Université Paris 7
U.F.R. de Mathématiques
B. Keller

Un corrigé de l'examen du 01.02.95

1) Soit x le nombre de dents dont il faut faire avancer la grande roue. D'après les informations fournies, nous avons

$$\begin{aligned} x &\equiv 1 \ (25) \\ x &\equiv 1 \ (8) \\ x &\equiv 2 \ (9). \end{aligned}$$

Les nombres $25, 8, 9$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution x dont la classe modulo $25 \times 8 \times 9 = 1800$ est unique. Pour trouver x, nous déterminons d'abord x_1, x_2, x_3 dont les classes sont les images réciproques de $(1,0,0), (0,1,0), (0,0,1)$ par la projection

$$\mathbf{Z}/1800 \xrightarrow{\sim} \mathbf{Z}/25 \oplus \mathbf{Z}/8 \oplus \mathbf{Z}/9.$$

Nous avons

$$\begin{array}{llll} 72\,u_1 + 25\,v_1 = 1; & \text{sol. part.} & 72 \times 8 + 25 \times (-23) = 1. & \text{Posons} \quad x_1 = 576. \\ 225\,u_2 + 8\,v_2 = 1; & \text{sol. part.} & 225 \times 1 + 8 \times (-28) = 1. & \text{Posons} \quad x_2 = 225. \\ 200\,u_3 + 9\,v_3 = 1; & \text{sol. part.} & 200 \times (-4) + 9 \times 89 = 1 & \text{Posons} \quad x_3 = -800. \end{array}$$

Nous avons donc $x \equiv 1 \times 576 + 1 \times 225 - 2 \times 800 \equiv -799 \equiv 1001 \ (1800)$. **Il faut faire avancer la grande roue de** 1001 **dents.**

2) Nous avons $14 = 2 \times 7$, $12 = 3 \times 4$ et $72 = 8 \times 9$. Trois applications du théorème chinois donnent donc un isomorphisme entre A et

$$D = \mathbf{Z}/2 \oplus \mathbf{Z}/4 \oplus \mathbf{Z}/8 \oplus \mathbf{Z}/3 \oplus \mathbf{Z}/7 \oplus \mathbf{Z}/9.$$

De même, les factorisations $6 = 2 \times 3$, $28 = 4 \times 7$ et $72 = 8 \times 9$ permettent de conclure que $B \cong D$; et les factorisations $6 = 2 \times 3$, $36 = 4 \times 9$, $56 = 7 \times 8$ montrent que $C \cong D$. Donc **les groupes** A**,** B **et** C **sont isomorphes deux à deux.**

3) Notons P l'ensemble des produits hk, où $h \in H$ et $k \in K$.

L'élément neutre e de G appartient à K et H. Donc $e = ee$ appartient aussi à P.

Supposons maintenant que h_1k_1 et h_2k_2 sont deux éléments de P (où $h_1, h_2 \in H$ et $k_1, k_2 \in K$). Nous avons

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})(k_1k_2).$$

Puisque H est distingué, nous avons $k_1h_2k_1^{-1} \in H$. Donc nous avons $h_1(k_1h_2k_1^{-1}) \in H$, $k_1k_2 \in K$, et $(h_1k_1)(h_2k_2)$ appartient bien à P.

Finalement, supposons que $hk \in P$, $h \in H$, $k \in K$. Alors

$$(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1}.$$

Puisque H est distingué, $k^{-1}h^{-1}k$ appartient encore à H. Ainsi $(hk)^{-1}$ appartient à P.

On en conclut que P est un sous-groupe de G.

