Examen lundi 12 décembre 2011

1. Géométrie

Exercice 1. *Dans le plan on se donne cinq points distincts notés $M_i, i \in \mathbb{Z}/5\mathbb{Z}$. Déterminer cinq points $P_i, i \in \mathbb{Z}/5\mathbb{Z}$, tels que pour tout $i \in \mathbb{Z}/5\mathbb{Z}$, M_i soit le milieu de $[P_iP_{i+1}]$.*

Exercice 2. *Étant donnés un segment $[AB]$ de longueur c et deux nombres réels strictement positifs a et m, contruire tous les triangles ABC tel que la longueur de $[BC]$ soit a et la longueur de la médiane issue de A soit m.*

2. Arithmétique

Exercice 3. Nous allons montrer qu'un nombre premier de la forme $4n+1$ est la somme de deux carrés.

Notons n un entier tel que le nombre $p = 4n+1$ soit premier et $E = \{1, 2, \dots, p-1\}$ l'ensemble des entiers strictement compris entre 0 et p.

(1) *Montrer qu'il existe une bijection $i : E \to E$ telle que $xi(x) \equiv 1 \mod p$ pour tout $x \in E$.*

(2) *Montrer que pour tout $x \in E$ l'ensemble $E_x = \{x, i(x), p-x, p-i(x)\}$ a exactement deux ou quatre élements. Montrer que le nombre de partie E_x ayant exactement deux éléments est pair. Donner E_1, en déduire qu'il existe un entier $c \in E$ tel que $c^2 + 1 \equiv 0 \mod p$.*

(3) *On note e la partie entière de $\sqrt{p}$. Montrez que $(e+1)^2 - 1 \geq p$.*

(4) *L'application $\{0, 1, \dots, e\}^2 \to \{0, 1, \dots, p-1\}; (x, y) \mapsto a$ où $a \equiv x + cy \mod p$ est-elle injective ?*

(5) *Montrez qu'il existe deux couples distincts d'entiers compris entre 0 et e que l'on notera (x_1, y_1) et (x_2, y_2) vérifiant $y_1 - cx_1 \equiv y_2 - cx_2 \mod p$.*

(6) *En déduire l'existence d'un couple d'entier compris entre $\sqrt{p}$ et $\sqrt{p}$ tel que $b \equiv ca \mod p$ et $p = a^2 + b^2$.*

Et les autres ?

(7) *Un nombre premier de la forme $4n-1$ pour $n \in \mathbb{N}^*$ peut-il être somme de deux carré ?*

(8) *Un nombre premier peut-il n'être ni de la forme $4n+1$ ni de la forme $4n-1$?*

Exercice 4. Nous allons montrer qu'il existe des polynômes $P \in \mathbb{Z}[X]$ prenant une infinité de valeurs premières sur $\mathbb{N}$. Néanmoins un tel polynôme devra aussi y prendre une infinité de valeurs composées.

Soient $a \in \mathbb{N}, a > 2$, p un nombre premier, $p > a$ et $E_r = \{p \in \mathbb{N} \mid p \text{ premier }, p \equiv r \mod a\}$. On notera $N = \prod_{\substack{q \text{ premier} \\ q \leq p}} q$, $a = \prod_{p \text{ premier}} p^{\alpha_p}$ la factorisation de a en produit de nombres premier et $\alpha = max\{\alpha_p \mid p \text{ premier}\}$

(1) *Montrez que $a \wedge (N^\alpha - 1) = 1$. En déduire que $N^\alpha - 1$ admet un diviseur premier de la forme $an + r$ avec $2 \leq r \leq a-1$ strictement plus grand que p.*

(2) *Montrer que $\cup_{r=2}^{a-1} E_r$ est un ensemble infini et en déduire un polynôme Q tel que l'ensemble $\{n \in \mathbb{N} \mid Q(n) \text{ premier}\}$ soit infini.*

Soit $P \in \mathbb{Z}[X]$ un polynôme non constant.

(3) *Montrer qu'il existe $N \in \mathbb{N}$ tel que si $n \geq N$ alors $|P(n)| > 1$ en déduire que $P(N)$ admet un diviseur premier que l'on notera p. Vérifier que pour tout $k \in \mathbb{N}^*$ assez grand $|P(N + kp)| > p$.*

(4) *Montrer que $P(N + kp) \equiv P(N) \mod p$ et en déduire que l'ensemble des entier n tels que $P(n)$ ne soit pas premier est infini.*

Par exemple, choisissons $P(X) = X^2 + X - 1$.

