Théorie des Nombres - TD1
Rappels d'arithmétique élémentaire

Exercice 1 : Trouver tous les entiers $n \in \mathbb{N}$ tels que $\varphi(n) = 6$. Même question avec $\varphi(n) = 12$. Caractériser les entiers $n \in \mathbb{N}$ tels que $\varphi(n)$ ne soit pas multiple de 4.

Solution de l'exercice 1.
- Résolvons $\varphi(n) = 6$. On décompose $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ en facteurs premiers. Alors $\varphi(n) = \prod_i p_i^{\alpha_i - 1}(p_i - 1)$. Supposons $\varphi(n) = 6 = 2.3$. Alors pour tout i, si $\alpha_i \geq 2$, on a $\alpha_i = 2$ et $p_i = 2$ ou 3. Si $\alpha_i = 1$, alors $p_i - 1$ divise 6, donc $p_i = 2, 3$ ou 7. Donc n est de la forme $2^a.3^b.7^c$, avec $0 \leq a, b \leq 2$ et $0 \leq c \leq 1$. On vérifie facilement que les seules solutions sont alors $n = 7, 9, 14, 18$.
- Résolvons $\varphi(n) = 12$. On décompose $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ en facteurs premiers. Alors $\varphi(n) = \prod_i p_i^{\alpha_i - 1}(p_i - 1)$. Supposons $\varphi(n) = 12 = 2^2.3$. Alors pour tout i, si $\alpha_i \geq 3$, on a $\alpha_i = 3$ et $p_i = 2$. Si $\alpha_i = 2$, alors $p_i = 2$ ou 3. Si $\alpha_i = 1$, alors $p_i - 1$ divise 12, donc $p_i = 2, 3, 5, 7$ ou 13. Donc n est de la forme $2^a.3^b.5^c.7^d.13^e$, avec $0 \leq a \leq 3$, $0 \leq b \leq 2$ et $0 \leq c, d, e \leq 1$. On vérifie facilement que les seules solutions sont alors $n = 13, 21, 26, 28, 36, 42$.
- On décompose $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ en facteurs premiers. Alors 4 ne divise pas $\varphi(n)$ si et seulement si (n admet exactement un facteur premier impair congru à 3 modulo 4 et $v_2(n) \leq 1$) ou $n = 1, 2, 4$ si et seulement si $n = 1, 2, 4, p^m, 2.p^m$, où p est un nombre premier, $p \equiv 3$ [4] et $m \geq 1$.

Exercice 2 : Montrer que $n = \sum_{d|n} \varphi(d)$.

Solution de l'exercice 2. On considère l'ensemble E des fractions $\frac{k}{n}$, avec $1 \leq k \leq n$. Alors $\#E = n$ et tout élément de E s'écrit d'une façon unique sous la forme réduite $\frac{a}{d}$, avec d diviseur de n et $1 \leq a \leq d$ premier à d. Récirpoquement, toute fraction $\frac{a}{d}$ de cette forme est dans E. Par conséquent, on peut partitionner E en fonction du dénominateur de l'écriture irréductible des éléments de E. On a donc une union disjointe

$$E = \bigcup_{d|n} \left\{ \frac{a}{d} : 1 \leq a \leq d, d|n \text{ et } \operatorname{pgcd}(a, d) = 1 \right\} .$$

D'où le résultat en calculant les cardinaux des deux côtés. Remarque : cela revient à étudier le groupe des racines n-ièmes de l'unité dans $\mathbb{C}$ et le partitionner en fonction de l'ordre des éléments de ce groupe.

Exercice 3 : Soit $n \in \mathbb{N}$, $n \geq 2$. Montrer que $\varphi(n) \geq \frac{\log 2}{2} \frac{n}{\log n}$.

Solution de l'exercice 3. On décompose n en facteurs premiers $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, avec p_i premiers, $p_1 < \dots < p_r$ et $\alpha_i \geq 1$. On a alors $\frac{\varphi(n)}{n} = \prod_i \left(1 - \frac{1}{p_i}\right)$. Or pour tout i, $p_i \geq i + 1$, donc $\frac{\varphi(n)}{n} \geq \prod_i \left(1 - \frac{1}{i+1}\right) = \frac{1}{r+1} \geq \frac{1}{2r}$. Enfin, il est clair que $2^r \leq n$, donc $r \leq \frac{\log n}{\log 2}$, donc finalement $\frac{\varphi(n)}{n} \geq \frac{\log 2}{2 \log n}$, ce qui conclut.

Exercice 4 : Soient $d, m \in \mathbb{N}$. Résoudre le système suivant, d'inconnues $x, y \in \mathbb{Z}$:

$$\begin{cases} \operatorname{pgcd}(x, y) = d \\ \operatorname{ppcm}(x, y) = m \end{cases} .$$

Combien de solutions obtient-on dans le cas où $d = 12$ et $m = 11760$? Et en général, donner une formule pour le nombre de solutions du système.