4) Il s'agit de montrer que G contient un élément d'ordre n. Pour tout diviseur d de n soit $c(d)$ le nombre d'éléments d'ordre d dans G. Nous avons

$$n = |G| = \sum_{d|n} c(d)$$

et donc

$$c(n) = n - \sum_{d|n, d<n} c(d) \geq n - \sum_{d|n, d<n} \varphi(d)$$

car $c(d) \leq \varphi(d)$ pour tout $d|n, d < n$ d'après l'hypothèse. Or, on sait que

$$n = \sum_{d|n} \varphi(d).$$

Donc $c(n) \geq \varphi(n) \geq 1$. Ainsi G contient au moins un élément d'ordre n.

5) a) On a $10^n \equiv (-1)^n \ (11)$ pour tout $n \in \mathbf{Z}$. Donc

$$a = 123456789012345 \equiv (5-4)+(3-2)+(1-0)+(9-8)+(7-6)+(5-4)+(3-2)+1 \equiv 8 \ (11)$$

et $r = 8$.

b) Nous avons $a \equiv -2 \ (7)$ et $a^6 \equiv 1 \ (7)$. Comme $2000 \equiv 2 \ (6)$, il s'ensuit que $a^{2000} \equiv a^2 \equiv 4 \ (7)$. Donc $r = 4$.

c) Le nombre $p = 101$ est premier. D'après le petit théorème de Fermat, nous avons donc $a^p \equiv a \ (p)$. Ainsi $53^{101} \equiv 53 \ (101)$ et $r = 53$.

d) Soit $n \in \mathbf{N}$. D'après le théorème d'Euler, nous avons

$$5^{\varphi(2^n)} \equiv 1 \ (2^n).$$

Or $\varphi(2^n) = 2^{n-1}$. En posant $n = 10$ nous trouvons $r = 1$.

e) Soit p un nombre premier. On sait que $p+1$ est d'ordre p^{n-1} dans $(\mathbf{Z}/p^n\mathbf{Z})^*$ pour tout $n \in \mathbf{N}$. En particulier, $p+1$ est d'ordre p dans $\mathbf{Z}/p^2\mathbf{Z}$. Donc $(p+1)^{(p+1)} \equiv p+1 \ (p^2)$. En posant $p = 23$ nous trouvons $r = 24$.

f) Le nombre 17 est premier. D'après le petit théorème de Fermat, il suffit de connaître la classe de 5^9 modulo $17 - 1 = 16$ pour calculer 3^{5^9}. Or 5 est d'ordre 2^{n-2} dans $(\mathbf{Z}/2^n\mathbf{Z})^*$ pour tout $n \geq 2$. Donc $5^4 \equiv 1 \ (16)$ et $5^9 \equiv 5 \ (16)$. Ainsi

$$3^{5^9} \equiv 3^5 \equiv 27 \times 9 \equiv 5 \ (17)$$

et $r = 5$.

6) a) Le nombre 4 divise $52 = 53 - 1$. L'équation $x^4 = 1$ admet donc 4 solutions distinctes, puissances d'une solution primitive. Comme 2 engendre $(\mathbf{Z}/53\mathbf{Z})^*$ (table des indices), une solution primitive est 2^{13}. Comme $2^{10} \equiv 17 \ (53)$ (table des indices), nous avons $2^{13} \equiv 17 \times 8 \equiv 30 \ (53)$. Donc **l'ensemble des solutions est** $\{1, 30, -1, -30\}$ **dans** $\mathbf{Z}/53\mathbf{Z}$.

b) L'équation $x^3 \equiv 11 \ (53)$ est équivalente à $3 \times \mathrm{ind}_2(x) = \mathrm{ind}_2(11)$ dans $\mathbf{Z}/52$. Or $\mathrm{ind}_2(11) = 6$, d'après la table des indices. Comme 3 est inversible dans $\mathbf{Z}/52\mathbf{Z}$, il s'ensuit que $\mathrm{ind}_2(x) = 2$ et donc que $x = 4$ est l'unique solution dans $\mathbf{Z}/53\mathbf{Z}$.

