ISM MP, Mathématiques
Année 2024/2025

Feuille d'exercices n°85

Exercice 1 (*)

Résoudre les équations d'inconnue x dans $\mathbb{Z}$:

1. $5x \equiv 3\ [6]$ 2. $3x \equiv 5\ [6]$ 3. $x^2 \equiv 1\ [8]$ 4. $x^2 \equiv -1\ [7]$

Corrigé : 1. On a $5 \equiv -1\ [6]$ d'où

$$\boxed{x \equiv -3\ [6]}$$

2. On a $$3x \equiv 5\ [6] \iff \exists k \in \mathbb{Z} \quad | \quad 3x + 6k = 5$$

ce qui est absurde puisque 3 ne divise pas 5. Ainsi

$$\boxed{\text{L'équation n'admet pas de solutions.}}$$

3. Pour $x \in \mathbb{Z}$ solution, on a nécessairement $\bar{x} \in \mathrm{U}(\mathbb{Z}/8\mathbb{Z})$. On se concentre donc sur les carrés de $\mathrm{U}(\mathbb{Z}/8\mathbb{Z})$ et on trouve

$$\bar{1}^2 = \bar{1} \qquad \bar{3}^2 = \bar{1} \qquad \bar{5}^2 = \bar{1} \qquad \bar{7}^2 = \bar{1}$$

Ainsi $$\boxed{x^2 \equiv 1\ [8] \iff x \in \mathrm{U}(\mathbb{Z}/8\mathbb{Z})}$$

4. On liste les carrés non nuls du corps $\mathbb{Z}/7\mathbb{Z}$:

$$\bar{1}^2 = \bar{1} \qquad \bar{2}^2 = \bar{4} \qquad \bar{3}^2 = \bar{2} \qquad \bar{4}^2 = \bar{2} \qquad \bar{5}^2 = \bar{4} \qquad \bar{6}^2 = \bar{1}$$

On constate que $-\bar{1}$ n'est pas un carré de $\mathbb{Z}/7\mathbb{Z}$ et par conséquent

$$\boxed{\text{L'équation n'admet pas de solution.}}$$

Exercice 2 (*)

Résoudre les équations d'inconnues x, y dans $\mathbb{Z}$:

1. $\begin{cases} 2x + 3y \equiv 4\ [13] \\ 3x + 2y \equiv 5\ [13] \end{cases}$ 2. $\begin{cases} 3x \equiv 2\ [5] \\ 5x \equiv 1\ [7] \end{cases}$ 3. $x^2 - 5y^2 = 3$

Corrigé : 1. Sans difficulté, on trouve

$$\begin{cases} 2x + 3y \equiv 4\ [13] \\ 3x + 2y \equiv 5\ [13] \end{cases} \implies \begin{cases} 5x \equiv 7\ [13] \\ 5y \equiv 2\ [13] \end{cases}$$

Avec l'algorithme d'Euclide, on obtient $1 = 2 \times 13 - 5 \times 5$ d'où $\bar{5}^{-1} = -\bar{5}$ dans $\mathbb{F}_{13}$ et par suite, l'implication réciproque étant immédiate

$$\boxed{\begin{cases} x \equiv 4\ [13] \\ y \equiv 3\ [13] \end{cases}}$$

2. On remarque que $3 \times 2 \equiv 1\ [5]$ et $5 \times 3 \equiv 1\ [7]$ (au pire, on peut appeler Bezout en renfort...). Ainsi

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

Avec l'égalité $1 = 5 \times 3 - 7 \times 2$, en s'appuyant sur l'isomorphisme d'anneaux $\pi : \mathbb{Z}/35\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, \bar{x} \mapsto (\widehat{x}, \dot{x})$, on conclut

$$\boxed{\text{L'ensemble des solutions est } \{-7 \times 2 \times 4 + 5 \times 3 \times 3 + 35k, k \in \mathbb{Z}\}.}$$

3. Soit $(x, y) \in \mathbb{Z}^2$ solution de $x^2 - 5y^2 = 3$. Il s'ensuit $x^2 \equiv 3\ [5]$. On liste les carrés non nuls du corps $\mathbb{F}_5$:

$$\bar{1}^2 = \bar{1} \qquad \bar{2}^2 = -\bar{1} \qquad \bar{3}^2 = -\bar{1} \qquad \bar{4}^2 = \bar{1}$$

On constate que $\bar{3}$ n'est pas un carré de $\mathbb{F}_5$ et par conséquent

$$\boxed{\text{L'équation n'admet pas de solutions.}}$$

Exercice 3 (*)

A-t-on $\overline{18} \in \mathrm{U}(\mathbb{Z}/49\mathbb{Z})$? Si oui, préciser son inverse.