Solution de l'exercice 4. Tout d'abord, il est clair que pour que le système ait une solution, il faut que $d|m$. On suppose donc désormais que d divise m. On décompose $d = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $m = p_1^{\beta_1} \dots p_r^{\beta_r}$, avec $\beta_i \geq \alpha_i$. Soient $x, y \in \mathbb{Z}^2$. Alors (x, y) solution si et seulement si il existe $x', y' \in \mathbb{Z}^2$ premiers entre eux, tels que $x = dx'$, $y = dy'$ et $\mathrm{ppcm}(x', y') = \frac{m}{d}$. On se ramène donc au cas où $d = 1$.
On résoud donc le système suivant, dans $\mathbb{N}^2$:

$$\begin{cases} \mathrm{pgcd}(x', y') = 1 \\ \mathrm{ppcm}(x', y') = p_1^{\beta_1 - \alpha_1} \dots p_r^{\beta_r - \alpha_r} \end{cases} .$$

Il est clair que les solutions de ce sytème dans $\mathbb{N}^2$ sont en bijection avec l'ensemble des parties de $F := \{1 \leq i \leq r : \beta_i > \alpha_i\}$: l'ensemble des solutions n'est autre que

$$\mathcal{S}' = \left\{ \left(\prod_{i \in I} p_i^{\beta_i - \alpha_i}, \prod_{i \notin I} p_i^{\beta_i - \alpha_i} \right) ; I \subset F \right\} .$$

Par conséquent, l'ensemble des solutions dans $\mathbb{Z}^2$ du système initial est

$$\mathcal{S} = \left\{ \left(\epsilon \prod_{i \in I} p_i^{\beta_i}, \epsilon' \prod_{i \notin I} p_i^{\beta_i} \right) ; I \subset F; \epsilon, \epsilon' \in \{\pm 1\} \right\} .$$

En particulier, le nombre de solutions du système est égal à $2^{\#F+2}$, où $\#F$ n'est autre que le nombre de facteurs premiers de $\frac{m}{d}$.
Dans l'exemple proposé, on a bien $d|m$, et $\frac{m}{d} = 980 = 2^2.5.7^2$. Donc $\frac{m}{d}$ a trois facteurs premiers, donc le système admet $2^5 = 32$ solutions. Quitte à changer les signes de x et y, et à échanger x et y, les solutions sont donc $(12, 11760)$, $(48, 2940)$, $(60, 2352)$ et $(588, 240)$.

Exercice 5 : Soit A un anneau commutatif. Soient I, J des idéaux de A tels que $I + J = A$.

a) Montrer que pour tout $m, n \geq 1$, on a $I^m + J^n = A$.

b) Montrer que l'on a des isomorphismes canoniques d'anneaux

$$A/(I^m J^n) \xrightarrow{\cong} A/(I^m \cap J^n) \xrightarrow{\cong} A/I^m \times A/J^n .$$

c) En déduire que si $m_1, \dots, m_n$ sont des entiers deux-à-deux premiers entre eux, alors on a un isomorphisme canonique

$$\mathbb{Z}/(\prod_i m_i \mathbb{Z}) \xrightarrow{\cong} \prod_i (\mathbb{Z}/m_i\mathbb{Z}) .$$

d) Pour $n = 2$ et $n = 3$, expliciter la réciproque de l'isomorphisme précédent.

Solution de l'exercice 5.

a) Par hypothèse, il existe $i, j \in I$ tels que $1 = i + j$. On pose $r := m + n - 1$. Alors on a

$$1 = 1^r = (i + j)^r = \sum_{k=0}^{r} \binom{r}{k} i^k j^{r-k} .$$

Or, si $k < m$, on a $r - k \geq n$, donc $i^k j^{r-k} \in J^n$, et si $k \geq m$, on a $i^k j^{r-k} \in I^m$. Par conséquent, en posant $i_0 := \sum_{k=m}^{r} \binom{r}{k} i^k j^{r-k}$ et $j_0 := \sum_{k=0}^{m-1} \binom{r}{k} i^k j^{r-k}$, on a $1 = i_0 + j_0$, avec $i_0 \in I^m$ et $j_0 \in J^n$, donc $1 \in I^m + J^n$, donc $I^m + J^n = A$.

b) Par la question précédente, il suffit de considérer le cas $m = n = 1$. On considère le morphisme d'anneaux naturel $\psi : A \to A/I \times A/J$ qui envoie un élément $a \in A$ sur le couple $(a \mod I, a \mod J)$. Tout d'abord, il est clair que $\mathrm{Ker}(\psi) = I \cap J$. Montrons que ψ est surjectif. Par hypothèse, il existe $i \in I$ et $i \in J$ tels que $1 = i + j$. Soient $b, c \in A$. On définit $a := c.i + b.j$.

Alors on a $a \equiv b.j \bmod I$, et $j \equiv 1 \bmod I$, donc finalement $a \equiv b \bmod I$ (cela revient à écrire $a = b + (c-b)i$). De même, $a \equiv c \bmod J$ (i.e. $a = c + (b-c)j$). Donc on a construit $a \in A$ tel que $\psi(a) = (b \bmod I, c \bmod J)$. Donc ψ est surjectif. Par conséquent, ψ induit un isomorphisme

$$\overline{\psi} : A/(I \cap J) \xrightarrow{\cong} A/I \times A/J\,.$$

Il reste à montrer que $I \cap J = I.J$. On a d'abord l'inclusion évidente $I.J \subset I \cap J$. Montrons l'inclusion inverse : soit $a \in I \cap J$. Par hypothèse, il existe $i \in I$ et $j \in J$ tels que $1 = i + j$. Donc $a = a(i+j) = ia + aj$. Puisque $a \in I \cap J$, on a $ia, aj \in I.J$, donc $a \in I.J$. Par conséquent, $I \cap J = I.J$, ce qui conclut la question.

c) C'est une application directe de la question précédente : on montre d'abord que si $k, l \in \mathbb{Z}$ sont premiers entre eux, alors on a un isomorphisme canonique $\mathbb{Z}/(kl\mathbb{Z}) \xrightarrow{\cong} \mathbb{Z}/k\mathbb{Z} \times Z/l\mathbb{Z}$ (cas $n = 2$). Ceci résulte de la question b), en prenant $A = \mathbb{Z}$, $m = n = 1$, $I = k\mathbb{Z}$ et $J = l\mathbb{Z}$. Le cas général se démontre par récurence en utilisant le cas $n = 2$.

