INSTITUT DES HAUTES ÉTUDES

POUR LE DÉVELOPPEMENT DE LA CULTURE, DE LA SCIENCE ET DE LA TECHNOLOGIE EN BULGARIE

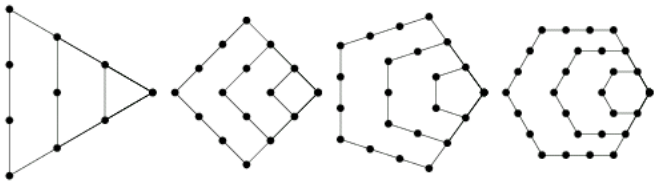
http://www.iheb.org

Concours Général de Mathématiques "Minko Balkanski"

10 mai 2009

La clarté et la précision de la rédaction, qui doit être obligatoirement en **français** *ou en* **anglais**, *seront prises en compte dans la note finale. La durée de la composition est de 4 heures.*

Problème 1. Un nombre polygonal est un nombre naturel qui peut être représenté par des points disposés en polygone régulier (triangle, carré, pentagone, hexagone etc.). Etant donnés deux nombres entiers $n \geq 3$ et $k \geq 1$ on note $P_n(k)$ le k-ième nombre n-gonal, sachant que $P_n(1) = 1$. Par exemple, le k-ième nombre carré est $P_4(k) = k^2$. La figure suivante représente les nombres polygonaux pour $3 \leq n \leq 6$ et $1 \leq k \leq 4$:



Le but de cet exercice est de trouver un critère permettant de déterminer rapidement si un nombre naturel donné N est un nombre polygonal.

1.a) Déterminer $P_3(k)$ pour tout $k \geq 1$. Démontrer, d'abord en utilisant la formule, puis graphiquement que tout nombre carré est somme de deux nombres triangulaires consécutifs.

1.b) Trouver les 3 premiers nombres pentagonaux $P_5(1), P_5(2), P_5(3)$. Prouver graphiquement que tout nombre pentagonal se décompose en une somme de trois nombres triangulaires. En déduire la formule suivante : $P_5(k) = \frac{k(3k-1)}{2}$.

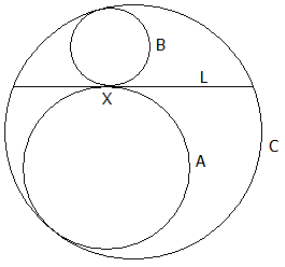
1.c) Prouver par récurrence pour tout $n \geq 3$ et tout $k \geq 1$ la formule :

$$P_n(k) = \frac{k}{2}\left((n-2)k - (n-4)\right).$$

1.d) En déduire que $8(n-2)P_n(k) + (n-4)^2$ est un carré. Réciproquement, démontrer que tout entier $N \geq 1$, tel que $8(n-2)N + (n-4)^2$ est un carré, est un nombre n-gonal.

1.e) Montrer que 6, 66 et 666 sont des nombres hexagonaux.

Problème 2. Soit L une corde d'un cercle C et soient A et B deux cercles distincts tangents à C et tangents à L au même point X. On note a et b les rayons respectifs de A et B et l'on suppose que $a \geq b$. Montrer que le quotient $\frac{a}{b}$ ne dépend pas de la position de X sur la corde L.



Problème 3. Soient p et q deux nombres premiers distincts. On considère leur produit $n = pq$ et l'on choisit un entier e, $1 < e < \varphi(n)$ relativement premier avec $\varphi(n)$, où φ désigne la fonction indicatrice d'Euler.

3.a) Montrer qu'il existe un unique entier d, $1 < d < \varphi(n)$, vérifiant $ed \equiv 1 \pmod{\varphi(n)}$.

3.b) Montrer que pour tout entier M, on a $M^{ed} \equiv M \pmod{n}$ (*l'on pourra distinguer deux cas suivant que M et n sont relativement premiers ou non*).

On appelle e l'exposant de chiffrement et d l'exposant de déchiffrement. La paire (n, e) est la *clé publique*, qui permet de chiffrer un message, et la paire (n, d) est la *clé privée*, qui permet de déchiffrer un message chiffré. Un message est représenté par un entier $M \in [0, n-1]$. Sachant la clé publique (n, e), l'on chiffre le message en calculant $C \equiv M^e \pmod{n}$. La clé privée (n, d) permet de déchiffrer C, car en vertu du 3.b., l'on a $M \equiv C^d \pmod{n}$. C'est la méthode de cryptage RSA.

Une attaque possible contre RSA consiste à tenter de factoriser n pour retrouver p et q, afin de calculer $\varphi(n)$, puis l'exposant de déchiffrement d. Cependant décomposer un grand entier n en facteurs premiers est en général infaisable.

