**39** Montrer que 419 est un nombre premier.
On expliquera clairement la méthode utilisée.

**41** Soit $n \in \mathbb{N}$. On pose $N = 2n^2 + n - 10$.
**1.** Factoriser $N$ par $(n - 2)$.
**2.** Pour quelle valeur de $n$, le nombre $N$ est-il premier ?

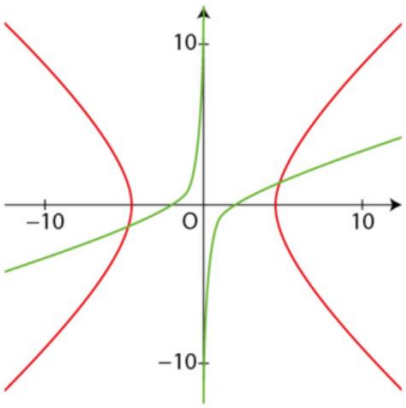
**48** Soit un entier relatif $n$ tel que : $n^2 = 17p + 1$ où $p$ est un nombre premier.
**1.** Écrire $17p$ comme un produit de facteurs fonction de $n$.
**2.** Montrer que $n$ est de la forme :
$n = 17k + 1$ ou $n = 17k - 1$ avec $k \in \mathbb{Z}$
On citera le théorème utilisé.
**3.** Montrer qu'une seule valeur de $k$ convient.
En déduire les valeurs de $n$ et $p$

**39** $p$ désigne un nombre premier.
$P = 2 \times 3 \times 5 \times \ldots \times p$ est le produit des nombres entiers naturels premiers inférieurs ou égaux à $p$.
**a)** Démontrer que les $(p-1)$ nombres entiers naturels consécutifs $P+2, P+3, \ldots, P+p$ ne sont pas premiers.
**b)** Donner un exemple de dix nombres entiers naturels consécutifs non premiers.

**52** **1.** Décomposer en produit de facteurs premiers 2 650 et 1 272.
**2.** En déduire PGCD(2 650 , 1 272).
**3.** Retrouver ce résultat à l'aide de l'algorithme d'Euclide puis comparer les deux méthodes.

**54** **1.** Quelle est la condition sur les puissances des facteurs premiers d'un carré parfait ?
**2.** Trouver un nombre de trois chiffres qui soit un carré parfait divisible par 56.

**60** Dans le repère ci-dessous, la courbe rouge a pour équation $x^2 - y^2 = 21$ et la courbe verte a pour équation $x(2x - 6y) = 8$.




**a)** Déterminer les points à coordonnées entières appartenant à :
- la courbe rouge ;
- la courbe verte.

**b)** Les points d'intersection de ces courbes sont-ils à coordonnées entières ?

**63** **1. a)** Vérifier que $M_{13} = 2^{13} - 1$ est premier.
**b)** En déduire que $2^{12}M_{13}$ est parfait.
**2.** Démontrer la propriété d'Euclide :
Pour tout entier naturel $n \geqslant 1$, si $M_n = 2^n - 1$ est premier, alors $N = 2^{n-1}M_n$ est parfait.

Dire qu'un nombre entier naturel $n$ est parfait signifie que la somme de ses diviseurs stricts est égale à $n$.

**63** Démontrer qu'un entier naturel $n$ est un carré parfait si, et seulement si, le nombre de ses diviseurs est impair.

## 128 Problème de lampes

On considère 1 000 lampes numérotées de 1 à 1 000 qui peuvent être allumées ou éteintes. Une lampe change d'état lorsqu'elle passe d'éteinte à allumée et réciproquement. Au départ toutes les lampes sont éteintes et l'on effectue les 1 000 étapes suivantes.

**Étape 1** On allume toutes les lampes.
**Étape 2** Seules les lampes où le numéro est multiple de 2 changent d'état.
**Étape 3** Seules les lampes où le numéro est multiple de 3 changent d'état.
Ainsi de suite jusqu'à :
**Étape 1 000** Seules les lampes où le numéro est multiple de 1 000 changent d'état.
Quels sont les numéros des lampes qui sont allumées après ces 1 000 étapes ?