Corrigé : On a $18 \wedge 49 = 1$ d'où $\overline{18} \in \mathrm{U}(\mathbb{Z}/49\mathbb{Z})$. On trouve avec l'algorithme d'Euclide

$$49 = 18 \times 2 + 13 \qquad 18 = 13 \times 1 + 5 \qquad 13 = 5 \times 2 + 3 \qquad 5 = 3 \times 1 + 2 \qquad 3 = 2 \times 1 + 1$$

Puis on remonte les calculs en partant de 1 et on trouve

$$\begin{aligned} 1 &= 3 - 2 = 3 - 2(5 - 3) = 2 \times 3 - 5 = 2(13 - 5 \times 2) - 5 = 2 \times 13 - 5 \times 5 \\ &= 2 \times 13 - 5 \times (18 - 13) = 7 \times 13 - 5 \times 18 = 7(49 - 18 \times 2) - 5 \times 18 \\ 1 &= 7 \times 49 - 19 \times 18 \end{aligned}$$

Ainsi $$\boxed{\overline{18} \in \mathrm{U}(\mathbb{Z}/49\mathbb{Z}) \quad \text{et} \quad \overline{18}^{-1} \equiv -\overline{19}\ [49]}$$

Exercice 4 (*)

Résoudre dans $\mathbb{Z}/37\mathbb{Z}$ le système $$\begin{cases} \bar{6}x + \bar{7}y = \bar{0} \\ \bar{6}x - \bar{7}y = \overline{30} \end{cases}$$

Corrigé : L'entier 37 étant premier, on a dans le corps $\mathbb{F}_{37}$

$$\begin{cases} \bar{6}x + \bar{7}y = \bar{0} \\ \bar{6}x - \bar{7}y = \bar{30} \end{cases} \iff \begin{cases} \overline{12}x = \overline{30} \\ \overline{14}y = -\overline{30} \end{cases}$$

En effet, l'implication directe s'obtient en effectuant $\mathrm{L}_1 + \mathrm{L}_2$, $\mathrm{L}_1 - \mathrm{L}_2$ et l'implication directe avec $\bar{2}^{-1}(\mathrm{L}'_1 + \mathrm{L}'_2)$, $\bar{2}^{-1}(\mathrm{L}'_1 - \mathrm{L}'_2)$. Sans difficulté, on a

$$\overline{12}x = \overline{30} \iff -3 \times \overline{12}x = -3 \times \overline{30} \iff x = \overline{21}$$

Pour résoudre $\overline{14}y = -\overline{30}$, c'est moins évident. On utilise l'algorithme d'Euclide. On a

$$37 = 14 \times 2 + 9 \qquad 14 = 9 \times 1 + 5 \qquad 9 = 5 \times 1 + 4 \qquad 5 = 4 \times 1 + 1$$

d'où $\quad 1 = 5 - 4 \times 1 \qquad 4 = 9 - 5 \times 1 \qquad 5 = 14 - 9 \times 1 \quad$ et $\quad 9 = 37 - 14 \times 2$

et

$$1 = (14 - 9 \times 1) - (9 - 5 \times 1) \times 1 = (14 - (37 - 14 \times 2)) - (37 - 14 \times 2 - (14 - (37 - 14 \times 2) \times 1) \times 1$$

d'où $$1 = -3 \times 37 + 8 \times 14$$

Ainsi $$\overline{14}y = -\overline{30} \iff \overline{14}y = \bar{7} \iff 8 \times \overline{14}y = 8 \times \bar{7} \iff \overline{y} = \overline{19}$$

On conclut $$\boxed{\begin{cases} \bar{6}x + \bar{7}y = \bar{0} \\ \bar{6}x - \bar{7}y = \overline{30} \end{cases} \iff (x, y) = (\overline{21}, \overline{19})}$$

Exercice 5 (*)

Soient m et n deux entiers non nuls non premiers entre eux. Les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ sont-ils isomorphes ?

