ISM MP, Mathématiques
Année 2025/2026

Feuille d'exercices n°86

Exercice 1 (**)

Soient p et q deux nombres premiers distincts. On note $n = pq$. Soit d entier premier avec $w = (p-1)(q-1)$.

1. Justifier qu'il existe un entier e tel que $de \equiv 1\ [w]$.
2. Montrer $\qquad \forall x \in \mathbb{Z} \qquad x^{de} \equiv x\ [n]$

Corrigé : 1. On a $d \wedge w = 1$ d'où $\bar{d} \in \mathrm{U}(\mathbb{Z}/w\mathbb{Z})$. Ainsi, il existe $\bar{e} \in \mathbb{Z}/w\mathbb{Z}$ tel que $\bar{d}\bar{e} = \bar{1}$ et en choisissant un entier $e \in \bar{e}$, on conclut

$$\boxed{\text{Il existe } e \text{ entier tel que } de \equiv 1\ [w].}$$

2. Soit $x \in \mathbb{Z}$. D'après l'isomorphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, on a

$$x^{de} \equiv x\ [n] \iff \begin{cases} x^{de} \equiv x\ [p] \\ x^{de} \equiv x\ [q] \end{cases}$$

Si $x \wedge p = 1$, alors $x^{p-1} \equiv 1\ [p]$ d'après le petit théorème de Fermat et comme $de = 1 + kw$ avec $k \in \mathbb{Z}$, il vient dans le corps $\mathbb{F}_p$ avec $\bar{x} \neq \bar{0}$

$$\bar{x}^{de} = \bar{x}^{1+k(p-1)(q-1)} = \bar{x}\left(\bar{x}^{p-1}\right)^{k(q-1)} = \bar{x}$$

Sinon, on a $p|x$ d'où $p|x^{de}$ et par conséquent

$$x^{de} \equiv x \equiv 0\ [p]$$

Le même raisonnement vaut évidemment modulo q. On conclut

$$\boxed{\forall x \in \mathbb{Z} \qquad x^{de} \equiv x\ [n]}$$

Remarque : Il s'agit du fondement du *chiffrement RSA*. La donnée (n, e) est la clé publique communiquée par M à James Bond. James chiffre un entier $x \in [\![\, 0\,;\, n-1 \,]\!]$ par $x \mapsto x^e\ [n]$ et M le décrypte avec sa clé privée d par l'opération $y \mapsto y^d\ [n]$. Un espion interceptant la clé publique (n, e) souhaitant déchiffrer le message aurait besoin de déterminer d, l'inverse modulaire de e modulo w. Si w est connu, le problème est facile à résoudre avec l'algorithme d'Euclide étendu. En revanche, si w est inconnu, factoriser n permettrait d'extraire p et q, mais on ne sait pas faire cette factorisation en temps raisonnable si p et q sont très grands.

Exercice 2 (***)

Soit n entier impair, $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$ et $\mathrm{Z} = \sum_{k=0}^{n-1} \omega^{k^2}$. Calculer $|\mathrm{Z}|^2$.

Corrigé : Soit $k \in [\![\, 0\,;\, n-1 \,]\!]$. On observe $\omega^k = \omega^\ell$ pour $(k, \ell) \in \bar{k}^2$. Ainsi, la valeur de ω^ℓ est indépendante du choix de $\ell \in \bar{k}$. On définit

$$\forall k \in [\![\, 0\,;\, n-1 \,]\!] \qquad \omega^{\bar{k}} = \omega^k$$

En remarquant l'égalité $\bar{\omega} = \omega^{-1}$, il vient

$$|\mathrm{Z}|^2 = \left(\sum_{k=0}^{n-1}\omega^{k^2}\right)\left(\overline{\sum_{\ell=0}^{n-1}\omega^{\ell^2}}\right) = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{k^2}\bar{\omega}^{\ell^2} = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{k^2-\ell^2} = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{(k+\ell)(k-\ell)}$$

Ainsi $$|\mathrm{Z}|^2 = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{\overline{(k+\ell)(k-\ell)}} = \sum_{0\leqslant k,\ell\leqslant n-1}\omega^{(\bar{k}+\bar{\ell})(\bar{k}-\bar{\ell})}$$