d) Traitons d'abord le cas $n = 2$: par construction (voir la preuve de la question b)), on dispose d'entiers $u, v \in \mathbb{Z}$ tels que $1 = um_1 + vm_2$. On définit alors un morphisme $\tau : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/m_1m_2\mathbb{Z}$ par $(a, b) \mapsto bum_1 + avm_2 \bmod m_1m_2\mathbb{Z}$. On vérifie facilement que c'est un morphisme d'anneaux. On vérifie que son moyau est exactement l'idéal $m_1\mathbb{Z} \times m_2\mathbb{Z} \subset \mathbb{Z} \times \mathbb{Z}$, donc τ induit un morphisme $\overline{\tau} : \mathbb{Z}/m_1Z \times \mathbb{Z}/m_2\mathbb{Z} \to \mathbb{Z}/m_1m_2\mathbb{Z}$. On vérifie enfin que $\overline{\psi} \circ \overline{\tau} = \mathrm{id}$ et $\overline{\tau} \circ \overline{\psi} = \mathrm{id}$, ce qui conclut le cas $n = 2$. Pour $n = 2$, on applique deux fois de suite le cas $n = 2$. Par Bezout, on écrit $1 = um_1 + vm_2$ et $1 = w(m_1m_2) + xm_3$. On obtient que la réciproque de l'isomorphisme $\mathbb{Z}/m_1m_2m_3\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \mathbb{Z}/m_3\mathbb{Z}$ est donnée par

$$(a \bmod m_1\mathbb{Z}, b \bmod m_2\mathbb{Z}, c \bmod m_3\mathbb{Z}) \mapsto cwm_1m_2 + buxm_1m_3 + avxm_2m_3 \bmod m_1m_2m_3\mathbb{Z}\,.$$

Exercice 6 : On dispose d'un certain nombre d'objets. On les range par paquets de 2, il en reste un tout seul. On les range par 3, il en reste 2. Par 4, il en reste 3. Par 5, il en reste 4. Par 6, il en reste 5. Quel est le nombre minimal d'objets dont on dispose ? Même question en allant jusqu'à des paquets de 10, de sorte qu'il en reste 9. Et plus généralement, que dire si on va jusqu'à des paquets de n objets, de sorte qu'il en reste $n - 1$?

Solution de l'exercice 6.

– On note x le nombre total d'objets. Le problème équivaut alors au système suivant, d'inconnue $x \in \mathbb{N}$:

$$\begin{cases} x \equiv 1\ [2] \\ x \equiv 2\ [3] \\ x \equiv 3\ [4] \\ x \equiv 4\ [5] \\ x \equiv 5\ [6] \end{cases}.$$

On peut réécrire ce système sous la forme équivalente suivante :

$$\begin{cases} x \equiv -1\ [2] \\ x \equiv -1\ [3] \\ x \equiv -1\ [4] \\ x \equiv -1\ [5] \\ x \equiv -1\ [6] \end{cases}.$$

Le lemme chinois assure que ce système équivaut alors au suivant :

$$\begin{cases} x \equiv -1\ [4] \\ x \equiv -1\ [3] \\ x \equiv -1\ [5] \end{cases}.$$

Or $3.4.5 = 60$, donc une nouvelle application du lemme chinois assure que ce système équivaut à l'équation

$$x \equiv -1 \ [60] \, .$$

Par conséquent, la solution positive minimale du problème initial est $x = 59$.

– En allant jusqu'á 10 objets, le même raisonnement aboutit au système

$$\begin{cases} x \equiv -1 \ [8] \\ x \equiv -1 \ [9] \\ x \equiv -1 \ [5] \\ x \equiv -1 \ [7] \end{cases} ,$$

lequel équivaut à l'équation

$$x \equiv -1 \ [2520] \, .$$

donc la solution positive minimale est $x = 2519$.

– Dans le cas général, un raisonnement exactement similaire assure que la solution minimale du système avec $n-1$ équations est

$$x = \left(\prod_{p^r \leq n < p^{r+1}} p^r \right) - 1 \, .$$

On peut écrire ce nombre également de la façon suivante :

$$x = \mathrm{ppcm}(1, 2, \ldots, n) - 1 \, .$$

Exercice 7 : Résoudre le système suivant, d'inconnue $x \in \mathbb{Z}$:

$$\begin{cases} 2x \equiv 4 \ [5] \\ 4x \equiv 5 \ [7] \\ 3x \equiv 1 \ [8] \end{cases} .$$

Solution de l'exercice 7. Le système est équivalent au système suivant :

$$\begin{cases} x \equiv 2 \ [5] \\ x \equiv 3 \ [7] \\ x \equiv 3 \ [8] \end{cases} .$$

Pour résoudre ce système, on utilise le théorème chinois : puisque 5 et 7 sont premiers entre eux, on a un isomorphisme d'anneaux $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/35\mathbb{Z}$. La relation de Bezout $3.5 - 2.7 = 1$ assure que cet isomorphisme est donné par $(a \bmod 5, b \bmod 7) \mapsto 3.5.b - 2.7.a \bmod 35$, donc les deux premières lignes du système équivalent à l'équation $x \equiv 17 \ [35]$. On est donc ramené à résoudre le système

$$\begin{cases} x \equiv 17 \ [35] \\ x \equiv 3 \ [8] \end{cases} .$$

On utilise une nouvelle fois le théorème chinois et la relation de Bezout $3.35 - 13.8 = 1$, pour montrer que le système précédent est équivalent à l'équation suivante $x \equiv -1453 \ [280]$, c'est-à-dire à $x \equiv 227 \ [280]$. L'ensemble des solutions du système est donc l'ensemble des entiers de la forme $227 + 280k$, $k \in \mathbb{Z}$.

