Université Paris 7-Denis Diderot — MT-282
D.E.U.G.- S.M. — Année 1999-00

Corrigé de l'EXAMEN du 20 janvier 2000

Exercice 1

1. On a $5^4.2^{28}-1 = (5.2^7)^4-1 = ((5.2^7)^2-1)((5.2^7)^2+1) = (5.2^7-1)(5.2^7+1)((5.2^7)^2+1)$ et $5^4.2^{28}+2^{32} = 2^{28}(5^4+2^4)$. Cela établit les relations de divisibilité cherchées. Comme $5.2^7+1 = 641 = 5^4+2^4$, 641 divise $5^4.2^{28}+2^{32}-(5^4.2^{28}-1) = 2^{32}+1$.
2. Pour $n=5$, on a $2^{2^n}+1 = 2^{32}+1$ qui est divisible par 641. Or $2^{32}+1 > 641$, si bien que $2^{32}+1$ n'est pas un nombre premier.
3. Comme $2^{32}+1 \equiv 0 \bmod 641$, on a $2^{64} \equiv (2^{32})^2 \equiv (-1)^2 \equiv 1 \bmod 641$. L'ordre de $\bar{2}$ divise donc 64. Or 64 possède un unique diviseur maximal : c'est 32. On a $\bar{2}^{32} = -\bar{1} \neq \bar{1}$ dans $(\mathbf{Z}/641\mathbf{Z})^*$. L'ordre de $\bar{2}$ est donc 64.
4. Le nombre 641 est premier, en effet il n'est pas divisible par 2, 3, 5, 7, 11, 13, 17, 19 et 23, c'est-à-dire par les nombres premiers $< \sqrt{641}$. Le groupe $(\mathbf{Z}/641\mathbf{Z})^*$ est donc cyclique.
5. Le groupe $(\mathbf{Z}/641\mathbf{Z})^*$ est cyclique d'ordre $641-1 = 640$. Soit g un générateur de ce groupe. Il existe un entier n tel que $g^n = \bar{2}$. L'ordre de g^n est $640/\mathrm{PGCD}(n,640)$ et l'ordre de 2 est 32. On a donc $32 = 640/\mathrm{PGCD}(n,640)$, c'est-à-dire $\mathrm{PGCD}(n,640) = 20$ et donc $20|n$ et donc $5|n$. On a donc $\bar{2} = (g^{n/5})^5$.

Exercice 2

1. Écrivons la décomposition de m en produit de facteurs premiers : $m = \prod_p p^{e_p}$. Posons $m' = l^{e_l}$ et $m" = m/m' = \prod_{p \neq l} p^{e_p}$. Ces nombres satisfont les conditions demandées puisque l ne divise pas $m"$. Comme m' est nécessairement la plus grande puissance de l divisant m et comme $m" = m/m'$, le couple $(m', m")$ est unique.

Puisque $m"$ est premier à l, il est premier à toute puissance de l et donc à m'. C'est pourquoi on peut appliquer le théorème de Bézout pour établir l'existence de a et b.
2. L'ordre de $x^{am'}$ est égal à $m/\mathrm{PGCD}(m, am')$. Or, puisque $m'|m$, on a $\mathrm{PGCD}(m, am') = m'\mathrm{PGCD}(m/m', a) = m'\mathrm{PGCD}(m", a)$. Comme on a l'identité $am' + bm" = 1$, $m"$ et a sont premiers entre eux, *i.e.* on a $\mathrm{PGCD}(m", a) = 1$. L'ordre de $x^{am'}$ est donc $m/m' = m"$. De même on trouve que l'ordre de $x^{bm"}$ est m'.

3. Posons $x' = x^{bm"}$ et $x" = x^{am'}$. Ces éléments ont les ordres demandés. On a $x'x" = x^{bm"}x^{am'} = x^{am'+bm"} = x^1 = x$ et on a de même $x"x' = x$.