(5) *Soit d un diviseur premier de $P(2)$ et montrer que d divise $P(2 + dk)$ pour tout $k \in \mathbb{N}$.*

(6) *Résoudre l'équation aux congruences $(2n+1)^2 \equiv 0 \mod 5$.*

(7) *En déduire que l'ensemble des valeurs prises par P sur $\mathbb{N}$ qui sont divisibles par d est $\{P(2+dk) \mid k \in \mathbb{N}\}$.*

3. CORRECTION

Exercice 1. *c.f.* correction du contrôle continu.

Exercice 2. Nous allons contruire le triangle ABM où M est le milieu de $[BC]$. Comme $BM = a/2$, $AM = m$ et $AB = c$, une condition nécessaire et sufissante pour que le triangle existe et ne soit pas plat est que les **trois** inégalités triangulaires soient vérifiées : $a/2 + m > c$, $a/2 + c > m$ et $c + m > a/2$.

On construit alors le point M comme intersection du cercle de centre A et de rayon m et du cercle de centre B et de rayon $a/2$. Le point C est le symétrique de B par rapport à M. Lorsque les trois conditions ci-dessus sont vérifiés, on a deux triangles ABC satisfaisant les condition de l'énoncé.

Exercice 3.
(1) Si $x \in E$ alors $x \wedge p = 1$, d'après le théorème de Bézout il existe $(u, v) \in \mathbb{Z}^2$ tel que $xu + pv = 1$. En notant $i(x)$ le reste de la division euclidienne de u par p on a : $xi(x) \equiv 1 \mod p$.

$x \mapsto i(x)$ est bien définie car si y_1 et y_2 sont deux nombres de E vérifiant $xy_1 \equiv xy_2 \equiv 1 \mod p$ alors $x(y_1 - y_2)$ est un multiple de p. Or $x \wedge p = 1$ donc p divise $y_1 - y_2$. Mais $-p < y_1 - y_2 < p$ donc $y_1 = y_2$.

Par unicité de $i(x)$ on a $i \circ i(x) = x$. Puisque l'identité est injective, i est injective. Puisque l'identité est surjective, i est surjective.
(2) E_x a plus de deux éléments car p étant impair, $x \neq p - x$. Si E_x a moins de quatre éléments alors soit $x = i(x)$ et dans ce cas $p - x = p - i(x)$: E_x a deux éléments ; soit $x = p - i(x)$ et dans ce cas $p - x = i(x)$: E_x a deux éléments.

Soit $\mathscr{E} = \{E_x | x \in E\}$. Montrons que $\mathscr{E}$ est une partition de E. Si $a \in E_x \cap E_y$ alors $E_a \subset E_x \cap E_y$ et d'après la question précédente $E_a = E_x = E_y$. Ainsi pour tout $x \in E$ il existe une unique partie $P \in \mathscr{E}$ tel que $x \in P$. On a alors $\#E = \sum_{P \in \mathscr{E}} \#P$. Soit $\mathscr{E}_i = \{E_x | x \in E \text{ et } \#E_x = i\}$. On a $\mathscr{E} = \mathscr{E}_2 \cup \mathscr{E}_4$ et $\#E = 4\ \#\mathscr{E}_4 + 2\ \#\mathscr{E}_2$, c'est-à-dire $\#\mathscr{E}_2 = 2n - 2\ \#\mathscr{E}_4$.

$E_1 = \{1, p - 1\}$, il existe donc un $c \in E$, $c \notin E_1$, tel que $\#E_c = 2$. Pour cela on doit avoir $c = p - i(c)$ c'est-à-dire $-c^2 \equiv 1 \mod p$.
(3) On a $1 \leq e \leq \sqrt{p} < e + 1$ donc $p < (e+1)^2$. Comme nous comparons deux entiers on a en fait $p \leq (e+1)^2$.
(4) On a $\#\{1, \ldots, e\}^2 = (e+1)^2$ et $\#\{0, \ldots, p-1\} = p$. L'inégalité (3) interdit à l'application d'être injective.
(5) et (6) Il existe donc deux couples distincts tels que $x_1 + cy_1 \equiv x_2 + cy_2 \mod p$. En multipliant les deux cotés par $-c$ on obtient l'égalité voulue, c'est-à-dire $c(x_1 - x_2) = y_1 - y_2$. Posons $a = x_1 - x_2$ et $b = y_1 - y_2$. On a bien $ca \equiv b \mod p$ et $c^2a^2 \equiv b^2 \mod p$. Cette dernière congruence donne l'existence d'un entier k tel que $a^2 + b^2 = kp$.