L'application $(\bar{k},\bar{\ell}) \to (\bar{k}+\bar{\ell},\bar{k}-\bar{\ell})$ réalise une permutation de $(\mathbb{Z}/n\mathbb{Z})^2$. En effet, pour (k,ℓ) et (p,q) dans $[\![\,0\,;\,n-1\,]\!]^2$, on a

$$\begin{cases}\bar{k}+\bar{\ell}=\bar{p}\\ \bar{k}-\bar{\ell}=\bar{q}\end{cases} \iff \begin{cases}\bar{2}\bar{k}=\bar{p}+\bar{q}\\ 2\ell=\bar{p}-\bar{q}\end{cases} \iff \begin{cases}\bar{k}=\bar{2}^{-1}\,(\bar{p}+\bar{q})\\ \bar{\ell}=\bar{2}^{-1}\,(\bar{p}-\bar{q})\end{cases}$$

les équivalences ayant lieu car $\bar{2}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ puisque $2\wedge n = 1$. Ainsi, on a

$$|\mathrm{Z}|^2 = \sum_{0\leqslant p,q\leqslant n-1}\omega^{\bar{p}\bar{q}} = \sum_{0\leqslant p,q\leqslant n-1}\omega^{\overline{pq}} = \sum_{0\leqslant p,q\leqslant n-1}\omega^{pq} = n + \sum_{p=1}^{n-1}\underbrace{\sum_{q=0}^{n-1}(\omega^p)^q}_{=0}$$

On conclut $$\boxed{|\mathrm{Z}|^2 = n}$$

Remarque : Les sommes $\sum_{k=0}^{n-1}\omega^{k^2}$ avec $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$ et n entier non nul sont les célèbres *sommes de Gauss* dont la détermination du signe devant les expressions algébriques résista à Gauss durant plusieurs années.

Exercice 3 (***)

Déterminer les entiers $n \geqslant 2$ tel que $\varphi(n)$ divise n.

Corrigé : Notons $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i nombres premiers strictement ordonnés et les α_i entiers non nuls. On a $\varphi(n) = \prod_{i=1}^{r}\left[p_i^{\alpha_i-1}(p_i-1)\right]$ d'où

$$\varphi(n)|n \iff \prod_{i=1}^{r}(p_i-1)|\prod_{i=1}^{r}p_i$$

Or, excepté le cas où $p_i = 2$, on a p_i impair donc $p_i - 1$ pair. Si $p_1 > 2$, on a $2^r|\prod_{i=1}^{r}(p_i-1)$ d'où $2^r|\prod_{i=1}^{r}p_i$. Or, le nombre $\prod_{i=1}^{r}p_i$ est impair d'où l'absurdité. On a donc $p_1 = 2$. Si $r = 1$, alors $\varphi(2^\alpha) = 2^{\alpha-1}$ divise 2. Si $r > 1$, on a

$$2^{r-1}|\prod_{i=1}^{r}(p_i-1) \quad\Longrightarrow\quad 2^{r-2}|\prod_{i=2}^{r}p_i$$

Or, le nombre $\prod_{i=2}^{r}p_i$ est impair d'où $r = 2$. Ainsi, l'entier n s'écrit $n = 2^\alpha p^\beta$ avec α,β entiers non nuls et p un nombre premier impair. On a

$$\varphi(n)|n \iff 2^{\alpha-1}p^{\beta-1}(p-1)|2^\alpha p^\beta \iff \frac{p-1}{2}|p$$

Comme p est premier, ses seuls diviseurs sont 1 et lui même et comme on a $\dfrac{p-1}{2} < p$, il s'ensuit nécessairement

$$\frac{p-1}{2} = 1 \iff p = 3$$

On conclut $\boxed{\forall n \geqslant 2 \qquad \varphi(n)|n \iff n \in \left\{2^\alpha 3^\beta, (\alpha,\beta) \in \mathbb{N}^* \times \mathbb{N}\right\}}$

Exercice 4 (***)