Exercice 8 :

a) Soit $n \geq 1$. Combien l'équation $x^2 = 1$ a-t-elle de solutions dans $\mathbb{Z}/n\mathbb{Z}$?

b) On pose $n = 23275$. Combien l'équation $x^4 = 1$ a-t-elle de solutions dans $\mathbb{Z}/n\mathbb{Z}$.

c) Résoudre $x^2 - 4x + 15 = 0$ dans $\mathbb{Z}/45\mathbb{Z}$.

Solution de l'exercice 8.

a) On commence par traiter le cas $n = p^\alpha$, avec p premier impair et $\alpha \geq 1$. On sait que le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est cyclique d'ordre pair, donc il contient un unique sous-groupe d'ordre 2, donc l'équation $x^2 = 1$ admet exactement deux solutions dans $\mathbb{Z}/p^\alpha\mathbb{Z}$, pour tout p premier impair, $\alpha \geq 1$. Un raisonnement analogue assure que cette équation admet une solution dans $\mathbb{Z}/2\mathbb{Z}$, deux dans $\mathbb{Z}/4\mathbb{Z}$ et quatre dans $\mathbb{Z}/2^\alpha\mathbb{Z}$ avec $\alpha \geq 3$ (En utilisant le fait que $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$). Pour le cas général, on décompose $n = 2^r p_1^{\alpha_1} \dots p_s^{\alpha_s}$ en facteurs premiers, et on utilise le lemme chinois qui assure que le nombre de solutions de $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$ est égal au produit du nombre de solutions dans chacun des $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ et dans $\mathbb{Z}/2^r\mathbb{Z}$. Par conséquent, les raisonnements précédents assurent que le nombre de solutions est égal à 2^s si $r = 0$ ou 1, à 2^{s+1} si $r = 2$ et à 2^{s+2} si $r \geq 3$.

b) On écrit $n = 5^2 7^2 19$, donc il suffit de déterminer le nombre de solutions dans $\mathbb{Z}/25\mathbb{Z}$, $\mathbb{Z}/49\mathbb{Z}$ et $\mathbb{Z}/19\mathbb{Z}$. Puisque $\mathbb{Z}/19\mathbb{Z}$ est un corps, l'équation $x^4 = 1$ admet au plus quatre solutions. Puisque $19 \equiv 3$ [4], -1 n'est pas un carré modulo 19, donc l'équation $x^4 = 1$ admet exactement deux solutions modulo 19, qui sont ± 1. On sait que $(\mathbb{Z}/25\mathbb{Z})^*$ est cyclique d'ordre 20, donc il admet exactement quatre éléments d'ordre divisant 4, donc l'équation $x^4 = 1$ a exactement quatre solutions dans $\mathbb{Z}/25\mathbb{Z}$ (qui sont les classes de $1, -1, 7, -7$ modulo 25). On fait le même raisonnement pour $\mathbb{Z}/49\mathbb{Z}$: le groupe $(\mathbb{Z}/49\mathbb{Z})^*$ est cyclique d'ordre 42, donc contient exactement deux éléments d'ordre inférieur ou égal à 2. Donc $x^4 = 1$ admet exactement deux solutions modulo 49. Finalement, l'équation $x^4 = 1$ admet exactement $2.4.2 = 16$ solutions modulo 23275.

c) On a $x^2 - 4x + 15 = (x-2)^2 + 11$, donc l'équation initiale est équivalente au système

$$\begin{cases} (x-2)^2 \equiv 4 \ [5] \\ (x-2)^2 \equiv 7 \ [9] \end{cases}.$$

On résoud ces deux équations en calculant les racines carrées de 4 (resp. 7) modulo 5 (resp. 9), qui sont les classes de 2 et 3 (resp. de 4 et 5). Donc l'équation est équivalente à

$$\begin{cases} x - 2 \equiv 2 \text{ ou } 3 \ [5] \\ x - 2 \equiv 4 \text{ ou } 5 \ [9] \end{cases}.$$

Finalement, en réutilisant l'isomorphisme d'anneaux $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/45\mathbb{Z}$, via une relation de Bezout (par exemple $2.5 - 9 = 1$), on trouve que l'équation initale admet quatre solutions dans $\mathbb{Z}/45\mathbb{Z}$, qui sont $15, 24, 25, 34$ modulo 45.

Exercice 9 : Déterminer le nombre de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$, en fonction de la décomposition de n en facteurs premiers.

Solution de l'exercice 9. Puisque $\mathbb{Z}/n\mathbb{Z}$ est cyclique, pour tout $d|n$, $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe (nécessairement cyclique) de cardinal d (ce sous-groupe n'est autre que $(\frac{n}{d}\mathbb{Z})/n\mathbb{Z}$). Par conséquent, le nombre de sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est égal au nombre de diviseur de n. Or si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, le nombre de diviseurs de n est égal à $(\alpha_1 + 1) \dots (\alpha_r + 1)$. Finalement, le groupe $\mathbb{Z}/n\mathbb{Z}$ admet exactement $(\alpha_1 + 1) \dots (\alpha_r + 1)$ sous-groupes.

Exercice 10 :

a) Soit $n \in \mathbb{N}$. Montrer que l'on a un isomorphisme canonique de groupes : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

b) Soient p, q deux nombres premiers. Soit G un groupe d'ordre pq. Montrer que

i) si $p = q$, alors G est commutatif et soit $G \cong \mathbb{Z}/p^2\mathbb{Z}$, soit $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

ii) si $p < q$ et p ne divise pas $q-1$, alors G est commutatif et $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

iii) si $p < q$ et p divise $q-1$, alors soit G est commutatif et $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, soit G n'est pas commutatif et il est isomorphe à l'unique produit semi-direct non trivial $\mathbb{Z}/q\mathbb{Z} \rtimes Z/p\mathbb{Z}$.

c) Déterminer tous les groupes d'ordre 12, à isomorphisme près (on montrera d'abord qu'un tel groupe est produit semi-direct d'un groupe d'ordre 4 et d'un groupe d'ordre 3).