4. On a $y'x = y'y'y" = y'y"y' = xy'$ et $y"x = y"y"y' = y"y'y" = xy"$.

5. On a, en utilisant que x et y' commutent et que $x' = x^{bm"}$, $x'y' = x^{bm"}y' = y'x^{bm"} = y'x'$. On montre de même que $x"y" = y"x"$.

La relation $x'y' = y'x'$ équivaut à $y'^{-1}x' = x'y'^{-1}$. Considérons le produit t' des ordres de x' et y'. C'est une puissance de l. On a, puisque x' et y'^{-1} commutent, $(x'y'^{-1})^{t'} = x'^{t'}y'^{-t'}$. Or les ordres de x' et y' divisent t'. On a donc $x'^{t'} = 1$ et $y'^{-t'} = 1$. L'ordre de $x'y'^{-1}$ divise t' ; c'est donc une puissance de l.

On démontre que façon analogue que $x"^{-1}y"$ est d'ordre premier à l : notons $t"$ le produit des ordres de $x"$ et $y"$; il est premier à l. On a $(x"^{-1}y")^{t"} = 1$. L'ordre de $x"^{-1}y"$ divise $t"$ et est donc premier à l.

6. On a $x = x"x' = y"y'$. On a donc $x"x'y'^{-1} = y"$, ou encore $x'y'^{-1} = x"^{-1}y"$. Les ordres de $x'y'^{-1}$ et de $x"^{-1}y"$ sont donc égaux. Le premier est une puissance de l, le second est premier à l. La seule puissance de l qui est un nombre premier à l est 1. On a donc $x'y'^{-1} = x"^{-1}y = 1$ et donc $x' = y'$ et $x" = y"$.

7. Comme $\bar{2}$ est d'ordre $96/\mathrm{PGCD}(2,96) = 48 = m = 2^4.3$, On a $m' = 2^4 = 16$ et $m" = 3$. On a $16 - 3.5 = 1$, *i.e.* $a = 1$ et $b = -3$. On a $x' = (-5).\bar{2} = -\overline{10} = \overline{86}$ et $x" = 16.\bar{2} = \overline{32}$.

Exercice 3

1. Vérifions que c'est un sous-anneau de $\mathbf{Q}$. Voyons d'abord que $(\mathbf{Z}_{(p)}, +)$ est un sous-groupe de $(\mathbf{Q}, +)$. On a $0 \in \mathbf{Z}_{(p)} \neq \emptyset$. Soient u/v, $u'/v' \in \mathbf{Z}_{(p)}$. On a $u/v + u'/v' = (uv' + u'v)/vv'$. Comme $p \not| v$ et $p \not| v'$ et comme p est premier, on a $p \not| vv'$. On a donc $u/v + u'/v' \in \mathbf{Z}_{(p)}$ (stabilité par l'addition). On a $-u/v \in \mathbf{Z}_{(p)}$ et $u/v + (-u/v) = 0$; tout élément de $\mathbf{Z}_{(p)}$ admet un inverse. Cela prouve que $(\mathbf{Z}_{(p)}, +)$ est un groupe.

Pour vérifier que $\mathbf{Z}_{(p)}$ est un anneau, observons d'abord que $1 = 1/1 \in \mathbf{Z}_{(p)}$. De plus on a $(u/v)(u'/v') = uu'/vv'$, comme on l'a observé plus haut, vv' n'est pas divisible par p lorsque $p \not| v$ et $p \not| v'$. L'ensemble $\mathbf{Z}_{(p)}$ est donc stable pour la multiplication. Cela prouve que $\mathbf{Z}_{(p)}$ est un anneau.

2. Les éléments inversibles de $\mathbf{Z}_{(p)}$ sont les éléments u/v tels que $(u/v)^{-1} = v/u \in \mathbf{Z}_{(p)}$. C'est-à-dire tels que $p \not| u$.

