Solution du problème (sujet zéro du Capes 2011).

I: Calcul de $\varphi(n)$

1.a Supposons que $\dot{x}=\dot{y}$, c'est-à-dire que $ab|x-y$ donc $a|x-y$ et $b|x-y$ d'où $x-y\equiv 0 \mod a$ et $x-y\equiv 0 \mod b$ et par suite $\overline{x}=\overline{y}$ et $\overline{\overline{x}}=\overline{\overline{y}}$.

1.b.i Montrons que f est un morphisme d'anneaux. Soient alors $\dot{x},\dot{y}$ deux éléments de $\mathbb{Z}/ab\mathbb{Z}$. Nous avons $f(\dot{x}+\dot{y})=f(\dot{x+y})=(\overline{x+y};\overline{\overline{x+y}})=(\overline{x};\overline{\overline{x}})+(\overline{y};\overline{\overline{y}})=f(\dot{x})+f(\dot{y})$. Il s'ensuit ainsi que f est un morphisme de groupes.
On montre alors de même que $f(\dot{(}x)\times dot(y))=f(\dot{x\times y})=(\overline{x\times y};\overline{\overline{x\times y}})=(\overline{x};\overline{\overline{x}})\times(\overline{y};\overline{\overline{y}})=f(\dot{x})\times f(\dot{y})$.
Enfin, $f(\dot{1})=(\overline{1};\overline{\overline{1}})$ d'où f est un morphisme d'anneaux.

1.b.ii Montrons que f est injectif. Soient alors $\dot{x}$ et $\dot{y}$ deux éléments de $\mathbb{Z}/ab\mathbb{Z}$ tels que $f(\dot{x})=f(\dot{y})$. Alors $(\overline{x};\overline{\overline{x}})=(\overline{y};\overline{\overline{y}})$. Aussi, $\overline{x}=\overline{y}$ donc $\overline{x-y}=\overline{0}$, c'est-à-dire que $x-y$ est divisible par a. De même, puisque $\overline{\overline{x}}=\overline{\overline{y}}$, nous déduisons que $x-y$ est divisible par b. Enfin, puisque $a\wedge b=1$, nous en déduisons alors que $x-y$ est divisible par ab, soit $\dot{\widehat{x-y}}=\dot{0}$ et donc $\dot{x}=\dot{y}$. Il s'ensuit donc que f est injective.

1.b.iii La fonction f est une injection entre $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$. Or, puisque les ensembles $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ ont même cardinal (à savoir ab), il s'ensuit que f réalise une bijection entre $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$.

I.2 Raisonnons par récurrence sur l'entier naturel k.
Initialisation: Au rang $k=2$, la propriété est vraie par **I.1.b.iii**.
Hérédité: Soit $k\geq 2$ et supposons que la propriété est vraie au rang k. Soient alors $a_1,a_2,\cdots,a_k,a_{k+1}$ des entiers deux à deux premiers entre eux. Puisque $a_1\times\cdots\times a_k$ est premier avec a_{k+1}, nous en déduisons par la question **I.1.b.iii** que $\mathbb{Z}/(a_1a_2\cdots a_ka_{k+1})\mathbb{Z}$ est isomorphe à $\mathbb{Z}/(a_1\cdots a_k)\mathbb{Z}\times\mathbb{Z}/a_{k+1}\mathbb{Z}$. Or, par hypothèse de récurrence, nous savons que $\mathbb{Z}/(a_1\cdots a_k)\mathbb{Z}$ est isomorphe à $\mathbb{Z}/a_1\mathbb{Z}\times\mathbb{Z}/a_2\mathbb{Z}\times\mathbb{Z}/a_3\mathbb{Z}\times\cdots\times\mathbb{Z}/a_k\mathbb{Z}$ d'où nous obtenons bien l'hypothèse au rang $k+1$.

I.3 Raisonnons par double inclusion. Soit alors $x=(x_1,\cdots,x_k)\in U(A_1\times\cdots A_k)$. Aussi, par définition de l'inverse d'un élément, il existe $y=(y_1,\cdots,y_k)\in U(A_1,\cdots\times A_k)$ tel que $x\times y=1$, c'est-à-dire tel que $\forall i\in\{1,\cdots,k\}$, $x_i\times y_i=1_{A_i}$, d'où $x_i\in U(A_i)$ et donc nous en déduisons l'inclusion $U(A_1\times\cdots A_k)\subset U(A_1)\times U(A_2)\times\cdots\times U(A_k)$.

