Licence de Mathématiques.
Université d'Artois. 2008-2009.

Examen session 1
Éléments de correction

Cours et application. 1)-2)a)b) Voir le cours.

c) Commençons par vérifier que 51 et 106 sont premiers entre eux. Nous pourrions voir que $51 = 17 \times 3$ or ni 3, ni 17 (premiers) ne divisent 106. Toutefois, nous allons appliquer Euclide pour chercher une relation de Bézout. En posant $a = 106$ et $b = 51$, on a $a = 2b + r$ avec $r = 4$. Puis $b = 12r + r'$ avec $r' = 3$. Enfin, $r = r' + 1$, ce qui permet déjà de conclure que a et b sont bien premiers entre eux. En remontant, on trouve $1 = r - (b - 12r) = -b + 13(a - 2b) = 13a - 27b$. On en déduit que dans $\mathbb{Z}/106\mathbb{Z}$, on a $\dot{1} = -\dot{27} \cdot \dot{51}$ donc l'inverse de $\dot{51}$ est $-\dot{27} = \dot{24}$.

Exercice 1.

1) Si $x_0 \in \mathbb{Z}$ est une solution particulière, alors pour toute solution $x \in \mathbb{Z}$, on a $x - x_0$ qui est congru à 0 à la fois modulo 3; 4 et 5. Autrement dit, 3; 4 et 5 divisent $x - x_0$. Comme 3; 4 et 5 sont premiers entre eux deux à deux, on obtient que $3 \times 4 \times 5$ divise $x - x_0$. Plus précisément: 3 et 4 sont premiers entre eux donc 3×4 divise $x - x_0$. Puis 12 et 5 sont premiers entre eux donc 12×5 divise $x - x_0$. On a bien 60 divise $x - x_0$. Donc $x = x_0 + 60k$ où $k \in \mathbb{Z}$.

Réciproquement, si $x = x_0 + 60k$ où $k \in \mathbb{Z}$, on voit immédiatement que x est solution du problème.

2) Dans $\mathbb{Z}/3\mathbb{Z}$, la classe de $20.b_1$ est la même que celle de $2.b_1$ et on voit immédiatement que $b_1 = 2$ convient. De même, $b_2 = -1$ convient ou encore (même classe) $b_2 = 3$. Enfin $b_3 = 3$ convient.

3) Dans $\mathbb{Z}/3\mathbb{Z}$, la classe de a est la même que celle de $20.b_1$ donc de 1. Dans $\mathbb{Z}/4\mathbb{Z}$, la classe de a est la même que celle de $-15b_2$ donc de -1. Dans $\mathbb{Z}/5\mathbb{Z}$, la classe de a est la même que celle de $24b_3$ donc de 2. Ainsi $a = 67$ est une solution particulière. On peut donc conclure que l'ensemble des solutions est

$$67 + 60\mathbb{Z} = \{67 + 60k |\ k \in \mathbb{Z}\} = \{7 + 60l |\ l \in \mathbb{Z}\}$$

Exercice 2.

1) Il s'agit d'une simple conséquence de la décomposition en nombres premiers: $n \geq 1$ s'écrit comme un produit de la forme $\prod q_j^{\alpha_j}$ où les q_j sont des nombres premiers distincts et les $\alpha_j \geq 1$. Il y a des α_j de deux types: ceux qui sont pairs et ceux qui sont impairs. De toute façon, $\alpha_j = 2\alpha'_j + r_j$ où $r_j \in \{0, 1\}$. Ainsi, en écrivant $a = \prod q_j^{\alpha'_j}$ et $b = \prod q_j^{r_j}$, on a bien $n = a^2 b$.

b) b n'est divisible par aucun carré de nombre premier par unicité de la décomposition en nombres premiers. En effet, sinon il existe un nombre premier, nécessairement de la forme q_i tel que q_i^2 divise n, mais alors q_i devrait intervenir avec une puissance au moins 2 dans la décomposition en nombres premiers de n.

L'écriture est unique: supposons que $a^2 b = a'^2 b'$ (avec la forme du 1.a.). On peut diviser par le pgcd de a et a', on a donc $a_1^2 b = a_1'^2 b'$ où a_1 et a'_1 sont premiers entre eux. Ainsi, a_1^2 et $a_1'^2$ sont aussi premiers entre eux. Comme de plus, $a_1'^2$ divise $a_1^2 b$, on a nécessairement $a_1'^2$ divise b. Si $a'_1 \geq 2$, il est divisible par un nombre premier donc le carré de ce nombre premier divise b et ceci contredit le point précédent. Ainsi $a'_1 = 1$, ou encore $a = a'$ (puisque leur pgcd leur est égal). On a alors aussi $b = b'$.