Le groupe $\mathbf{Z}_{(p)}^*$ est contenu dans $\mathbf{Q}^*$. Soit $x \in \mathbf{Q}$ vérifiant $x^3 = 1$. On a alors $x = 1$. Or 1 est d'ordre 1 dans $\mathbf{Z}_{(p)}^*$. Il n'y a donc pas d'élément d'ordre 3 dans $\mathbf{Z}_{(p)}^*$.

Soit $a > 1$ un nombre entier premier à p. On a $a = a/1 \in \mathbf{Z}_{(p)}^*$. Ce n'est pas un élément d'ordre fini puisqu'on a $a^n \neq 1$ pour tout entier $n > 0$. Il y a donc bien des éléments d'ordre infini dans $\mathbf{Z}_{(p)}^*$.

3. Vérifions qu'on a affaire à un sous-groupe. On a $0 = 0/1 \in p\mathbf{Z}_{(p)}$. Soient u/v et $u'/v' \in p\mathbf{Z}_{(p)}$. On a $u/v + u'/v' = (uv' + u'v)/vv'$. Comme $p|u$ et $p|u'$, on a $p|(uv' + u'v)$ et donc $u/v + u'/v \in p\mathbf{Z}_{(p)}$. On a $-(u/v) \in p\mathbf{Z}_{(p)}$, car $p|u$ entraîne $p|(-u)$. Cela prouve que $p\mathbf{Z}_{(p)}$ est un groupe. Il est distingué puisque $\mathbf{Z}_{(p)}$ est un groupe commutatif.

4. Cette application est bien définie, puisque lorsque $u/v \in \mathbf{Z}_{(p)}$, on a $p \not| v$, si bien que v est inversible modulo p et qu'il est légitime de considérer $(\bar{v})^{-1}$.

Vérifions qu'on a un homomorphisme d'anneaux. On a $\phi(u/v + u'/v') = \phi((uv' + u'v)/vv') = \overline{(uv' + u'v)}(\overline{vv'})^{-1} = (\bar{u}\bar{v}' + \bar{u}'\bar{v})/\bar{v}\bar{v}' = \bar{u}/\bar{v} + \bar{u}'/\bar{v}' = \phi(u/v) + \phi(u'/v')$. On a $\phi(1) = \phi(1/1) = \bar{1}/\bar{1} = \bar{1}$. On a $\phi(u/v.u'/v') = \overline{uu'}(\overline{vv'})^{-1} = \bar{u}\bar{u}'/\bar{v}\bar{v}' = \phi(u/v)\phi(u'/v')$.

Soit $u/v \in \mathbf{Z}_{(p)}$. C'est un élément du noyau de ϕ si et seulement si $\phi(u/v) = \bar{0}$, c'est-à-dire si et seulement si $\bar{u}(\bar{v})^{-1} = \bar{0}$. Comme $(\bar{v})^{-1}$ est inversible, cela revient à dire que $\bar{u} = \bar{0}$, c'est-à-dire $u \in p\mathbf{Z}$, ou encore $u/v \in p\mathbf{Z}_{(p)}$. Le noyau de ϕ est donc $p\mathbf{Z}_{(p)}$.

Soit $\alpha \in (\mathbf{Z}/p\mathbf{Z})$, qui est la classe d'un entier $a \in \mathbf{Z}$. On a $\phi(a) = \phi(a/1) = \bar{a} = \alpha$. Tout élément de $(\mathbf{Z}/p\mathbf{Z})$ admet un antécédent par ϕ, qui est donc une application surjective.

5. L'application ϕ est un homorphisme de groupes qui est surjectif et a pour noyau $p\mathbf{Z}_{(p)}$. On a donc un isomorphisme de groupes entre $\mathbf{Z}_{(p)}/p\mathbf{Z}_{(p)}$ et l'image de ϕ qui est $(\mathbf{Z}/p\mathbf{Z})$.