**65** $\alpha$ et $\beta$ sont deux nombres entiers naturels non nuls tels que $n = 2^\alpha 3^\beta$.
Le nombre de diviseurs positifs de $n^2$ est le triple de celui de $n$.
**a)** Prouver que $(\alpha - 1)(\beta - 1) = 3$.
**b)** Quelles sont les valeurs possibles de $n$ ?

**65** Le produit de deux entiers naturels $a$ et $b$ avec $a < b$ est 11 340. On note $d = \text{PGCD}(a, b)$.
**1. a)** Pourquoi $d^2$ divise-t-il 11 340 ?
**b)** Pourquoi $d = 2^\alpha \times 3^\beta$ avec $0 \leqslant \alpha \leqslant 1$ et $0 \leqslant \beta \leqslant 2$ ?
**2.** On sait de plus que $a$ et $b$ ont six diviseurs communs et $a$ est un multiple de 5.
**a)** Démontrer que $d = 18$.
**b)** En déduire $a$ et $b$.

**66** **1.** Montrer que $4^{28} - 1$ est divisible par 29.
**2.** Montrer que pour tout $n$, $4^n - 1$ est divisible par 3.
**3.** Montrer que pour tout $k$, $4^{4k} - 1$ est divisible par 5 et par 17.
**4.** En déduire quatre diviseurs premiers de $4^{28} - 1$.

**67** Soit $n \in \mathbb{N}^*$. On note $a = n^{13} - n$.
**1.** Montrer que $a$ est divible par 13 et 7.
**2.** En déduire que $a$ est divisible par 182.

**69** **1.** Soit $p$ un nombre premier supérieur à 2.
Montrer que $p$ divise $1 + 2 + 2^2 + \ldots + 2^{p-2}$.
**2.** Est-ce que 97 divise la somme $S$ telle que

$$S = \sum_{n=1}^{98} n^{96} ?$$

**83** On donne $n = pq$ avec $p$ et $q$ des nombres premiers tels que $p \neq 2$, $q \neq 2$ et $p \neq q$.
$a$ est un nombre entier naturel qui n'est ni divisible par $p$ ni par $q$.
**a)** Justifier que :

$$\left(a^{p-1}\right)^{\frac{q-1}{2}} \equiv 1\ [p] \text{ et } \left(a^{q-1}\right)^{\frac{p-1}{2}} \equiv 1\ [q].$$

**b)** En déduire que $a^{\frac{(p-1)(q-1)}{2}} \equiv 1\ [pq]$.
**2.** Démontrer que $a^{(p-1)(q-1)} \equiv 1\ [pq]$.

**106** On se propose de coder le nom « FERMAT » de la façon suivante :
• à chaque entier $x$ compris entre 0 et 30, on lui associe une lettre de l'alphabet français ou un symbole (A : 0, B : 1, …, Z : 25, α : 26, β : 27, γ : 28, δ : 29, ε : 30) ;
• on calcule le reste $y$ de la division euclidienne de $x^7$ par 31 ;
• on fait correspondre à $y$ l'un des symboles précédents.
**Exemple**
La première lettre F est associée à 5.
Ainsi $5^7 \equiv 5\ [31]$ donc $y = 5$ et F est codée F.
**1.** Coder le mot FERMAT.
**2.** Montrer que 7 et 30 sont premiers entre eux et écrire l'égalité de Bézout correspondante.
**3.** Démontrer que deux lettres distinctes sont codées par deux lettres distinctes.
**4. a)** Démontrer que $y \equiv x^7\ [31]$ équivaut à $x \equiv y^{13}\ [31]$.
**b)** Décoder le mot XCQMMQ.