Corrigé : Soit $(\widehat{x}, \dot{y}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. On a $(m \vee n)(\widehat{x}, \dot{y}) = (\widehat{0}, \dot{0})$ avec $m \vee n < mn$ puisque $(m \vee n)(m \wedge n) = mn$. Alors, aucun élément de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ n'est d'ordre mn alors que le groupe $(\mathbb{Z}/mn\mathbb{Z}, +)$ est cyclique et admet un tel élément. On conclut

$$\boxed{\text{Les anneaux } \mathbb{Z}/mn\mathbb{Z} \text{ et } \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{ ne sont pas isomorphes.}}$$

Variante : Soit $\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ un morphisme d'anneaux. On a $\varphi(\bar{1}) = (\widehat{1}, \dot{1})$ et

$$\forall k \in \mathbb{Z} \qquad \varphi(\bar{k}) = \varphi(k\bar{1}) = k\varphi(\bar{1}) = k(\widehat{1}, \dot{1}) = (\widehat{k}, \dot{k})$$

Par conséquent $$\varphi(\overline{m \vee n}) = (\widehat{0}, \dot{0}) \quad \text{et} \quad \overline{m \vee n} \neq \bar{0}$$

puisqu'on a $m \vee n \in [\![1 ; mn - 1]\!]$. On retrouve le fait qu'un tel morphisme d'anneaux (qui est unique) n'est pas bijectif.

Exercice 6 (**)

Pour n entier non nul, on note $\tau(n)$ le nombre de diviseurs de n.

1. Déterminer une expression de $\tau(n)$ pour $n \geqslant 2$.
2. Montrer que si m et n sont deux entiers premiers entre eux, alors $\tau(mn) = \tau(m)\tau(n)$.

Corrigé : 1. Soit n entier $\geqslant 2$. Notons $\mathcal{D}_n$ l'ensemble des diviseurs de n. Pour $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls, on a

$$\mathcal{D}_n = \left\{ \prod_{i=1}^{r} p_i^{\beta_i}, \forall i \in [\![1 ; r]\!] \quad \beta_i \in [\![0 ; \alpha_i]\!] \right\}$$

Ainsi $$\boxed{\forall n \geqslant 2 \qquad \tau(n) = \prod_{i=1}^{r} \text{Card}\, [\![0 ; \alpha_i]\!] = \prod_{i=1}^{r} (\alpha_i + 1)}$$

Remarque : On peut aussi écrire

$$\forall n \in \mathbb{N}^* \qquad \tau(n) = \prod_{p \in \mathcal{P}} (1 + v_p(n))$$

2. Soient m et n des entiers premiers entre eux. Ils n'ont aucun facteur premier en commun. On peut donc écrire $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ et $n = \prod_{i=r+1}^{q} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls. Par suite

$$\boxed{\tau(mn) = \prod_{i=1}^{q} (\alpha_i + 1) = \prod_{i=1}^{r} (\alpha_i + 1) \times \prod_{i=r+1}^{q} (\alpha_i + 1) = \tau(m)\tau(n)}$$

Exercice 7 (**)

Soit n entier avec $n \geqslant 2$. Montrer que n ne divise pas $2^n - 1$.

Corrigé : Supposons $n|2^n - 1$. Soit p le plus petit facteur premier de n. On a clairement p impair puisque $2^n - 1$ est impair. Puis, on trouve $2^n \equiv 1\ [p]$. Ainsi, dans $\mathrm{U}(\mathbb{Z}/p\mathbb{Z})$, on a $o(\bar{2})|n$ et comme $\varphi(p) = p - 1$, on a aussi $o(\bar{2})|p - 1$. Or, l'entier p est le plus petit facteur premier de n d'où $o(\bar{2}) = 1$ ce qui signifie $2 \equiv 1\ [p]$ et qui est absurde. Ainsi

$$\boxed{\text{Pour } n \geqslant 2, \text{ l'entier } n \text{ ne divise pas } 2^n - 1.}$$

Exercice 8 (**)

Déterminer les nilpotents de $\mathbb{Z}/n\mathbb{Z}$ avec n entier non nul.