Solution de l'exercice 10.

a) Le morphisme $\varphi : \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^*$ est défini par $\varphi(\psi) := \psi(1) \in \mathbb{Z}/n\mathbb{Z}$. Puisque 1 engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$, pour tout $\psi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, $\psi(1)$ engendre $\mathbb{Z}/n\mathbb{Z}$, donc $\psi(1) \in (\mathbb{Z}/n\mathbb{Z})^*$. On vérifie que φ est un morphisme de groupes. Sa réciproque est donnée par $\varphi^{-1} : (\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ défini pour tout $r \in (\mathbb{Z}/n\mathbb{Z})^*$ par $\varphi^{-1}(r) : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto r.x$. On vérifie facilement que les deux morphismes sont inverses l'un de l'autre.

b) i) Si $p = q$, G est un p-groupe, donc son centre est non trivial. En particulier, G admet un sous-groupe central d'ordre p. Et le quotient par ce sous-groupe central est un groupe cyclique d'ordre p. Donc G est commutatif d'ordre p^2, il est donc isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, selon que G admette un élément d'ordre p^2 ou non.

ii) Si $p < q$, le théorème de Sylow assure l'existence d'un sous-groupe $H \subset G$ de cardinal q. Or le nombre de tels q-Sylows est congru à 1 modulo q et divise p, donc il est nécessairement égal à 1, ce qui signifie que H est distingué dans G. Le quotient $Q := G/H$ est alors d'ordre p, donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Puisque G admet aussi un p-Sylow, dont l'intersection avec H est nécessairement réduite à l'élément neutre, la suite exacte

$$1 \to H \to G \to Q \to 1$$

est scindée et G est donc un produit semi-direct $H \rtimes Q$, pour l'action de Q sur H définie par la conjugaison via une section. Cette action est un morphisme de groupes $Q \to \mathrm{Aut}(H)$, c'est-à-dire un morphisme de groupes $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Or la question a) assure que $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) = (\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$, donc le produit semi-direct G est donné par un morphisme de groupes $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$. Ici, p ne divise pas $q-1$, donc ce morphisme est nécessairement trivial, donc l'action de Q sur H est triviale, donc G est isomorphe au produit direct $H \times Q \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

iii) Si p divise $q-1$, le groupe $\mathbb{Z}/(q-1)\mathbb{Z}$ admet un unique sous-groupe d'ordre p, et il existe donc un morphisme non constant $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$, unique à un automorphisme de $\mathbb{Z}/p\mathbb{Z}$ près. Or deux tels morphismes $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$, puisqu'ils diffèrent d'un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, induisent des produits semi-directs $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ isomorphes. Le raisonnement précédent assure alors que ce produit semi-direct est l'unique (à isomorphisme près) groupe non commutatif d'ordre pq, ce qui conclut la preuve.

c) Les théorèmes de Sylow assurent que si G est un groupe de cardinal 12, il admet un ou quatre 3-Sylows. S'il en admet un seul, alors ce 3-Sylow est distingué et G est un produit semi-direct du quotient (qui est un groupe d'ordre 4) par ce sous-groupe d'ordre 3. Si G admet quatre 3-Sylows, alors G admet $4.2 = 8$ éléments d'ordre 3, donc nécessairement exactement 3 éléments d'ordre 2 ou 4, donc un unique 4-Sylow (qui est donc distingué) formé de ces trois éléments et du neutre. Donc dans ce second cas, G est produit semi-direct d'un groupe à 3 éléments par un groupe à 4 éléments. Il reste donc à déterminer tous ces produits semi-directs à isomorphisme près. Pour cela, on voit d'abord qu'il existe un unique morphisme non constant $\mathbb{Z}/4Z \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, ce qui définit un unique produit semi-direct non trivial $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$. Ensuite il existe des morphismes non constants $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, et deux tels morphismes diffèrent d'un automorphisme de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, d'où un unique produit semi-direct non trivial $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Ensuite, tout morphisme $\mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ est constant, donc il n'y a pas de produit semi-direct non trivial de $\mathbb{Z}/4\mathbb{Z}$ par $\mathbb{Z}/3\mathbb{Z}$. Enfin, il existe deux morphismes non constants $\mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathfrak{S}_3$, qui diffèrent d'un automorphisme de $\mathbb{Z}/3\mathbb{Z}$,

d'où un unique produit semi-direct non trivial $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$. Finalement, on obtient les cinq classes d'isomorphismes de groupes suivantes : $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} = \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$, $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/3\mathbb{Z}$.

Exercice 11 : Montrer qu'il existe des suites arbitrairement longues de nombres entiers consécutifs non premiers.

Solution de l'exercice 11. Soit $n \geq 2$. On considère les $(n-1)$ entiers suivants : $n!+2, n!+3, \ldots, n!+n$. Pour tout $2 \leq k \leq n$, k divise $n!+k$, et $n!+k > k$, donc $n!+k$ n'est pas premier. Par conséquent, on a construit, pour tout $n \geq 2$, une suite de $n-1$ entiers consécutifs non premiers.

Exercice 12 : On note p_n le n-ième nombre premier, et $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x.

a) Montrer que $p_n < 2^{2^n}$.

b) En déduire un encadrement (grossier) de $\pi(x)$.

c) Montrer qu'il existe une infinité de nombres premiers de la forme $6k+5$.

d) Montrer que si $\text{pgcd}(a,b) = 1$, tout diviseur premier impair de a^2+b^2 est congru à 1 modulo 4.

e) En déduire qu'il existe une infinité de nombres premiers de la forme $8k+5$.

