est premier et $k = 1, \ldots, p-1$, alors le nombre $\binom{p}{k}$ est divisible par p.

c) Soit $p \in \mathbb{N}^*$. On rappelle la formule

$$(1+X)^p = \sum_{k=0}^{p} \binom{p}{k} X^k$$

Vérifier la formule pour $p = 2$ et $p = 3$.

d) Sans utiliser le petit théorème de Fermat, démontrer *par récurrence* que $n^7 - n$ est multiple de 7, pour tous $n \in \mathbb{N}$.

Tournez la page

Exercice 4. *(2 points)* En fouillant votre chambre vous retrouvez un vieux 'deck' Pokemon qui devait avoir à peu près une soixantaine de cartes. Vous les distribuez équitablement à vos 3 petits cousins, et il reste 2 cartes. Entre temps deux autres amis arrivent, donc vous récupérez toutes les cartes et refaites une distribution équitable. Il vous reste cette fois 4 cartes. Combien y avait-il de cartes dans le 'deck' ? (Justifier la réponse.)

Exercice 5. *(4 points)*

a) Expliquer comment fonctionne le principe général de la « cryptographie à clef publique » avec la notion de « fonction à sens unique ».

b) Alice et Bob utilisent le chiffrement RSA. Alice veut envoyer le message $m = 89$ à Bob. La clef publique de Bob est $(n = 91, e = 5)$. Indiquer quel calcul doit effectuer Alice pour chiffrer son message avant de l'envoyer, et faire ce calcul.

c) Soit d la clef privée de Bob. On note x le message chiffré envoyé par Alice. Quel calcul doit faire Bob pour déchiffrer ce message ? (Expliquer pourquoi il retrouvera bien le message initial.)

d) Camille cherche à briser la clef de Bob par une attaque par « force brute ». Indiquer les étapes à suivre. Quelle est donc la clef privée d de Bob ?

Fin de l'énoncé