Corrigé : On a $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls. Soit $x \in \mathbb{Z}$ tel que $\bar{x}$ est un nilpotent de $\mathbb{Z}/n\mathbb{Z}$, *i.e.* il existe N entier non nul tel que

$$x^{\mathrm{N}} \equiv 0\ [n]$$

Par suite $$\forall i \in [\![1\,;\, r]\!] \qquad p_i | x$$

et les p_i étant premiers distincts, on en déduit

$$x \in \left(\prod_{i=1}^{r} p_i \right) \mathbb{Z}$$

Réciproquement, soit $x \in \left(\prod_{i=1}^{r} p_i \right) \mathbb{Z}$. Avec $\alpha = \underset{i \in [\![1\,;\, n]\!]}{\mathrm{Max}} \alpha_i$, on a $n|x^\alpha$ d'où $x^\alpha \equiv 0\ [n]$ ce qui prouve que $\bar{x}$ est nilpotent. On conclut

$$\boxed{\text{L'ensemble des nilpotents de } \mathbb{Z}/n\mathbb{Z} \text{ est l'idéal } \left(\prod_{i=1}^{r} p_i \right) \mathbb{Z}/n\mathbb{Z}.}$$

Exercice 9 (**)

Soit n entier non nul. Déterminer $\sum_{d|n} \varphi(d)$.

Corrigé : On a $$[\![1\,;\, n]\!] = \bigsqcup_{d|n} \{k \in [\![1\,;\, n]\!] \mid k \wedge n = d\}$$

Par ailleurs, pour $d|n$, on a

$$k \wedge n = d \iff \exists !(k', n') \in \mathbb{Z}^2 \quad | \quad k = k'd \qquad n = n'd \quad \text{et} \quad k' \wedge n' = 1$$

Comme n est entier non nul, alors n' l'est également. Ainsi, on peut mettre en bijection $k \in [\![1\,;\, n]\!]$ vérifiant $k \wedge n = d$ avec $k' \in [\![1\,;\, n']\!]$ vérifiant $k' \wedge n' = 1$. Il s'ensuit

$$\mathrm{Card}\ \{k \in [\![1\,;\, n]\!] \mid k \wedge n = d\} = \mathrm{Card}\ \{k' \in [\![1\,;\, n']\!] \mid k' \wedge n' = 1\} = \varphi(n')$$

Comme il s'agit d'union disjointe, on obtient

$$\mathrm{Card}\, [\![1\,;\, n]\!] = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$$

et comme l'application $d \mapsto \dfrac{n}{d}$ réalise une permutation de l'ensemble des diviseurs de n (involutive), on conclut

$$\boxed{\forall n \in \mathbb{N}^* \qquad \sum_{d|n} \varphi(d) = n}$$

Variante : Notons $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls. L'ensemble $\mathcal{D}_n$ des diviseurs de n est

$$\mathcal{D}_n = \left\{ \prod_{i=1}^{r} p_i^{\beta_i}, \forall i \in [\![1\,;\, r]\!] \quad \beta_i \in [\![0\,;\, \alpha_i]\!] \right\}$$

Par suite, on a

$$\sum_{d|n} \varphi(d) = \sum_{(\beta_i)_{i \in [\![1\,;\, r]\!]} \in \prod_{i=1}^{r} [\![0\,;\, \alpha_i]\!]} \varphi\left(\prod_{i=1}^{r} p_i^{\beta_i} \right)$$

D'après le caractère multiplicatif de la fonction φ puis séparations des variables, il vient

$$\sum_{d|n} \varphi(d) = \sum_{(\beta_i)_{i \in [\![1\,;\, r]\!]} \in \prod_{i=1}^{r} [\![0\,;\, \alpha_i]\!]} \prod_{i=1}^{r} \varphi\left(p_i^{\beta_i} \right) = \prod_{i=1}^{r} \sum_{\beta_i=0}^{\alpha_i} \varphi(p_i^{\beta_i}) = \prod_{i=1}^{r} \left(1 + \sum_{\beta_i=1}^{\alpha_i} \left[p_i^{\beta_i} - p_i^{\beta_i - 1} \right] \right)$$

Par téléscopage, on retrouve

$$\boxed{\sum_{d|n} \varphi(d) = \prod_{i=1}^{r} p_i^{\alpha_i} = n}$$

Exercice 10 (**)

Soit n un entier impair non multiple de 5. Montrer qu'il existe un multiple positif de n dont l'écriture décimale est constituée de 1.