Solution de l'exercice 12.

a) On reprend la preuve d'Euclide qui montre l'infinitude de l'ensemble des nombres premiers. Partant de $p_1, \ldots, p_n$ les n premiers nombres premiers, on en construit un nouveau, supérieur à tous les autres, en prenant un facteur premier q de $p_1 \ldots p_n + 1$. On a donc $q \leq p_1 \ldots p_n + 1$, donc $p_{n+1} \leq p_1 \ldots p_n + 1$. Une récurrence facile permet alors de conclure.

b) Pour tout $x, n \in \mathbb{N}$, on a $\pi(x) \geq n$ si et seulement si $p_n \leq x$. Donc la question a) assure que $\pi(x) \geq n$ dès que $x \geq 2^{2^n}$. On en déduit alors que $\pi(x) \geq \log_2(\log_2(x))$. Finalement, on a donc l'encadrement naif suivant

$$\log_2(\log_2(x)) \leq \pi(x) \leq x\,.$$

c) Soient $l_1, \ldots, l_n$ des nombres premiers distincts tels que $l_i \equiv 5\ [6]$. On pose $N := l_1 \ldots l_n + 4$ si n est pair, $N := l_1 \ldots l_n + 6$ si n est impair. Alors $N \equiv 5\ [6]$. Donc il existe un nombre premier l divisant N, tel que $l \equiv 5\ [6]$ (sinon, tous les facteurs premiers de N serait congrus à 1 modulo 6, donc N serait congru à 1 modulo 6, ce qui n'est pas). Alors l est distinct de tous les l_i (sinon $l = 2$ ou 3, ce qui n'est pas possible). Cette construction assure qu'il existe une infinité de nombres premiers de la forme $6k+5$.

d) Soit p un diviseur premier de a^2+b^2. D'abord, p est impair On a $a^2+b^2 \equiv 0\ [p]$. Puisque $\text{pgcd}(a,b) = 1$, on peut supposer que p ne divise pas b. Alors -1 est un carré dans $\mathbb{F}_p^*$ (c'est le carré de $\frac{b}{a}$), donc $p \equiv 1\ [4]$.

e) Soient $l_1, \ldots, l_n$ des nombres premiers distincts tels que $l_i \equiv 5\ [8]$. On note $N := (l_1 \ldots l_n)^2 + 4$. La question d) assure que tout diviseur premier de N est congru à 1 modulo 4. Supposons que tous ces diviseurs premiers soient congrus à 1 modulo 8. Alors $N \equiv 1\ [8]$. Or pour tout i, $l_i^2 \equiv 1\ [8]$, donc $N \equiv 5\ [8]$, ce qui est contradictoire. Donc il existe un diviseur premier de N, noté l_{n+1}, qui est congru à 5 modulo 8. En outre, $l_{n+1} \neq l_i$ pour tout $1 \leq i \leq n$, puisque $l_{n+1} \neq 2$. Donc on a construit un nouveau nombre premier l_{n+1} congru à 5 modulo 8. Cela assure qu'il existe une infinité de nombres premiers de la forme $8k+5$.

Exercice 13 : Déterminer tous les entiers relatifs a, b tels que $\cos(\frac{2\pi a}{b})$ est rationnel.
[Indication : on pourra utiliser le polynôme $X^2 - 2\cos(\frac{2\pi a}{b})X + 1$].

Solution de l'exercice 13. Par périodicité et parité de la fonction cosinus, on peut supposer $0 \leq a < b$ et $\text{pgcd}(a,b) = 1$.

On suppose $\cos(\frac{2\pi a}{b}) \in \mathbb{Q}$. On note $P(X) := X^2 - 2\cos(\frac{2\pi a}{b})X + 1$. Alors on a $P(e^{\frac{2i\pi a}{b}}) = 0$, donc $P(X) \in \mathbb{Q}[X]$ annule $e^{\frac{2i\pi a}{b}}$. Or $e^{\frac{2i\pi a}{b}}$ est une racine de l'unité, c'est une racine primitive b-ième de l'unité. Or le polynôme minimal de $e^{\frac{2i\pi a}{b}}$ est le polynôme cyclotomique ϕ_b, de degré $\varphi(b)$. Par conséquent, ϕ_b divise $P(X)$, donc $\varphi(b) = 1$ ou 2. Donc $b = 1, 2, 3, 4$ ou 6. Donc $\frac{a}{b} \in \left\{0, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{6}, \frac{5}{6}\right\}$. Réciproquement, on sait que ces valeurs de $\frac{a}{b}$ donnent des valeurs rationnelles de $\cos(\frac{2\pi a}{b}$. Finalement, l'ensemble des rationnels $\frac{a}{b}$ recherchés est (modulo $\mathbb{Z}$ et au signe près) :

$$\left\{0, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{6}, \frac{5}{6}\right\}.$$

Exercice 14 :

a) Soit A un anneau principal.

i) Montrer que A est noethérien.

ii) On définit

$$E := \{(a); a \in A, a \neq 0, a \text{ ne se décompose pas en produit d'un inversible par des irréductibles}\}.$$

Montrer, en raisonnant par l'absurde, que $E = \emptyset$.

iii) Soit $p \in A$ irréductible. Montrer que (p) est un idéal maximal, donc premier.

iv) En déduire que A est factoriel.

b) Montrer qu'un anneau euclidien est principal.

c) Donner un exemple d'anneau factoriel non noethérien.

d) Montrer que $\mathbb{Z}[i\sqrt{5}]$ est un anneau intègre noethérien non factoriel.
[Indication : décomposer 9 en produit d'irréductibles dans $\mathbb{Z}[i\sqrt{5}]$].

e) Donner un exemple d'anneau factoriel non principal.

f) On note $\alpha := \frac{1+i\sqrt{19}}{2}$ et $A := \mathbb{Z}[\alpha]$.