2) On a $a^2 \leq a^2 b \leq N$ donc $a \leq \sqrt{N}$. D'autre part, on sait déjà que b est un élément de $\left\{ \prod_{i=1}^{J} p_i^{\varepsilon_i} |\ \varepsilon_i \in \{0, 1\} \right\}$ pour un certain $J \geq 1$. Mais comme $n \in \mathcal{E}_j(N)$, pour tout $k > j$, p_k ne divise

pas n donc ne divise pas b, ainsi nécessairement $\varepsilon_k = 0$ pour tout $k > j$, donc b est un élément de $\left\{ \prod_{i=1}^{j} p_i^{\varepsilon_i} | \, \varepsilon_i \in \{0,1\} \right\}$.

3)a) F est bien définie par l'unicité de l'écriture $n = a^2 b$ (question 1.b.). Elle est injective car si $F(n) = F(m) = (a,b)$ alors n et m valent $a^2 b$ par définition, donc $n = m$.

b) Comme F est injective, le cardinal de $\mathcal{E}_j(N)$ est inférieur à celui de l'ensemble $\{1, \ldots, \sqrt{N}\} \times \left\{ \prod_{i=1}^{j} p_i^{\varepsilon_i} | \, \varepsilon_i \in \{0,1\} \right\}$. Or le cardinal d'un produit est le produit des cardinaux. Le cardinal de $\{1, \ldots, \sqrt{N}\}$ es trivialement $\sqrt{N}$. Le cardinal de $\left\{ \prod_{i=1}^{j} p_i^{\varepsilon_i} | \, \varepsilon_i \in \{0,1\} \right\}$ est celui de $\{(\varepsilon_1, \ldots, \varepsilon_j) | \, \varepsilon_i \in \{0,1\}\} = \{0,1\}^j$ d'après l'unicité de la décomposition en nombres premiers. Cela vaut donc $\Big(card\{0,1\}\Big)^j = 2^j$. D'où le résultat.

4)a) $\mathcal{E}_j(N) = \bigcap_{k>j} \{1 \leq n \leq N | \, p_k \text{ ne divise pas } n\}$.

Le complémentaire de l'intersection est la réunion des complémentaires. D'où le résultat par passage au complémentaire.

b) L'entier j_N qui est le plus grand indice J tel que p_J intervienne dans l'écriture des entiers de $\{1, \ldots, N\}$ convient. En fait l'ensemble de ces indices J est non vide majoré et on est sûr que $j_N < N$ (car $p_k > k$).

5) Le cardinal du complémentaire de $\mathcal{E}_j(N)$ dans $\{1, \ldots, N\}$ vaut $N - C_j(N)$. On déduit de 4. que c'est aussi le cardinal de $\bigcup_{j<k<j_N} \{1 \leq n \leq N | \, p_k \, divise \, n\}$ qui est inférieur à

$$\sum_{j<k<j_N} card\{1 \leq n \leq N | \, p_k \, divise \, n\}$$

Or $card\{1 \leq n \leq N | \, p_k \, divise \, n\}$ est le quotient de la division de N par p_k et est donc inférieur à $\dfrac{N}{p_k}\cdot$ D'où le résultat.

6) D'après le critère de Cauchy (puisqu'on a supposé que $\sum \frac{1}{p_k}$ converge), on a pour tout $\varepsilon > 0$, il existe $N_0 \geq 1$ tel que pour tous $j' \geq j \geq N_0$

$$\sum_{k=j+1}^{j'} \frac{1}{p_k} \leq \varepsilon$$

Ceci signifie exactement que $\lim_{j \to \infty} \sup_{j'>j} \sum_{k=j+1}^{j'} \dfrac{1}{p_k} = 0$.

7) Nous avons supposé que $\sum \dfrac{1}{p_k}$ converge. D'après 6., il existe $j \geq 1$ (qui restera fixé jusqu'à la fin du raisonnement) tel que $\sup_{j'>j} \sum_{k=j+1}^{j'} \dfrac{1}{p_k} \leq \dfrac{1}{2}$ (en fait n'importe quel nombre strictement inférieur à 1 aurait fait l'affaire). Pour tout entier $N \geq 2$, on a avec les notations précédentes (cf 5.):

$$N - C_j(N) \leq \frac{N}{2}\cdot$$

En même temps, $C_j(N) \leq 2^j \sqrt{N}$ (cf 3.b.) donc $N - 2^j \sqrt{N} \leq \dfrac{N}{2}$ donc

$$N \leq 4^{j+1}$$

ce qui est faux puisque N peut être arbitrairement grand. Par l'absurde, la preuve est achevée.