Corrigé : Supposons le problème résolu. Cela signifie qu'il existe k et N entiers non nuls tels que

$$kn = \sum_{i=0}^{\mathrm{N}-1} 10^i = \frac{10^{\mathrm{N}} - 1}{10 - 1} \iff 9kn + 1 = 10^{\mathrm{N}}$$

Comme n est impair et non multiple de 5, on a $10 \wedge n = 1$ et aussi $10 \wedge 9 = 1$ d'où $\overline{10} \in \mathrm{U}\left(\mathbb{Z}/9n\mathbb{Z}\right)$. Ainsi, prenant $\mathrm{N} = o(\overline{10})$ l'ordre de $\overline{10}$ dans $\mathrm{U}\left(\mathbb{Z}/9n\mathbb{Z}\right)$, on a bien $10^{\mathrm{N}} \equiv 1\ [9n]$, autrement dit on dispose de $k \in \mathbb{Z}$ tel que

$$10^{\mathrm{N}} = 1 + 9kn$$

Il est clair que k est strictement positif et on conclut

$$\boxed{\exists k \in \mathbb{N}^* \quad | \quad kn = \sum_{i=1}^{\mathrm{N}-1} 10^i}$$

Exercice 11 (**)

1. Soit $\mathrm{P} = \sum_{k=0}^{n} a_k \mathrm{X}^k \in \mathbb{Z}[\mathrm{X}]$ avec $a_0 \neq 0$ et $a_n \neq 0$. On suppose que P admet une racine rationnelle $r = \dfrac{p}{q}$ écrite sous forme irréductible. Montrer

$$p | a_0 \quad \text{et} \quad q | a_n$$

2. Le polynôme $\mathrm{P} = \mathrm{X}^3 + 3\mathrm{X} - 1$ est-il irréductible dans $\mathbb{Q}[\mathrm{X}]$?

Corrigé : 1. On a $\mathrm{P}(r) = 0 \iff \sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k = 0 \iff \sum_{k=0}^{n} a_k p^k q^{n-k} = 0$

Ainsi $$a_0 q^n = p\sum_{k=1}^{n} a_k p^{k-1} q^{n-k} \quad \text{et} \quad a_n p^n = q\sum_{k=0}^{n-1} a_k p^k q^{n-1-k}$$

On a $p \wedge q = 1$ d'où $p \wedge q^n = 1$ et $q \wedge p^n = 1$. Ainsi, d'après le théorème de Gauss, on conclut

$$\boxed{p|a_0 \quad \text{et} \quad q|a_n}$$

2. Si P n'est pas irréductible, il admet nécessairement un diviseur dans $\mathbb{Q}[\mathrm{X}]$ de degré égal à 1 ce qui implique que P admet une racine rationnelle. D'après le critère précédemment établi, si on dispose d'une racine rationnelle $r = p/q$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$, alors $p| - 1$ et $q|1$ d'où $r = \pm 1$. Or, ni 1, ni -1 n'est racine de P. On conclut

$$\boxed{\text{Le polynôme P est irréductible dans } \mathbb{Q}[\mathrm{X}].}$$

Exercice 12 (**)

Soit p un nombre premier impair. Dans $\mathbb{F}_p$, déterminer $\sum_{k=1}^{p-1} \bar{k}^{-1}$.

Corrigé : L'application $\mathbb{F}_p^* \to \mathbb{F}_p^*, x \mapsto x^{-1}$ est une permutation. Par conséquent, on a

$$\sum_{k=1}^{p-1} \bar{k}^{-1} = \sum_{k=1}^{p-1} \bar{k} \quad \text{et} \quad \sum_{k=1}^{p-1} k = \frac{p(p-1)}{2} \equiv 0 \ [p]$$

puisque $2|p - 1$. Ainsi

$$\boxed{\sum_{k=1}^{p-1} \bar{k}^{-1} = \bar{0}}$$

Exercice 13 (**)

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

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.