Réciproquement, soit $x=(x_1,\cdots,x_k)\in U(A_1)\times U(A_2)\times\cdots\times U(A_k)$. Pour tout $i\in\{1,\cdots,k\}$, il existe donc $y_i\in U(A_i)$ tel que $x_i\times y_i=1_{A_i}$ et donc si $y=(y_1,\cdots,y_k)$, on a $x\times y=1$, d'où nous en déduisons que $x\in U(A_1\times\cdots\times A_k)$ d'où l'inclusion réciproque $U(A_1)\times\cdots U(A_k)\subset U(A_1\times\cdots A_k)$.

I.4.a Montrons que $(U(A),\times)$ est un groupe. Nous savons déjà que $\times$ est une loi de composition interne sur $U(A)$, et elle est associative (car $(A,+,\times)$ est un anneau). L'anneau A étant supposé unitaire, nous en déduisons que $1_A\in U(A)$, d'où $\times$ admet un élément neutre dans $U(A)$. Tout élément x de $U(A)$ admet bien un symétrique (inverse) puisqu'il existe $y\in U(A)$ tel que $x\times y=y\times x=1_A$. Il s'ensuit donc que $(U(A);\times)$ est un groupe.

I.4.b On suppose donc l'existence d'un isomorpime $f:A\to B$ d'anneaux. On note $\overline{f}$ la restriction de f à $U(A)$: montrons donc que $f(U(A))=U(B)$. Soit $x\in U(A)$. Il existe donc $y\in U(A)$ tel que $x\times y=1_A$ et puisque f est un isomorphisme, nous en déduisons que $f(x\times y)=f(x)\times f(y)$. Or, $f(x\times y)=f(1_A)=1_B$ (car $f(1_A\times x)=f(1_A)\times f(x)$ et donc $f(1_A)=1_B$). Il s'ensuit donc que $f(x)\in U(B)$, et donc l'image de $U(A)$ par f est dans $U(B)$. Réciproquement, si $y\in U(B)$, alors il exite $y'\in U(B)$ tel que $y\times y'=1_B$. Puisque f réalise une bijection entre A et B, il existe $x,x'\in A$ tel que $f(x)=y$ et $f(x')=y'$. Nous avons alors: $f(x\times x')=y\times y'=1_B$. Or, l'unique antécédent de 1_B par f est 1_A, d'où $x\times x'=1_A$ et donc $x\in U(A)$. Il s'ensuit donc que $\overline{f}$ est un isomorphisme de $U(A)$ sur $U(B)$.

I.5 Par l'identité de Bezout, nous savons que $x\wedge n=1$ si et seulement s'il existe $(u,v)\in\mathbb{Z}^2$ tels que $xu+nv=1$, et donc $\overline{xu}=\overline{x}\times\overline{u}=\overline{1}$, si et seulement si $\overline{x}\in U(\mathbb{Z}/n\mathbb{Z})$. Nous en déduisons donc que $U(\mathbb{Z}/n\mathbb{Z})=\{\overline{x};x\in\{1,\cdots,n\},\ x\wedge n=1\}$.

I.6 On suppose $n=p^k$ avec p premier et $k\in\mathbb{N}^*$.

I.6.a Soit $x\in\mathbb{Z}$. Nous savons par **I.5** que $\overline{x}\notin U(\mathbb{Z}/n\mathbb{Z})$ si et seulement si $x\wedge n\neq 1$. Or, $n=p^k$, donc $x\wedge n=1$ ssi $p|x$.

I.6.b Dans l'ensemble $\{1,\cdots,p^k\}$, il y a p^{k-1} multiples de p: aussi en dénombrant l'ensemble complémentaire, nous en déduisons que le cardinal de l'ensemble $U(\mathbb{Z}/n\mathbb{Z})$ est égal à p^k-p^{k-1} d'où $\varphi(p^k)=p^k-p^{k-1}$.

