Université Pierre et Marie Curie 2006–2007

LM220 Maths-Info groupes 1, 2 et 5

Corrigé du devoir maison n° 1

1 Préliminaires

1.1 Soit r un entier > 0. On considère la proposition de récurrence suivante :

« Pour tout entier $n \geqslant 0$ s'écrivant sous la forme $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où les p_i sont des nombres premiers distincts et les α_i des entiers $\geqslant 1$, on a un isomorphisme de groupes

$$(\mathbf{Z}/n\mathbf{Z})^\times \approx \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \text{ . »}$$

Pour $r = 2$, c'est une conséquence du théorème chinois (cf. remarque 24 p.67 de votre cours). Supposons la proposition de récurrence vérifiée pour un entier $r \geqslant 2$. On considère $n = p_1^{\alpha_1} \cdots p_{r+1}^{\alpha_{r+1}}$ un entier naturel décomposé en un produit de $r + 1$ puissances de nombres premiers distincts. On écrit $n = mp_{r+1}^{\alpha_{r+1}}$ où $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. On a alors

$$(\mathbf{Z}/n\mathbf{Z})^\times \approx (\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/p_{r+1}^{\alpha_{r+1}}\mathbf{Z})^\times$$

d'après le théorème chinois (m et $p_{r+1}^{\alpha_{r+1}}$ sont premiers entre eux). Or d'après l'hypothèse de récurrence, on a

$$(\mathbf{Z}/m\mathbf{Z})^\times \approx \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \ .$$

On en déduit immédiatement l'isomorphisme

$$(\mathbf{Z}/n\mathbf{Z})^\times \approx \prod_{i=1}^{r+1} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \ .$$

D'où la proposition par récurrence.

1.2 Le groupe G étant abélien, on a $(xy)^{ab} = x^a y^b = 1$. On en déduit que l'ordre de xy divise ab. Réciproquement, si $d \geqslant 1$ est un entier tel que $(xy)^d = 1$, alors, en élevant cette égalité à la puissance a, on obtient $y^{ad} = 1$. On en déduit que b divise ad. Comme par ailleurs les entiers a et b sont premiers entre eux, b divise d (lemme de Gauss). De même, a divise d. En utilisant à nouveau le fait que a et b sont premiers entre eux, il vient que ab divise d. D'où le fait que l'ordre de xy est ab.

2 Le cas $p \neq 2$

2.1 On a $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. On en déduit que le groupe $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ est d'ordre $p^{\alpha-1}(p-1)$. L'entier $1+p$ est premier avec p^α. Il est donc inversible dans $\mathbf{Z}/p^\alpha\mathbf{Z}$.

2.2 Soit i un entier compris entre 1 et $p-1$. On a l'égalité

$$iC_i^p = pC_{p-1}^{i-1}.$$

Les entiers p et i étant premiers entre eux, on en déduit que p divise C_p^i.

Si $i \geqslant 3$, il est clair que p^3 divise $C_p^i p^i$. Et, si $i = 2$, comme p divise C_p^i on a encore $C_p^i p^i$ divisible par p^3.

2.3 On écrit

$$(1+p)^p = \sum_{i=0}^{p} C_p^i p^i = 1 + p^2 + \sum_{i=2}^{p} C_p^i p^i.$$

Dans la seconde somme ci-dessus, tous les termes sont divisibles par p^3 d'après la question précédente. On écrit

$$\sum_{i=2}^{p} C_p^i p^i = up^3, \quad \text{avec } u \in \mathbf{N}^*.$$

On en déduit l'égalité demandée

$$(1+p)^p = 1 + p^2(1+up).$$

2.4 On considère, pour k entier $\geqslant 1$, la proposition de récurrence suivante.

« Il existe λ_k, premier à p, tel que

$$(1+p)^{p^k} = 1 + \lambda_k p^{k+1} \text{ ».} \tag{1}$$

Pour $k = 1$, c'est le résultat de la question précédente. Supposons donc la proposition vérifiée pour $k \geqslant 1$. On a alors

$$\begin{aligned}(1+p)^{p^{k+1}} &= \left((1+p)^{p^k}\right)^p \\ &= (1+\lambda_k p^{k+1})^p \quad \text{d'après l'hypothèse de récurrence} \\ &= 1 + \lambda_k p^{k+2} + \sum_{i=2}^{p} C_p^i \lambda_k^i (p^{k+1})^i.\end{aligned}$$