**81** Soit $q > 5$, un nombre premier et $M$ le produit des nombres premiers de 5 à $q$ :

$$M = 5 \times 7 \times 11 \times \ldots \times q.$$

On pose : $N = 2^2 \times M + 3$.
**1. a)** Montrer que $N$ est impair.
**b)** Montrer que $N \not\equiv 0\ (3)$.
**2.** Soit $p$ un nombre premier divisant $N$.
**a)** Montrer que $p > q$.
**b)** Montrer que : $p \equiv 1\ (4)$ ou $p \equiv 3\ (4)$.
**3.** Soit $N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ la décomposition de $N$ en facteurs premiers.
**a)** Montrer en raisonnant par l'absurde qu'il existe un facteur premier $p_i$ avec $i \in [\![1 ; r]\!]$ tel que : $p_i \equiv 3\ (4)$.
**b)** En déduire qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

**94** Le but de cet exercice est de trouver tous les entiers relatifs $x$ solutions de

$$(E) : x^2 - 2x + 2 \equiv 0\ (17)$$

**1.** Montrer que $\alpha = 5$ est une solution de (E).
**2.** On pose $X = x - \alpha$, trouver alors toutes les solutions de (E).

**95** **1.** Montrer que pour tous réels $x$ et $y$, on a :

$$x^3 - y^3 = (x - y)(x^2 + xy + y^2).$$

**2.** Résoudre alors dans $\mathbb{N}^2$ l'équation :

$$x^3 - y^3 = 127.$$

**130 Le théorème de Wilson** Démo
Soit un nombre premier $p > 3$ et l'ensemble des naturels $A = [2 ; p - 2]$.
**1.** Montrer que pour tout $x \in A$, $p$ ne divise pas $x^2 - 1$.
**2. a)** Soit $x \in A$, montrer qu'il existe $u \in \mathbb{Z}$ tel que : $xu \equiv 1\ (p)$.
**b)** En déduire l'existence d'un unique entier $r \in A$ distinct de $x$ tel que $xr \equiv 1\ (p)$.
**c)** Établir que : $2 \times 3 \times \ldots \times (p-2) \equiv 1\ (p)$ puis que $(p-1)! \equiv -1\ (p)$.
**3.** Ce résultat est-il encore vrai pour $p = 2$ et $p = 3$ ?
**4.** Réciproquement, soit $p$ un entier ($p \geqslant 2$) tel que : $(p-1) \equiv -1\ (p)$.
En raisonnant par l'absurde, montrer que $p$ est premier.
**5.** En déduire le théorème de Wilson : « Un entier naturel $n$ est premier si, et seulement si, $(n-1)! + 1$ est divisible par $n$ ».
**6.** Application : montrer que 13 est premier à l'aide du théorème de Wilson.
Ce théorème est-il judicieux comme test de primalité ?

**107** $p$ désigne un nombre premier.
Dire que $-1$ est un résidu quadratique modulo $p$ signifie qu'il existe un nombre entier $x$ tel que $x^2 \equiv -1\ [p]$.
**1.** Montrer que $-1$ est un résidu quadratique modulo 2.
**2.** On suppose que $p \equiv 3\ [4]$ et qu'il existe un entier $x$ tel que $x^2 \equiv -1\ [p]$.
**a)** En remarquant que $x^{p-1} = \left(x^2\right)^{\frac{p-1}{2}}$, montrer que :

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}}\ [p].$$

**b)** Quelle est la parité de $\frac{p-1}{2}$ ?
En utilisant le petit théorème de Fermat, montrer que :

$$1 \equiv -1\ [p].$$

**c)** En déduire que $p = 2$ et conclure.
**3.** On suppose que $p \equiv 1\ [4]$ et on admet le théorème de Wilson : si $p$ est premier alors $(p-1)! \equiv -1\ [p]$.
**a)** Vérifier que :

$$\left(p - \frac{p-1}{2}\right) \times \ldots \times (p-1) \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!\ [p]$$

**b)** En écrivant

$$(p-1)! = 1 \times 2 \times \ldots \times \frac{p-1}{2} \times \left(p - \frac{p-1}{2}\right) \times \ldots \times (p-1)$$

montrer que $(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2\ [p]$,
puis que $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1\ [p]$.
**c)** Que peut-on conclure ?
**3.** $-1$ est-il un résidu quadratique modulo 157 ?