I.7 Raisonnons par récurrence sur l'entier s (nombre de facteurs premiers de n).
Initialisation: Si $s=1$, alors $s=p_1^{\alpha_1}$ et par la question précédente, $\varphi(p_1^{\alpha_1})=p_1^{\alpha_1}-p_1^{\alpha_1-1}$.
Hérédité: Soit $s\geq 1$, et supposons l'hypothèse au rang s soit vraie, et soit alors $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}p_{s+1}^{\alpha_{s+1}}$. Alors, puisque $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}\wedge p_{s+1}^{\alpha_{s+1}}=1$, nous en déduisons que

$$\varphi(n)=\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s})\times\varphi(p_{s+1}^{\alpha_{s+1}})=\varphi(p_1^{\alpha_1})\times\varphi(p_2^{\alpha_2})\times\cdots\varphi(p_s^{\alpha_s})\varphi(p_{s+1}^{\alpha_{s+1}})=n\prod_{1\leq i\leq n}\left(1-\frac{1}{p_i}\right)$$

II.1.1 Montrons que $AB = \{ab, a \in A, b \in B\}$ est un sous-groupe de G. Déjà, AB est non vide puisque $e \in A$ et $e \in B$ puisque se sont des sous-groupes, d'où $e \in AB$. Ensuite, le produit de deux éléments de AB est aussi un élément de AB puisque G est commutatif. Reste à montrer que AB est stable par passage au symétrique: si $ab \in AB$, alors $a^{-1}b^{-1} \in AB$ et vérifie $ab \times a^{-1}b^{-1} = 1$. Il s'ensuit que AB est un sous-groupe de G.

II.1.2 Soient $(a, b), (a', b') \in A \times B$. Alors $f((a, b) \times (a', b')) = f((aa', bb')) = aa'bb' = f((a, b)) \times f((a', b'))$, d'où f est bien un morphisme de groupes. Reste à montrer que c'est un isomorphisme. Pour ce faire, considérons $f((a, b)) = f((a', b'))$. Alors $ab = a'b'$, et donc $bb'^{-1} = a'a^{-1}$. Aussi, l'élément $a'a^{-1} = bb'^{-1} = e$ car appartient à la fois à A et B. Par unicité de l'inverse d'un élément, nous en déduisons que $a = a'$ et $b = b'$ d'où f est injective. Elle est clairement surjective, d'où f réalise une bijection de $A \times B$ dans AB.

II.1.3.a Supposons G fini de cardinal $n = 2m$, et qu'il existe $a, b \in G$ avec $o(a) = m$ et $o(b) = 2$, et tel que $b \notin < a >$. Supposons donc l'existence de $i, j \in \{1, 2, \cdots, n\}$ tels que $a^i = a^j$ et raisonnons par l'absurde en supposant par exemple que $i < j$. Nous déduisons alors que $a^{j-i} = 1_G$. Or, $1 < j - i < m$ d'où nous obtenons une contradiction avec le fait que $o(a) = m$.

I.1.3.b La question précédente implique directement que $Card(\{a^i, i \in \{1, \cdots, m\}) = m$. Ensuite, tout élément de la forme $a^i b$ n'est pas un élément de $< a >$ puisque sinon, nous aurions $b \in < a >$ ce qui n'est pas. Aussi les deux ensembles en question sont-ils disjoints. Enfin, il est aisé de voir que tous les éléments de $a^i b$ sont différents puisque si $a^i b = a^j b$ alors $a^i = a^j$ et donc par la question précédente, $i = j$. Aussi, nous en déduisons que le cardinal de l'ensemble considéré est égal à $2m$.

I.1.3.c Nous savons que, par définition du produit de deux groupes, $< a >< b >= \{a^i b^j, i \in \{1, \cdots, m\}, j \in \{1, 2\}\}$ est un sous-groupe de G de même cardinal que G d'où $G =< a >< b >$.

I.1.3.d Reprenons l'application f de la question **II.1** avec $A =< a >$ et $B =< b >$. Nous en déduisons alors que $< a > \times < b >$ est isomorphe à $G =< a >< b >$.

I.2 $G_k = U(\mathbb{Z}/2^k\mathbb{Z})$.

I.2.1 G_1 est donc le groupe des unités de $\mathbb{Z}/2\mathbb{Z}$ donc est l'ensemble $\{1\}$.
G_2 est le groupe des unités de $\mathbb{Z}/4\mathbb{Z}$, donc en faisant la table nous en déduisons que $G_2 = \{1, 3\}$.
G_3 est le groupe des unités de $\mathbb{Z}/8\mathbb{Z}$, donc en faisant la table du groupe nous en déduisons que $G_3 = \{1, 3, 5, 7\}$.