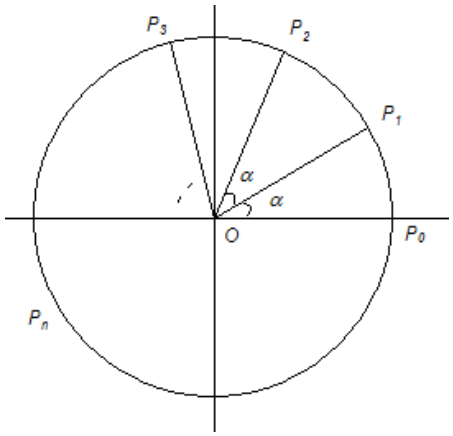
3.c) On suppose que le même message M est chiffré deux fois (pour deux personnes différentes) avec clés (n, e) et (n, e') pour donner C et C'. Sous l'hypothèse que e et e' sont relativement premiers, montrer que l'on peut retrouver "rapidement" M à partir de C et C'.

3.d) Afin d'accélérer la fonction de chiffrement dans le cryprosystème RSA, on est amené à prendre un exposant e aussi petit que possible. Expliquez pourquoi $e = 2$ ne satisfait jamais nos hypothèses de départ? Soit $e = 3$ et supposons que le même message M est chiffré en C, C' et C'' en utilisant trois clés distinctes $(n, 3)$, $(n', 3)$ et $(n'', 3)$. Si $M < \min(n, n', n'')$, montrer que l'on peux retrouver "rapidement" M à partir de C, C' et C''.

Problème 4. La dernière question de ce problème est indépendante du reste et peut être traitée séparément. Soit $\alpha = \arccos(\frac{4}{5}) \in [0, \frac{\pi}{2}]$

a) Calculer $\sin(\alpha)$. Démontrer que pour chaque nombre entier $n \geq 0$, $\cos(n\alpha)$ et $\sin(n\alpha)$ sont tous les deux rationnels.

Nous allons noter P_n le point du cercle unité ayant pour coordonnées $(\cos(n\alpha), \sin(n\alpha))$.



b) Montrer que pour tout $n > m \geq 0$ la distance entre P_{2n} et P_{2m} est un nombre rationnel.

c) Prouver que pour tout $n > 0$, $\sin(n\alpha) \neq 0$. Déduire que les points P_n, $n \geq 0$, sont deux à deux distincts.

d) Démontrer que pour tout entier $N \geq 2$, il existe N points du plan dont aucun triplet n'est colinéaire (sur la même droite), et de sorte que la distance entre tout couple de points soit un nombre entier.

e) Soient A et B deux points du plan et d un nombre réel positif ou nul strictement inférieur à AB. L'ensemble des points Z tels que $|AZ - BZ| = d$ s'appelle une hyperbole.

On peut désormais supposer que deux hyperboles distinctes ont au plus quatre points d'intersection. Démontrer que s'il existe un nombre infini de points dans le plan, tels que la distance entre tout couple de points soit un nombre entier, alors tous ces points sont situés sur la même droite.

FIN

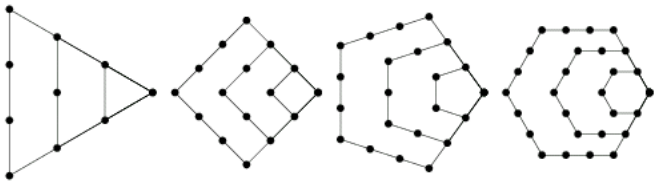
INSTITUT DES HAUTES ÉTUDES
POUR LE DÉVELOPPEMENT DE LA CULTURE, DE LA SCIENCE ET DE LA TECHNOLOGIE EN BULGARIE
http://www.iheb.org

Concours Général de Mathématiques "Minko Balkanski"

May 10th 2009

All the answers must be given in **English** *or in* **French**. *The clarity and precision will be taken into account for the final grade.Time limit : 4 hours.*

Problem 1. A polygonal number is a number represented as dots arrayed in the shape of a regular polygon (triangle, square, pentagon, etc.). Given two natural numbers $n \geq 3$ and $k \geq 1$ we denote $P_n(k)$ the k-th n-gonal number, knowing that $P_n(1) = 1$. For example, the k-th square number is $P_4(k) = k^2$. The following figure shows the polygonal numbers for $3 \leq n \leq 6$ and $1 \leq k \leq 4$:



The goal of this exercice is to find a criterion allowing to quickly verify whether a given natural number N is polygonal or not.

1.a) Calculate $P_3(k)$ for each $k \geq 1$. Prove that each square number is representable as a sum of two consecutive triangular numbers, first by using the formula, then graphically.

1.b) Find the first 3 pentagonal numbers $P_5(1), P_5(2), P_5(3)$. Prove by a graphical method that each pentagonal number can be decomposed as the sum of three triangular numbers. Deduce the following formula : $P_5(k) = \frac{k(3k-1)}{2}$.