Et, comme à la question 2.3, on montre que p^{k+3} divise $C_p^i(p^{k+1})^i$ dès que $i \geqslant 2$. On pose alors $\sum_{i=2}^{p} C_p^i \lambda_k^i (p^{k+1})^i = p^{k+3}u$. On en déuit l'égalité

$$(1+p)^{p^{k+1}} = 1 + (\lambda_k + up)p^{k+2}.$$

Les entiers λ_k et p étant premiers entre eux par hypothèse de récurrence, on a le résultat en posant $\lambda_{k+1} = \lambda_k + up$.

2.5 L'égalité (1) appliquée à $k = \alpha - 1$ fournit la congruence $(1+p)^{p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}$. On en déduit que l'ordre de $1+p$ dans le groupe multiplicatif $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ est un diviseur de $p^{\alpha-1}$. Or, toujours d'après (1), $(1+p)^{p^{\alpha-2}} = 1 + \lambda p^{\alpha-1}$ avec λ et p premiers entre eux. D'où $(1+p)^{p^{\alpha-2}} \not\equiv 1 \pmod{p^\alpha}$ et le fait que $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$.

2.6 Le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'après le rappel fait au début de l'énoncé. Autrement dit, il contient un élément d'ordre $p-1$. L'application π étant surjective (on l'a admis car c'est évident), cet élément s'écrit $\pi(x)$ pour un certain x dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$.

2.7 Soit d l'ordre de x. D'après les propriétés des morphismes de groupes, on a

$$1 = \pi(x^d) = \pi(x)^d.$$

Or $\pi(x)$ est d'ordre $p-1$ donc $p-1$ divise d. On écrit $d = (p-1)k$. L'élément x^k est alors d'ordre exactement $p-1$.

2.8 Les éléments $y = x^k$ et $(1+p)$ du groupe $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ sont d'ordres respectifs $p-1$ et $p^{\alpha-1}$, donc d'après la question 1.2, l'élément $y(1+p)$ est d'ordre $p^{\alpha-1}(p-1)$. Or le groupe $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ est d'ordre $p^{\alpha-1}(p-1)$ d'après la question 2.1. On en déduit qu'il est cyclique (engendré par $y(1+p)$).

3 Le cas $p = 2$

3.1 On a $(\mathbf{Z}/2\mathbf{Z})^\times = \{1\}$ et $(\mathbf{Z}/4\mathbf{Z})^\times = \{1, 3\} = \langle 3 \rangle$. Ces deux groupes sont donc cycliques.

3.2 L'ordre de $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ est $\varphi(2^\alpha) = 2^{\alpha-1}$.

3.3 On considère, pour k entier $\geqslant 1$, la proposition de récurrence suivante.

« Il existe λ_k impair tel que $5^{2^k} = 1 + \lambda_k 2^{k+2}$ ».

Pour $k = 1$, c'est simplement l'égalité $25 = 1 + 3 \cdot 8$. Supposons la proposition de récurrence vérifiée pour k entier $\geqslant 1$. On a

$$\begin{aligned} 5^{2^{k+1}} = (5^{2^k})^2 &= (1 + \lambda_k 2^{k+2})^2 \quad \text{par hypothèse de récurrence} \\ &= 1 + 2^{k+3}(\lambda_k + \lambda_k^2 2^{k+1}). \end{aligned}$$

D'où le résultat en posant $\lambda_{k+1} = \lambda_k + \lambda_k^2 2^{k+1}$.

3.4 On a $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ d'après la question précédente. On en déduit que 5 est d'ordre divisant $2^{\alpha-2}$. Par ailleurs, $5^{2^{\alpha-3}} = 1 + \lambda_{\alpha-3} 2^{\alpha-1} \not\equiv 1 \pmod{2^\alpha}$ ($\lambda_{\alpha-3}$ est impair). On en déduit comme à la question 2.5 que 5 est d'ordre $2^{\alpha-2}$.