Soient m, n des entiers non nuls. Établir

$$(3^n - 1) \wedge (3^m - 1) = 3^{n \wedge m} - 1$$

Corrigé : Notons $c = (3^n - 1) \wedge (3^m - 1)$ et $d = n \wedge m$. On a $d|n$ d'où $n = dk$ avec $k \in \mathbb{N}$ puis, avec l'identité de Bernoulli

$$3^n - 1 = (3^d)^k - 1 = (3^d - 1)\sum_{j=0}^{k-1} 3^{jk} \quad \Longrightarrow \quad 3^d - 1 | 3^n - 1$$

et de même pour $3^m - 1$ donc $3^d - 1|c$. D'après la propriété de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $d = um + vn$. Les entiers relatifs u et v ne sont pas tous deux strictement positifs sinon d serait strictement supérieur à n et m alors qu'il en est un diviseur et comme d est positif, les entiers u et v ne sont pas tous deux strictement négatifs. Sans perte de généralité, on peut supposer $u \leqslant 0$ et $v \geqslant 0$. Puis, on trouve

$$3^d - 1 = 3^{um+vn} - 1 = 3^{um+vn} - 3^{vn} + 3^{vn} - 1 = -3^{um+vn}(3^{-um} - 1) + 3^{vn} - 1$$

et à nouveau par des factorisations avec l'identité de Bernoulli, on obtient

$$3^d - 1 = (3^m - 1)(-3^d)3^v n \sum_{j=0}^{-u-1} 3^{mj} + (3^n - 1)\sum_{j=0}^{v-1} 3^{nj} \in (3^m - 1)\mathbb{Z} + (3^n - 1)\mathbb{Z} = c\mathbb{Z}$$

ce qui prouve $c|3^d - 1$. Les entiers c et $3^d - 1$ sont donc associés et on conclut

$$\boxed{(3^n - 1) \wedge (3^m - 1) = 3^{n \wedge m} - 1}$$

Variante : On conserve les notations précédentes. On effectue la division euclidienne $n = mq + r$ avec $r \in [\![0\,;\, m - 1]\!]$. On a

$$3^n - 1 = 3^{mq+r} - 1 = 3^{mq+r} - 3^r + 3^r - 1 = 3^r(3^{mq} - 1) + 3^r - 1$$

$$= 3^r(3^m - 1)(1 + 3^m + \ldots + 3^{m(q-1)}) + 3^r - 1 = (3^m - 1)\mathrm{Q} + 3^r - 1$$

avec $\mathrm{Q} = 3^r(1 + 3^m + \ldots + 3^{m(q-1)})$. D'après le théorème d'Euclide, on a

$$(3^n - 1) \wedge (3^m - 1) = (3^m - 1) \wedge (3^r - 1)$$

Il suffit ensuite d'utiliser l'algorithme d'Euclide. On définit la suite $(u_k)_k$ par $u_0 = n$, $u_1 = m$ et u_{k+2} le reste de la division euclidienne de u_k par u_{k+1}. Il existe un seuil p entier tel que $u_{p+1} = 0$. D'après la propriété établie, la suite $\left((3^{u_k} - 1) \wedge (3^{u_{k+1}} - 1)\right)_k$ est constante. Ainsi

$$(3^n - 1) \wedge (3^m - 1) = (3^{u_p} - 1) \wedge (3^{u_{p+1}} - 1) = 3^{u_p} - 1$$

et l'algorithme d'Euclide se termine avec $u_p = n \wedge m$ ce qui prouve le résultat souhaité.

Exercice 5 (***)

Soit p nombre premier impair. Déterminer le nombre de carrés dans $\mathbb{F}_p$.

Corrigé : 1. Notons $\Psi : \mathbb{F}_p \to \mathbb{F}_p, \bar{x} \mapsto \bar{x}^2$. Pour $x \in \mathbb{F}_p$, on a

$$\Psi(\bar{x}) = \bar{0} \iff \bar{x}^2 = \bar{0} \iff \bar{x} = \bar{0}$$

par intégrité du corps $\mathbb{F}_p$. Ceci prouve que $\bar{0}$ est un carré avec $\bar{0}$ pour unique antécédent. Soit $\bar{y} \in \text{Im } \Psi \setminus \{\bar{0}\}$. On dispose de $\bar{a} \in \mathbb{F}_p^*$ tel que $\psi(\bar{a}) = \bar{y}$ puis, pour $\bar{x} \in \mathbb{F}_p$