Puisque $0 \leq x_1 < \sqrt{p}$ et $0 \leq x_2 < \sqrt{p}$ on a $-\sqrt{p} \leq a < \sqrt{p}$; de même pour b. En conséquent $a^2 + b^2 < 2p$ ainsi $a^2 + b^2 = p$.
(7) Un carré est congru modulo 4 à 0 ou 1. La somme de deux carré ne peut pas être congrus à 3 modulo 4.
(8) A part 2, les nombres premier sont impairs et donc congrus à 1 ou -1 modulo 4.

Exercice 4.
(1) Puisque $p > a$ les diviseurs premiers de a sont plus petits que p et

$$a = \prod_{p \text{ premier}} p^{\alpha_p} = \prod_{q \text{ premier}} q^{\alpha_q} = \prod_{\substack{q \text{ premier} \\ q \leq p}} q^{\alpha_q}.$$

Puisque pour tout q premier $\alpha \geq \alpha_q$ a divise N^α et est donc premier à $N^\alpha - 1$.

Soit d un diviseur premier de $N^\alpha - 1$. Tous les nombres premiers plus petit que p divisant N, ils ne divisent pas $N^\alpha - 1$ et $d > p$. Par division euclidienne, $d = an + r$ avec $r \in \{0, \ldots a - 1\}$. Puisque d est premier plus grand que a, $r \neq 0$. Si tous les diviseurs premiers de $N^\alpha - 1$ étaient congrus à 1 modulo a, il en serait de même de leurs produits en particulier de $N^\alpha - 1$. Or celui-ci est congru à -1. Il existe donc un diviseur premier de $N^\alpha - 1$ congru à $r \in \{2, \ldots a - 1\}$ modulo a.
(2) D'après (1), $\cup E_r \neq \emptyset$. Notons p_0 un ces éléments. Pour $n \in \mathbb{N}$, si p_n un premier dans $\cup E_r$ alors, par (1), il existe $p_{n+1} > p_n$ dans $\cup E_r$. Cette réunion finie d'ensemble est donc infinie et l'un des ensemble E_r doit être infini, disons E_{r_0}. Le polynome $Q(X) = aX + r_0$ répond à la question.
(3) Puisque $|P(n)| \underset{n \to +\infty}{\longrightarrow} +\infty$, il existe N tel que si $n \geq N$ alors $|P(n)| > 1$. Tout entier différent de -1 et 1 admet un diviseur premier. Puisque $|P(N + kp)| \underset{k \to +\infty}{\longrightarrow} +\infty$, pour tout $A \in \mathbb{Z}$ il existe K tel que si $k \geq K$ alors $|P(N + kp)| > A$. En particulier pour $A = p \ldots$
(4) Les congruences étant compatibles au sommes et aux produits, $N + kp \equiv N \mod p$ implique $P(N + kp) \equiv P(N) \mod p$ (Ceci montre aussi (5)). Pour tout k assez grand le nombre $P(N + kp)$ est strictement plus grand que p et divisible par p / c'est donc un nombre composé.
(6) 5 étant premier, $(2n + 1)^2 \equiv 0 \mod 5$ si et seulement si $2n + 1 \equiv 0 \mod 5$ c'est-à-dire $2n \equiv 4 \mod 5$. Comme $2 \wedge 5 = 1$ ceci est équivalent à $n \in 2 + 5\mathbb{Z}$.
(7) En développant on obtient $(2n + 1)^2 \equiv -P(n) \mod 5$ donc $\{n \in \mathbb{Z} | P(n) \equiv 0 \mod 5\} = 2 + 5\mathbb{Z}$ et $\{P(n) \in \mathbb{Z} | P(n) \equiv 0 \mod 5\} = \{P(2 + 5k) | k \in \mathbb{Z}\}$.