II.2.2 Puisque 5 et 2^k sont premiers entre eux, d'après le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tels que $5u + 2^k v = 1$. Aussi en déduisons nous que $5u \equiv 1 \mod 2^k$ et par suite $\overline{5} = \overline{1}$.

II.2.3.a Soient alors $i \in \mathbb{N}$ et $x \in \mathbb{Z}$. En utilisant la formule du multinome $(a+b+c)^2 = a^2+b^2+c^2+2ab+2ac+2bc$ (la formule est valable car nous sommes dans un anneau commutatif) nous obtenons que

$$(1 + 2^{i+2} + x2^{i+3})^2 \equiv 1 + 2^{2i+4} + x^2 2^{2i+6} + 2^{i+3} + x2^{i+4} + x2^{2i+5} \equiv 1 + 2^{i+3} + x2^{i+4} \mod 2^{2i+4}.$$

II.2.3.b Raisonnons par récurrence sur l'entier naturel i.
Initialisation: Pour $i = 1$, puisque $5 = 2^2 + 1$, par la formule du binôme de Newton nous obtenons que: $(1 + 2^2)^2 \equiv 1 + 2^3 + 2^4 \equiv 1 + 2^3 \mod 2^4$ et la formule est donc vraie.
Hérédité: Supposons la propriété vraie au rang i et démontrons là au rang $i + 1$. Nous avons:

$$5^{2^{i+1}} = \left(5^{2^i}\right)^2 = (1 + 2^{i+2} + x2^{i+3})^2 \equiv 1 + 2^{i+2} + x2^{i+4} \mod 2^{2i+4}.$$

Aussi, nous en déduisons que : $5^{2^{i+1}} \equiv 1 + 2^{i+2} \mod 2^{i+3}$.

II.2.4 Nous savons par la question précédente que $5^{2^i} = 1 + 2^{i+2} + x2^{i+3}$, d'où $5^{2^i} - 1 = 2^{i+2} + x2^{i+3} = (1 + 2x)2^{i+2}$. Or, $1 + 2x$ est toujours impaire, donc $5^{2^i} - 1 \equiv 0 \mod 2^k$ si et seulement si $i + 2 \geq k$, c'est-à-dire $i \geq k - 2$. Nous en déduisons alors que $\overline{5}$ est d'ordre $k - 2$ dans G_k.

II.2.5 Raisonnons par l'absurde en supposant que $\overline{-1} \in < \overline{5} >$, c'est-à-dire qu'il existe $i \in \{1, \cdots, 2^{k-2}\}$ tel que $5^i \equiv -1 \mod 2^k$. Alors en élevant cette relation de congruence au carré, nous obtenons $(-1)^2 \equiv 5^{2i} \mod 2^k$, soit $5^{2i} \equiv 1 \mod 2^k$. Or, 5 est un élément d'ordre 2^{k-2} donc $2^{k-2}|2i$ soit $2^{k-3}|i$. Nous en déduisons alors puisque $i \in \{1, \cdots, 2^{k-2}\}$ que $i = 2^{k-3}$ ou $i = 2^{k-2}$. Le second cas aboutit à une absurdité puisque si $i = k - 2$ alors $5^{2^{k-2}} \equiv 1 \mod 2^k$ donc n'est pas congru à -1 mor 2^k. Reste alors à étudier le cas $i = 2^{k-3}$. La relation précédente montre que $5^{2^{k-3}} \equiv 1+2^{k-3} \mod 2^k$; il suffit alors de remarquer que $1+2^{k-3} < 2^k - 1$ pour en déduire que $\overline{5}^{2^{k-3}} \neq \overline{-1}$ dans G_k. Il s'ensuit alors que $\overline{-1} \notin < \overline{5} >$.

II.2.6 G_k est donc un groupe d'ordre 2^{k-1} (tous les éléments non multiples de 2 sont inversibles: comme il y a autant d'éléments pairs que d'impairs, nous en déduisons ce cardinal), contenant un élément $a = \overline{5}$ d'ordre 2^{k-2} et $b = \overline{-1}$ d'ordre 2. Nous pouvons alors appliquer le résultat obtenu pour $a = \overline{5}$ et $b = -1$, et il s'ensuit que $G_k = \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par la question **II.1.3.d**.