$$\Psi(\bar{x}) = \bar{y} \iff \Psi(\bar{x}) = \Psi(\bar{a}) \iff (\bar{x} - \bar{a})(\bar{x} + \bar{a}) = \bar{0} \iff \bar{x} \in \{\bar{a}, -\bar{a}\}$$

par intégrité du corps $\mathbb{F}_p$. Par ailleurs, on a

$$\bar{a} = -\bar{a} \iff \bar{2}\bar{a} = \bar{0} \underbrace{\iff}_{\bar{2} \in \mathrm{U}(\mathbb{F}_p)} \bar{a} = \bar{0}$$

d'où $\bar{a} \neq -\bar{a}$. Ainsi, tout élément de $\text{Im } \Psi \setminus \{\bar{0}\}$ admet exactement 2 antécédents dans $\mathbb{F}_p^*$ d'où

$$\text{Card } \mathbb{F}_p^* = p - 1 = 2 \,\text{Card } (\text{Im } \Psi \setminus \{\bar{0}\})$$

On conclut

$$\boxed{\text{Le nombre de carrés de } \mathbb{F}_p \text{ est } \frac{p+1}{2}.}$$

Exercice 6 (***)

Soit p entier avec $p \geqslant 2$. Montrer le théorème de *Wilson* :

$$(p-1)! \equiv -1 \ [p] \iff p \text{ premier}$$

Corrigé : Supposons p premier $\geqslant 3$. Les éléments de $\mathbb{F}_p$ qui sont leur propre inverse vérifient

$$\bar{x}^2 = \bar{1} \iff (\bar{x} - \bar{1})(\bar{x} + \bar{1}) = \bar{0} \iff \bar{x} \in \{\bar{1}, -\bar{1}\}$$

par intégrité du corps $\mathbb{F}_p$. On a $\bar{1} \neq -\bar{1}$ puisque $p > 2$. Par conséquent, dans le produit $\prod_{k=1}^{p-1} \bar{k}$, exceptés $\bar{1}$ et $\overline{p-1}$ qui sont leur propre inverse, tous les autres termes admettent leur inverse dans la liste $\left\{\bar{2}, \ldots, \overline{p-2}\right\}$. En les associant par paire, il vient

$$\prod_{k=1}^{p-1} \bar{k} = \bar{1} \times \overline{p-1} = -\bar{1}$$

Si $p = 2$, le résultat est toujours vrai. Supposons $(p-1)! \equiv -1 \ [p]$. Par suite, toutes les classes $\bar{1}, \ldots, \overline{p-1}$ sont inversibles puisque

$$\forall k \in [\![\, 1 \,;\, p-1 \,]\!] \qquad \bar{k} \times \left(- \prod_{i \in [\![\, 1 \,;\, p-1 \,]\!] \setminus \{k\}} \bar{i} \right) = \bar{1}$$

d'où $\mathbb{Z}/p\mathbb{Z}$ est un corps ce qui implique p premier. Ainsi

$$\boxed{(p-1)! \equiv -1 \ [p] \iff p \text{ premier}}$$

Exercice 7 (***)

1. Soit $p > 2$ un nombre premier. Montrer :

$$-\bar{1} \text{ carré dans } \mathbb{F}_p \iff p \equiv 1 \ [4]$$

2. En déduire qu'il existe une infinité de nombres premiers de la forme $1 + 4n$ avec n entier.

Corrigé : 1. Supposons que $-\bar{1}$ soit un carré dans $\mathbb{F}_p$ et soit $\bar{x} \in \mathbb{F}_p$ tel que $\bar{x}^2 = -\bar{1}$. On a nécessairement $\bar{x} \in \mathbb{F}_p^*$. Comme $\bar{x}^4 = \bar{1}$, son ordre dans $\mathbb{F}_p^* = \mathrm{U}(\mathbb{F}_p)$ vérifie $o(\bar{x})|4$ et n'est ni 1 ni 2 d'où $o(\bar{x}) = 4$. Ainsi, on a 4 divise $p - 1$ d'où $p \equiv 1 \ [4]$. Réciproquement, si $p \equiv 1 \ [4]$, on note $p = 1 + 4n$ avec n entier non nul. D'après le théorème de Wilson, on a $(p-1)! \equiv -1 \ [p]$ d'où

$$\prod_{k=1}^{4n} k \equiv -1 \ [p] \iff \prod_{k=1}^{2n} k \times \prod_{k=1}^{2n} (-k) \equiv (-1)^{2n} (2n)!^2 \equiv (2n)!^2 \equiv -1 \ [p]$$