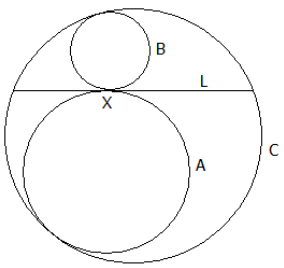
1.c) Prove by induction for every $n \geq 3$ and $k \geq 1$ the following formula :

$$P_n(k) = \frac{k}{2}\left((n-2)k - (n-4)\right).$$

1.d) Verify that $8(n-2)P_n(k) + (n-4)^2$ is a square. Conversely, prove that each natural number $N \geq 1$, such that $8(n-2)N + (n-4)^2$ is a square, is an n-gonal number.

1.e) Establish that 6, 66 and 666 are all hexagonal numbers.

Problem 2. Let L be a chord of a given circle C and let A and B be two distinct circles both tangent to C and tangent to L at the same point X. Let a and b be the radii of A and B respectively and suppose that $a \geq b$. Prove that the ratio a/b is independent of the position of X on the chord L.



Problem 3. Let p and q be two distinct prime numbers. We consider their product $n = pq$ and we choose an integer e coprime with $\varphi(n)$, such that $1 < e < \varphi(n)$, where φ denotes the Euler indicator function.

3.a) Prove that there exists an unique integer d, $1 < d < \varphi(n)$ verifying $ed \equiv 1 \pmod{\varphi(n)}$.

3.b) Establish that for every integer M, $M^{ed} \equiv M \pmod{n}$ (*two cases should be considered depending on whether M and n are coprime or not*).

The number e is the encryption exponent and d is the decryption exponent. The (n, e) couple is the *public key*, which allows the encryption of the message, and the couple (n, d) is the *private key* which decrypts the encrypted message. A message can be represented by an integer number $M \in [0, n-1]$. Knowing the public key (n, e), the message is encrypted by calculating $C \equiv M^e \pmod{n}$. The private key (n, d) is then used to decrypt C, according to 3.b., as we have $M \equiv C^d \pmod{n}$. This algorithm is known as RSA.

A possible attack against an RSA-encrypted message consists in trying to decompose n in order to determine p and q, then $\varphi(n)$, and finally the decryption exponent d. Nevertheless decomposing a large integer n in prime factors is unfeasible in general.

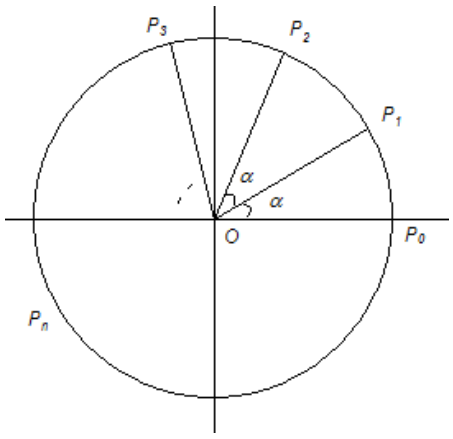
3.c) Suppose that the same message M is encrypted twice (for two different persons) with the keys (n, e) and (n, e'), thus obtaining C and C'. Prove that if e and e' are coprime, then M can be "quickly" recovered out of C and C'.

3.d) In order to accelerate the encryption process of the RSA algorithm, we should choose the smallest possible encryption exponent e. Explain why $e = 2$ never satisfies our initial assumptions? Let $e = 3$ and suppose that the same message M is encrypted as C, C' and C'' using three distinct public keys $(n, 3)$, $(n', 3)$ et $(n'', 3)$ respectively. If $M < \min(n, n', n'')$, prove that the message M can be "quickly" recovered out of C, C' and C''.

Problem 4. The last question of this problem is independent of the rest and can be treated separately. Let $\alpha = \arccos(\frac{4}{5}) \in [0, \frac{\pi}{2}]$

a) Compute $\sin(\alpha)$. Show by that for every integer $n \geq 0$, $\cos(n\alpha)$ and $\sin(n\alpha)$ are both rational numbers.

Denote by P_n the point of the unit circle with coordinates $(\cos(n\alpha), \sin(n\alpha))$.



b) Show that for all $n > m \geq 0$ the distance between P_{2n} and P_{2m} is a rational number.

c) Show that for all $n > 0$, $\sin(n\alpha) \neq 0$. Deduce that the points P_n, $n \geq 0$, are two by two distinct.

d) Prove that for any integer $N \geq 2$ there exist N points on the plane, none three of which being collinear (on the same line), such that the distance between any two of them is an integer number.

e) Let A et B be two points in the plane and d a non-negative real number strictly smaller than AB. The set of points Z such that $|AZ - BZ| = d$ is is called a hyperbola.

Assuming that two different hyperbolas intersect in at most four points, prove that if there are an infinite number of points in the plane, such that the distance between any two of them is an integer number, then all the points must lie on the same line.

END