7) a) On a $13 \equiv 1 \ (12)$ et donc $13^{13} \equiv 1^{13} \equiv 1 \ (12)$. Donc $13^{13} - 1 \equiv 0 \ (12)$ ce qui signifie que 12 divise $M = 13^{13} - 1$.

b) Soit p un diviseur premier de M qui ne divise pas 12. On a donc $13^{13} \equiv 1 \ (p)$ mais $13^1 \not\equiv 1 \ (p)$. Donc 13 est d'ordre 13 dans $(\mathbf{Z}/p\mathbf{Z})^*$. D'après le théorème de Lagrange, il s'ensuit que 13 divise $p - 1$. Donc $p - 1 = k \times 13$ pour un $k \in \mathbf{Z}$. Comme p est impair, $p - 1$ est pair et k doit être pair. Donc on a même $p \equiv 1 \ (26)$.

c) D'après a), M est divisible par 2 et 3. D'après c), les autres diviseurs premiers p inférieurs à 100 de M se trouvent parmi les nombres 27, 53 et 79. Or 27 n'est pas premier. Montrons que 53 divise M. En effet, nous avons $13 \equiv 2^{24} \ (53)$ d'après la table des indices, et donc $13^{13} \equiv 2^{13 \times 24} \equiv 1 \ (53)$ car, d'après le petit théorème de Fermat, $2^{52} \equiv 1 \ (53)$. Donc 53 divise M.

Montrons que 79 ne divise pas M. En effet, nous avons $13 \equiv 3^{34}$ (79) d'après la table des indices). Donc $13^{13} \equiv 13^{13\times 34}$ (79). Or $13 \times 34 = 2 \times 13 \times 17$ n'est pas divisible par $78 = 2 \times 3 \times 13$, qui est l'ordre de 3 dans $(\mathbf{Z}/79\mathbf{Z})^*$. Donc $13^{13} \not\equiv 1$ (79) et 79 ne divise pas M.

Les seuls diviseurs premiers de M inférieurs à 100 sont donc 2, 3 et 53.

8) a) Nous avons $\alpha = 2 \times (-1+8i)$ et $2 = (-i) \times (1+i)^2$. Il s'agit de décomposer $\beta = -1+8i$. La norme de β est égale à $65 = 5 \times 13$. Donc l'un des deux diviseurs premiers de 5, à savoir $1+2i$ ou $1-2i$, doit diviser β. Nous avons

$$\frac{-1+8i}{1+2i} = \frac{(-1+8i)(1-2i)}{5} = \frac{15+10i}{5} = 3+2i.$$

Donc $1+2i$ divise β. Le quotient $3+2i$ est premier, car sa norme $N(3+2i) = 13$ est un nombre premier de $\mathbf{Z}$. Ainsi la décomposition recherchée est

$$\alpha = (-i) \times (1+i)^2 \times (1+2i) \times (3+2i).$$

b) Si $(x,y) \in \mathbf{Z}^2$ vérifie $x^2+y^2 = p^2$, nous avons

$$(x+iy)(x-iy) = p^2.$$

Puisque $p \equiv 3$ (4), le nombre p reste premier dans $\mathbf{Z}[i]$. D'après le lemme de Gauss (pour $\mathbf{Z}[i]$), p divise l'un des deux facteurs $x+iy$ ou $x-iy$. Il divise donc les deux car si $z = pw$ alors $\overline{z} = \overline{pw} = p\overline{w}$, où la barre désigne le nombre complexe conjugué. Donc p divise $x+iy$. Disons $x+iy = \alpha p$ pour un $\alpha \in \mathbf{Z}[i]$. Pour les normes, nous obtenons

$$p^2 = N(x+iy) = N(\alpha)N(p) = N(\alpha) \times p^2.$$

Ainsi $N(\alpha) = 1$ et $\alpha \in \{1, i, -1, -i\}$. Donc $x+iy \in \{p, ip, -p, -ip\}$ ce qui signifie que

$$(x,y) \in \{(p,0), (0,p), (-p,0), (0,-p)\}.$$