Université Paris Diderot
Master de Mathématiques

Arithmétique
Année 2010-11
L. Merel

EXAMEN du 25 mai 2011

Durée : 3 h

L'usage de tout appareil électronique et de tout document autre que des notes de cours est interdit.

Exercice 1

1. Montrer que le nombre 2011 est premier.
2. Quel est l'ordre du groupe $(\mathbf{Z}/2011\mathbf{Z})^*$? Combien ce groupe a-t-il de générateurs ?
3. Combien y a-t-il de carrés dans $(\mathbf{Z}/2011\mathbf{Z})^*$?
4. Le nombre 1000 est-il un carré modulo 2011 ?
5. Soit n et m des entiers ≥ 1. Montrer que n^m engendre $(\mathbf{Z}/2011\mathbf{Z})^*$ si et seulement si n engendre $(\mathbf{Z}/2011\mathbf{Z})^*$ et m est premier à 2010.
6. L'ensemble des nombres premiers dont le carré est congru à 1000 modulo 2011 est-il infini ? Si oui, en donner la densité.
7. L'ensemble des nombres premiers qui engendrent $(\mathbf{Z}/2011\mathbf{Z})^*$ est-il infini ? Si oui, en donner la densité.
8. L'ensemble des nombres premiers $p > 2$ tels que $p^{(p-1)/2}$ engendre $(\mathbf{Z}/2011\mathbf{Z})^*$ est-il infini ? Si oui, sa densité est-elle $> 10^{-7}$?

Exercice 2

Pour n entier ≥ 1, notons p_n le n-ème nombre premier. Soit α un nombre réel > 0.

1. Montrer que $p_n \sim n\log(n)$ lorsque n tend vers l'infini.
2. Posons, pour k entier ≥ 2, $n_k = [\alpha k/\log(k)]$ et $m_k = [k/\log(k)]$, où $[x]$ désigne la partie entière du nombre réel x. Montrer que $\log(n_k) \sim \log(k)$ lorsque k tend vers l'infini.
3. En déduire que $p_{n_k} \sim \alpha k$ lorsque k tend vers l'infini.
4. Montrer que la suite p_{n_k}/p_{m_k} tend vers α lorsque k tend vers l'infini.
5. En déduire que l'ensemble des nombres rationnels de la forme p/q, où p et q sont premiers, est dense dans l'intervalle réel $[0, +\infty[$.
6. Montrer que $\sum_{p\leq x} 1/p \sim \log(\log(x))$, lorsque x tend vers l'infini et où, dans la somme, p parcourt les nombres premiers $\leq x$.
7. En déduire que la limite de $\sum_{\sqrt{x}\leq p\leq x} 1/p$, lorsque x tend vers l'infini et où, dans la somme, p parcourt les nombres premiers compris entre $\sqrt{x}$ et x.

Exercice 3

Soit p un nombre premier. Posons $\mathbf{Z}_{(p)} = \{u/v \in \mathbf{Q}/u \in \mathbf{Z}, v \in \mathbf{Z} - p\mathbf{Z}\}$. C'est l'ensemble des *nombres p-entiers*.

0. Montrer que $\mathbf{Z}_{(p)} = \mathbf{Z}_p \cap \mathbf{Q}$, où $\mathbf{Z}_p$ est l'anneau des entiers p-adiques. En déduire que $\mathbf{Z}_{(p)}$ est un sous-anneau de $\mathbf{Q}$ (ou le montrer directement).

On dit que deux éléments a et b de $\mathbf{Z}_{(p)}$ sont *congrus modulo* p et on note $a \equiv b \pmod{p}$ si on a $a - b \in p\mathbf{Z}_{(p)}$. On dit qu'une série entière $\sum_{k=0}^{\infty} c_k X^k/k!$ avec $c_k \in \mathbf{Z}_{(p)}$ est *p-périodique* si on a $c_k \equiv c_{k'} \pmod{p}$ lorsque $k \equiv k' \pmod{p-1}$.

Pour k entier ≥ 0, on note B_k le k-ème nombre de Bernoulli. Ces nombres sont donnés par la série génératrice $X/(e^X - 1) = \sum_{k=0}^{\infty} B_k X^k/k!$, que l'on notera $F(X)$. Soit $a \in \{1, 2, ..., p-1\}$ un entier qui engendre $(\mathbf{Z}/p\mathbf{Z})^*$.

1. Soit r un entier ≥ 0. Montrer que la série $e^{rX} = \sum_{k=0}^{\infty} r^k X^k/k!$ est p-périodique.
2. Montrer qu'une combinaison linéaire à coefficients dans $\mathbf{Z}_{(p)}$ de séries p-périodiques est p-périodique.
3. Montrer que la série $(e^X - 1)^m$ est p-périodique lorsque m est un entier ≥ 0.
4. En déduire que la série $\sum_{m=0}^{\infty} c_m (e^X - 1)^m$ est p-périodique lorsque $(c_m)_{m \geq 0}$ est une suite de nombres p-entiers.
5. Posons $G(u) = a/((1+u)^a - 1) - 1/u = \sum_{m=0}^{\infty} g_m u^m$. Montrer que g_m est p-entier pour tout m entier ≥ 0.
6. Montrer que $F(aX) - F(X) = XG(u)$, où $u = e^X - 1$.
7. En déduire que $B_k(a^k - 1)/k$ est p-entier, puis que B_k/k est p-entier, pour k entier ≥ 1 non divisible par $p - 1$.
8. En déduire que $B_k(a^k - 1)/k \equiv B_{k'}(a^{k'} - 1)/k' \pmod{p}$ lorsque $k \equiv k' \pmod{p-1}$.
9. En déduire que si k et k' sont des entiers congrus modulo $p - 1$ et non divisibles par $p - 1$, on a $B_k/k \equiv B_{k'}/k' \pmod{p}$ (c'est la *congruence de Kummer*).
10. Dans cette question, on fait l'hypothèse plus générale suivante : pour r entier ≥ 1, on a la congruence $B_k(a^k - 1)/k \equiv B_{k'}(a^{k'} - 1)/k' \pmod{p^r}$ lorsque k et k' sont congrus modulo $p^{r-1}(p-1)$. Montrer qu'on a $(a^k - 1)\zeta(1-k) \equiv (a^{k'} - 1)\zeta(1-k')' \pmod{p^r}$ lorsque k et k' sont congrus modulo $p^{r-1}(p-1)$, où ζ est la fonction ζ de Riemann. En déduire que la fonction $k \mapsto (1 - p^{k-1})\zeta(1-k)$ se prolonge par continuité p-adique en une fonction $\mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z} \mapsto \mathbf{Z}_p$.