i) On définit, pour $a \in A$, $N(a) := a\overline{a}$. Montrer que pour tout $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que ($r = 0$ ou $N(r) < N(b)$) et (a ou $2a$ s'écrit $bq + r$).
[Indication : on pourra écrire $t := \frac{a}{b} = x + y\alpha$ avec $x, y \in \mathbb{Q}$, et distinguer suivant la distance de y à sa partie entière].

ii) Montrer que l'idéal (2) de A est maximal.

iii) Montrer que A est principal.

iv) Montrer que dans un anneau euclidien B, il existe $b \in B$, $b \notin B^*$, tel que $B^* \cup \{0\}$ sur surjecte sur $B/(b)$.

v) Montrer que $A^* = \{\pm 1\}$.

vi) Montrer que pour tout $x \in A$, l'anneau $A/(x)$ n'est pas isomorphe à $\mathbb{Z}/2\mathbb{Z}$, ni à $\mathbb{Z}/3\mathbb{Z}$.

vii) Conclure que A est principal non euclidien.

g) Montrer que $\mathbb{Z}$, $k[X]$ (k est un corps) et $\mathbb{Z}[i]$ sont des anneaux euclidiens.

Solution de l'exercice 14.

a) i) Montrons par exemple que tout suite croissante d'idéaux de A est stationnaire. Soit $I_1 \subset I_2 \subset \ldots$ une telle suite. Définissons $I := \bigcup_{n \geq 1} I_n$. Alors I est clairement un idéal de A. Comme A est principal, il existe $a \in A$ tel que $I = (a)$. Donc $a \in \bigcup_n I_n$, donc il existe $n_0 \geq 1$ tel que $a \in I_{n_0}$. Alors on a $I_n = (a)$ pour tout $n \geq n_0$, donc la suite (I_n) est stationnaire. Donc A est noethérien.

ii) On suppose que $E \neq \emptyset$. Alors E est une famille non vide d'idéaux de A, donc E admet un élément maximal : il existe $a \in A$, tel que a ne soit pas décomposable en produit d'irréductibles et que (a) soit maximal dans E. En particulier, a n'est pas irréductible, donc il existe $b, c \in A$, qui ne sont pas des éléments inversibles de A, tels que $a = bc$. Alors (b) ou (c) est dans E (sinon $(a) = (bc)$ ne serait pas dans E) et (a) est contenu strictement dans (b) et dans (c). Cela contredit le caractère maximal de (a) dans E. Par conséquent, $E = \emptyset$.

iii) Soit I un idéal de A contenant (p). A est principal, donc $I = (a)$, avec $a \in A$. Puisque $(p) \subset (a)$, a divise p. Comme p est irréductible, a est inversible ou alors a est associé à p. Donc $(a) = A$ ou $(a) = (p)$. Donc (p) est maximal, donc premier.

iv) Tout d'abord, A est intègre car principal. Ensuite, la question a)ii) assure que tout élément de A est décomposable en un produit d'un inversible par des irréductibles. Montrons enfin que cette décomposition est unique à association près et à l'ordre près des facteurs. Soient $p_1, \dots, p_r$, $l_1, \dots, l_s$ des irréductibles de A, tels que les p_i (resp. les l_j) soient deux à deux non associés. Soient $\alpha_i, \beta_j \geq 1$. Supposons que $p_1^{\alpha_1} \dots p_r^{\alpha_r} = l_1^{\beta_1} \dots l_s^{\beta_s}$. Alors p_1 divise $l_1^{\beta_1} \dots l_s^{\beta_s}$, donc $l_1^{\beta_1} \dots l_s^{\beta_s} \in (p_1)$. Par la question a)iii), (p_1) est un idéal premier. Donc il existe $1 \leq j \leq s$ tel que $l_j \in (p_1)$. Donc l_j et p_1 sont associés. On divise par p_1 des deux côtés de l'égalité, puis on recommence. Par récurrence, on montre ainsi que pour tout i, il existe un unique j tel que p_i soit associé à l_j, $\alpha_i = \beta_j$ et $r = s$. Donc la décomposition en facteurs irréductibles est essentiellement unique. Donc A est factoriel.

b) Soit I un idéal de A, avec A euclidien de stathme v. Il existe $b \in I \setminus \{0\}$ tel que $v(b)$ soit minimal parmi les $v(i)$, $i \in I \setminus \{0\}$. Montrons que $I = (b)$. Soit $a \in I$. Alors la division euclidienne de a par b s'écrit $a = bq + r$, avec $r = 0$ ou $v(r) < v(b)$. Si $r \neq 0$, alors $r = a - bq$, donc $r \in I$ (car $a, b \in I$), et $v(r) < v(b)$. Cela contredit la minimalité de b. Donc $r = 0$, donc $a = bq$, donc $a \in (b)$. Donc $I = (b)$. Donc A est principal (A est intègre car euclidien).

c) Si k est un corps, l'anneau $A := k[X_1, X_2, \dots, X_n, \dots]$ avec une infinité de variables, est factoriel (car B factoriel implique $B[X]$ factoriel), mais il n'est pas noethérien : l'idéal $(X_n; n \geq 1)$ n'est pas engendré par un nombre fini de générateurs.

d) $A = \mathbb{Z}[i\sqrt{5}]$ est clairement intègre et noethérien. Or on a $9 = 3.3 = (2 + i\sqrt{5}).(2 - i\sqrt{5})$, et $3, 2 + i\sqrt{5}, 2 - i\sqrt{5}$ sont des éléments irréductibles de A. En effet, le module au carré d'un élément de A est un entier, et celui-ci vaut 1 si et seulement si l'élément est inversible. Or $|3|^2 = 9 = 3.3$, et l'équation $a^2 + 5b^2 = 3$ n'a pas de solution entière, donc 3 ne s'écrit pas comme un produit de deux éléments non inversibles de A. de même, $|2 \pm i\sqrt{5}|^2 = 9 = 3.3$, donc $2 \pm i\sqrt{5}$ est irréductible dans A. Montrons pour finir que 3 et $2 + i\sqrt{5}$ ne sont pas associés dans A. Les unités de A sont les éléments $a + ib\sqrt{5}$ tels que $a^2 + 5b^2 = 1$, i.e. $A^* = \{\pm 1\}$. Or $3 \neq \pm(2 + i\sqrt{5})$, donc 3 et $2 + i\sqrt{5}$ ne sont pas associés dans A. On a donc deux décompositions distinctes de 9 dans A, donc A n'est pas factoriel.