3.5 Soient (ε, a) et (ε', a') dans $\mu_2 \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$. Alors

$$f(\varepsilon, a) f(\varepsilon', a') = (\varepsilon \cdot 5^a)(\varepsilon' \cdot 5^{a'}) = \varepsilon\varepsilon' \cdot 5^{a+a'} = f((\varepsilon, a) \cdot (\varepsilon', a')).$$

L'application f est donc un morphisme de groupes.

3.6 Soit $a \in \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$. On suppose que $5^a = 1$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$. Or 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ d'après la question 3.4. On en déduit que $a = 0$ dans $\mathbf{Z}/2^{\alpha-2}\mathbf{Z}$. La réciproque est évidente.

Soit $a \in \mathbf{Z}$ tel que $5^a \equiv -1 \pmod{2^\alpha}$. Alors, il existe k dans $\mathbf{Z}$ tel que

$$5^a = 2^\alpha k - 1.$$

Or $\alpha \geqslant 3$ par hypothèse. En réduisant modulo 4 l'égalité ci-dessus, on obtient alors $1 \equiv -1 \pmod 4$ ce qui est bien sûr absurde. On en déduit que la congruence $5^a \equiv -1 \pmod{2^\alpha}$ n'a jamais lieu.

3.7 Montrons que f est injective. On choisit un élément (ε, a) de $\ker(f)$. On a alors $f(\varepsilon, a) = \varepsilon \cdot 5^a = 1$. Or $\varepsilon = 1$ ou -1. Donc $5^a = 1$ ou $5^a = -1$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$. La seconde égalité n'ayant jamais lieu d'après la question précédente, on a donc $5^a = 1$ et $a = 0$ dans $\mathbf{Z}/2^{\alpha-2}\mathbf{Z}$. Autrement dit, $\ker(f) = \{(1, 0)\}$.

3.8 L'application f étant injective entre deux ensembles de même cardinal fini, elle est bijective. En particulier, tout élément de $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ s'écrit de manière unique sous la forme $\varepsilon \cdot 5^a$ avec $\varepsilon \in \mu_2$ et $a \in \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$. Un tel élément étant d'ordre divisant l'ordre de 5 c'est le résultat voulu.

On en déduit, avec la question 3.2, que le groupe multiplicatif $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ n'est pas cyclique.

4 Conclusion

4.1 Supposons que les entiers a et b ne sont pas premiers entre eux. Si m désigne leur ppcm, alors pour tout couple $(x, y) \in \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$, on a $m \cdot (x, y) = (mx, my) = (0, 0)$. En particulier, l'ordre de élément (x, y) divise m. Or $m < ab$ car a et b ne sont pas premiers entre eux. On en déduit qu'il n'existe pas d'élément d'ordre ab dans $\mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$. Ce groupe n'est donc pas cyclique.

4.2 D'après les questions 2.8 et 3.1, si $n = 2$, 4, p^α ou $2p^\alpha$, (p premier, $\alpha \geqslant 2$), alors le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique.

Réciproquement, si $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique, alors n ne peut avoir deux facteurs premiers impairs distincts. En effet, si $p \neq q$ sont deux nombres premiers impairs distincts divisant n, alors (pour α et β deux entiers $\geqslant 1$), le groupe produit

$$(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \times (\mathbf{Z}/q^\beta\mathbf{Z})^\times$$

n'est pas cyclique d'après la question précédente (2 divise $\varphi(p^\alpha)$ et $\varphi(q^\beta)$).

Si n est impair, on en déduit que $n = p^\alpha$ (pour un p premier et $\alpha \geqslant 1$).

Si n est pair. Alors, soit $n = 2$ ou 4, soit n s'écrit sous la forme $2^\gamma p^\alpha$ (pour un p premier et $\alpha, \gamma \geqslant 1$). Or si $\gamma > 2$, le groupe $(\mathbf{Z}/2^\gamma\mathbf{Z})^\times$ n'est pas cyclique (question 4.1). On a donc $\gamma \leqslant 2$. Or le groupe produit

$$(\mathbf{Z}/4\mathbf{Z})^\times \times (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$$

n'est pas cyclique d'après la question précédente. On en déduit que $\gamma = 1$. D'où le résultat.