On conclut $\boxed{-1 \text{ carré dans } \mathbb{F}_p \iff p \equiv 1\ [4]}$

2. Supposons que les nombres premiers de la forme $1+4n$ avec n entier soient en nombre fini et notons p le plus grand d'entre eux. On pose $\mathrm{N} = 1 + (p!)^2$ et soit q facteur premier de N. On a $(p!)^2 \equiv -1\ [q]$ d'où q de la forme $1+4n$ avec n entier, d'après le résultat de la première question. Par hypothèse sur p, on a $q \leqslant p$ d'où q divise $p!$ et comme q divise N alors q divise $\mathrm{N} - (p!)^2 = 1$ ce qui est absurde. On conclut

$\boxed{\text{Il existe une infinité de nombres premiers de la forme } 1+4n \text{ avec } n \text{ entier.}}$

Remarque : Il s'agit d'un cas particulier du *théorème de Dirichlet* encore appelé *théorème de la progression arithmétique* : soient a et b des entiers premiers entre eux, il existe une infinité de nombres premiers de la forme $an+b$ avec n entier.

Exercice 8 (***)

Soit n un entier avec $n \geqslant 2$ et p un nombre premier. Montrer

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Corrigé : Soit $n \geqslant 2$. On a

$$v_p(n!) = v_p\left(\prod_{k=1}^{n} k\right) = \sum_{k=1}^{n} v_p(k) = \sum_{k=1}^{n} \left(\sum_{i \in \mathbb{N}^*,\ p^i | k} 1 \right)$$

La somme en i est finie puisque p^i divise k impose $p^i \leqslant k$ soit $i \leqslant \ln(k)/\ln(p)$. Comme les sommes sont finies, en changeant l'ordre de sommation, on obtient

$$v_p(n!) = \sum_{(k,i) \in [\![1\,;n]\!] \times \mathbb{N}^*,\ p^i | k} 1 = \sum_{i=1}^{+\infty} \left(\sum_{k \in [\![1\,;n]\!],\ p^i | k} 1 \right) = \sum_{i=1}^{+\infty} \left(\sum_{k \in \{p^i, 2p^i, \dots \lfloor n/p^i \rfloor p^i\}} 1 \right)$$

On conclut $\boxed{\forall n \geqslant 2 \qquad \forall p \in \mathcal{P} \qquad v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor}$

Remarque : Ce résultat s'intitule *Formule de Legendre.*

Exercice 9 (***)

Soit p premier et k entier. Montrer que

$$\sum_{\bar{x} \in \mathbb{F}_p} \bar{x}^k = \bar{0} \quad \text{ou} -\bar{1}$$

Corrigé : Soit $\bar{a} \in \mathbb{F}_p^*$. L'application $\bar{x} \mapsto \bar{a}\bar{x}$ est une permutation de $\mathbb{F}_p$. On a

$$\sum_{\bar{x} \in \mathbb{F}_p} \bar{x}^k = \sum_{\bar{x} \in \mathbb{F}_p} (\bar{a}\bar{x})^k = \bar{a}^k \sum_{\bar{x} \in \mathbb{F}_p} \bar{x}^k \quad \Longrightarrow \quad (\bar{1} - \bar{a}^k) \sum_{\bar{x} \in \mathbb{F}_p} \bar{x}^k = 0$$

Si $\bar{a}^k = 1$ pour tout $\bar{a} \in \mathbb{F}_p^*$ (possible avec $k = p-1$ par exemple), alors

$$\sum_{\bar{x} \in \mathbb{F}_p} \bar{x}^k = \bar{0} + \sum_{\bar{x} \in \mathbb{F}_p^*} \bar{x}^k = \overline{p-1} = -\bar{1}$$

D'où $\boxed{\sum_{\bar{x} \in \mathbb{F}_p} \bar{x}^k = \bar{0} \quad \text{ou} \quad = -\bar{1}}$

Exercice 10 (***)

Soit $n \geqslant 3$ entier impair.