e) Si $A = \mathbb{Z}[X]$, alors A est factoriel, noethérien, non principal (l'idéal $(2, X)$ de A n'est pas principal). Si $A := \mathbb{C}[X, Y]$, alors A est factoriel noethérien, mais pas principal (l'idéal (X, Y) de A n'est pas principal).

f) i) On pose $t := \frac{a}{b} = x + y\alpha$, avec $x, y \in \mathbb{Q}$. On note $d := \mathrm{dist}(y, \mathbb{Z})$.
- Supposons $d \leq \frac{1}{3}$, et notons x_0 (resp. y_0) l'entier relatif le plus proche de x (resp. y). On pose $t_0 := x_0 + y_0\alpha \in A$. Alors on a

$$N(t - t_0)(x - x_0)^2 + 5(y - y_0)^2 \leq \frac{1}{4} + \frac{1}{36} + \frac{1}{6} + \frac{19}{4.9} = \frac{35}{36} < 1\,.$$

D'où le résultat : on a bien $a = bt_0 + r_0$, avec $t_0 \in A$ et $r_0 \in A$, tels que $r_0 = 0$ ou $N(r_0) < N(b)$.
- Supposons $d > \frac{1}{3}$. Posons $a' := 2a$, on a $\frac{a'}{b} = 2x + 2y\alpha$. On vérifie que $\mathrm{dist}(2y, \mathbb{Z}) \leq \frac{1}{3}$, donc on peut appliquer la construction précédente à a' et b. D'où le résultat.

ii) On a $A \cong \mathbb{Z}[T]/(T^2-T+5)$, donc $A/(2) \cong \mathbb{F}_2[T]/(T^2+T+1)$. Or le polynôme T^2+T+1 est irréductible que $\mathbb{F}_2$, donc $A/(2) \cong \mathbb{F}_4$, donc $A/(2)$ est un corps, donc (2) est un idéal maximal, donc premier, de A.

iii) Soit I un idéal de A, $I \neq 0, A$. Supposons que $2 \notin I$. Soit $b \in I$ non inversible, non nul, tel que $N(b)$ soit minimal. Soit $a \in I$. D'après la question f)i), soit on peut faire la division euclidienne de a par b, auquel cas $a \in (b)$; soit on peut faire la division euclidienne de $2a$ par b. Dans ce cas, $2a \in (b)$. Donc $2a = b\beta$, $\beta \in A$. Donc $b\beta \in (2)$. Or (2) est premier, donc $b \in (2)$ ou $\beta \in (2)$. Supposons que $\beta \notin (2)$. Alors il existe $b' \in A$ tel que $b = 2b'$, et $(2, \beta) = A$ (car (2) est maximal), donc $1 = 2x + \beta y$, $x, y \in A$. Donc $b' = 2xb' + \beta y b'$, donc $b' \in I$. Mais $N(b') < N(b)$, ce qui contredit la minimalité de b. Donc finalement $\beta \in (2)$, donc il existe $\gamma \in A$ tel que $\beta = 2\gamma$, donc $a = b\gamma$, donc $a \in (b)$. Finalement, on a bien montré que $I = (b)$.

iv) Si B est un corps, c'est évident (prendre $b = 0$). Sinon, on prend pour b un élément non inversible, non nul, tel que $N(b)$ soit minimal. Alors la division euclidienne par b assure que $B^* \cup \{0\}$ sur surjecte sur $B/(b)$.

v) Si $a \in A^*$, alors $N(a) \in \mathbb{Z}$ est inversible dans $\mathbb{Z}$, donc $N(a) = \pm 1$. Écrivons $a = x + y\alpha$, avec $x, y \in \mathbb{Z}$. On a $N(a) = \left(x + \frac{y}{2}\right)^2 + \frac{19}{4}y^2 = 1$, donc $y = 0$ et $x = \pm 1$, donc $a = \pm 1$. Donc $A^* = \{\pm 1\}$.

vi) On raisonne par l'absurde. Supposons qu'il existe un tel $x \in A$. On dispose alors d'un morphisme surjectif $\varphi : A \to k$, où $k = \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. En particulier, on dispose de l'élément $\overline{\alpha} := \varphi(\alpha) \in k$. Or $\alpha \in A$ vérifie $\alpha^2 - \alpha + 5 = 0$ dans A, donc le polynôme $T^2 - T + 5$ admet une racine $\overline{\alpha}$ dans k. Mais la réduction de ce polynôme de $\mathbb{Z}[X]$ modulo 2 ou 3 est irréductible, donc on a une contradiction

vii) Si A était euclidien, les questions iv) et v) assureraient que A admettrait un quotient $A/(x)$, avec $x \notin A^*$, de cardinal 2 ou 3 (car $\#A^* \cup \{0\} = 3$), ce qui contredirait la question vi). Donc A n'est pas euclidien.

g) Les cas de $\mathbb{Z}$ et $k[X]$ sont bien connus. Pour $\mathbb{Z}[i]$, il suffit de considérer le stathme euclidien $N(a+ib) := a^2+b^2$ et de vérifier que la division euclidienne "naïve" (voir question f)i)) est bien une division euclidienne.