1. Soit p nombre premier impair et α entier non nul. Montrer
$$x^2 \equiv 1\ [p^\alpha] \iff x \equiv \pm 1\ [p^\alpha]$$
2. Combien y-a-t-il d'éléments x de $[\![\, 1\,;\, n-1\,]\!]$ vérifiant $x^2 \equiv 1\ [n]$?
3. Déterminer le nombre de carrés de $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$?

Corrigé : 1. On procède par récurrence sur α. Si $\alpha = 1$, le résultat est vrai par intégrité dans $\mathbb{F}_p$:
$$x^2 \equiv 1\ [p] \iff (x-1)(x+1) \equiv 0\ [p] \iff x \equiv \pm 1\ [p]$$
Supposons le résultat vrai au rang α entier non nul. Soit x entier tel que $x^2 \equiv 1\ [p^{\alpha+1}]$. Alors, on a $x^2 \equiv 1\ [p^\alpha]$ d'où $x = \varepsilon + kp^\alpha$ avec $\varepsilon \in \{-1, 1\}$ et $k \in \mathbb{Z}$. Puis
$$x^2 \equiv 1\ [p^{\alpha+1}] \iff (\varepsilon + kp^\alpha)^2 \equiv 1\ [p^{\alpha+1}] \iff \varepsilon^2 + 2k\varepsilon p^\alpha + k^2 p^{2\alpha} \equiv 1\ [p^{\alpha+1}]$$
Comme $p^{2\alpha} \equiv 0\ [p^{\alpha+1}]$, on trouve $2k\varepsilon p^\alpha \equiv 0\ [p^{\alpha+1}]$ autrement dit $2k\varepsilon \equiv 0\ [p]$. On a $2\varepsilon \in \mathrm{U}(\mathbb{F}_p)$ d'où $k \equiv 0\ [p]$, autrement dit $k = p\ell$ avec $\ell \in \mathbb{Z}$. Ainsi, on a
$$x = \varepsilon + \ell p^{\alpha+1} \equiv \pm 1\ [p^{\alpha+1}]$$
ce qui clôt la récurrence. On conclut
$$\boxed{x^2 \equiv 1\ [p^\alpha] \iff x \equiv \pm 1\ [p^\alpha]}$$
2. On décompose $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers et les α_i entiers non nuls. D'après le théorème d'isomorphisme des restes chinois, on a
$$x^2 \equiv 1\ [n] \iff \forall i \in [\![\, 1\,;\, r\,]\!] \qquad x^2 \equiv 1\ [p_i^{\alpha_i}]$$
Avec le résultat de la question précédente, on a donc
$$x^2 \equiv 1\ [n] \iff \forall i \in [\![\, 1\,;\, r\,]\!] \qquad x \equiv \pm 1\ [p_i^{\alpha_i}]$$
On conclut
$$\boxed{\text{Card } \{x \in [\![\, 1\,;\, n-1\,]\!] \mid x^2 \equiv 1\ [n]\} = 2^r}$$
3. On pose
$$\psi\colon \begin{cases} \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) \\ x \qquad\quad \longmapsto x^2 \end{cases}$$
Il s'agit d'un morphisme de groupes multiplicatifs. Le nombre de carrés de $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$ est précisément Card Im ψ et on a établi précédemment Card Ker $\psi = 2^r$. Pour $(x, y) \in \mathrm{U}(\mathbb{Z}/n\mathbb{Z})^2$, on a
$$\psi(x) = \psi(y) \iff xy^{-1} \in \text{Ker } \psi$$
Ainsi, on a $x = \alpha y$ avec $\alpha \in \text{Ker } \psi$. Pour un carré de $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$, il y a donc 2^r racines. On conclut
$$\boxed{\text{Il y a Card Im } \psi = \frac{\text{Card U}(\mathbb{Z}/n\mathbb{Z})}{\text{Card Ker } \psi} = \frac{\varphi(n)}{2^r} \text{ carrés dans U}(\mathbb{Z}/n\mathbb{Z}).}$$
Remarque : Il s'agit d'un cas particulier d'utilisation du résultat de l'exercice 3 feuille 81.