## 124 Le chiffrement RSA

### 1. Établir une propriété fondamentale

$n = pq$ est le produit de deux nombres premiers $p$ et $q$ distincts.
On pose $m = (p-1)(q-1)$ et on note $c$ un nombre premier avec $m$.
On note $x$ un entier naturel.

**a)** Démontrer qu'il existe des entiers $d$ et $k$ tels que :

$$cd = km + 1 \text{ (c'est-à-dire } cd \equiv 1\ [m]).$$

**b)** • **Cas où $x$ est non divisible par $p$**

Démontrer que $x^{p-1} \equiv 1\ [p]$.
En déduire que $x^{km} \equiv 1\ [p]$, puis que $x^{cd} \equiv x\ [p]$.

• **Cas où $x$ est divisible par $p$**

Démontrer que $x^{cd} \equiv x\ [p]$.

**c)** Démontrer de façon analogue que pour tout entier naturel $x$, $x^{cd} \equiv x\ [q]$.

**d)** En déduire que pour tout entier naturel $x$, $x^{cd} \equiv x\ [n]$.

**HISTOIRE DES MATHS**

Les trois lettres RSA sont les initiales de Rivest, Shamir, Adleman qui ont mis au point ce procédé en 1978.

Le système RSA 1 024 bits correspond à un nombre $n = pq$ de l'ordre de $2^{1024} \approx 10^{308}$ s'écrivant avec 309 chiffres.

**Principe**

• Pour chiffrer un message (cartes bancaires, internet, …), on choisit deux nombres premiers $p$ et $q$ distincts très grands et on calcule $n = pq$.
On pose $m = (p-1)(q-1)$.
On cherche deux nombres entiers naturels $c$ et $d$ tels que $cd \equiv 1\ [m]$.

• Les messages $x$ seront des entiers naturels appartenant à $\{0\,;1\,;\ldots\,;n-1\}$.
Le codage de ce message consiste à calculer $C(x) \equiv x^c\ [n]$.
Le décodage consiste à calculer $D(y) \equiv y^d\ [n]$.
On a bien $D(C(x)) \equiv x^{cd} \equiv x\ [n]$.

• Pour chiffrer un message on a besoin de connaître $c$ et $n$.
Le couple $(c\,;n)$ est appelé la **clé publique** car elle est connue de tous et répertoriée dans un annuaire.

• Pour déchiffrer, il faut connaître $d$ et $n$.
$d$ est appelée la **clé privée** car elle n'est connue que de la personne qui reçoit le message codé.

### 2. Application 1

Alex veut choisir une clé publique $(n\,;c)$ et sa clé privée $d$.
Il prend $p = 5$, $q = 11$ et donc $n = 55$ ($p$ et $q$ sont choisis petits, contrairement à la réalité, pour la simplicité des calculs).

**a)** Démontrer qu'il peut choisir $c = 3$ et $d = 27$.

**b)** Les lettres de l'alphabet sont chiffrées par A : 01, B : 02, …, Z : 26.
Paula, qui connaît la clé publique d'Alex, crypte le message :
« VIVE LA CRYPTOGRAPHIE » et lui envoie.
Quel message crypté Alex reçoit-il ?
Comment le décode-t-il ?

### 3. Application 2

Lise a pour clé publique $(n\,;c)$ avec $n = pq$, $p = 3$, $q = 13$.

**a)** Démontrer qu'elle peut choisir $c = 29$ et $d = 5$.

**b)** Elle reçoit le message crypté suivant de Félix : 28 01 12 21 11 12 03 28 05.
Décrypter ce message.

## 128 Les entiers de Gauss

On note $\mathbb{Z}[i]$ l'ensemble des entiers de Gauss, c'est-à-dire des nombres complexes $a+ib$ où $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.
La norme de $z = a+ib$ $(a \in \mathbb{Z}, b \in \mathbb{Z})$ est l'entier $N(z) = a^2 + b^2$.
Dire que $w$ divise $z$ dans $\mathbb{Z}[i]$ signifie qu'il existe un élément $v$ de $\mathbb{Z}[i]$ tel que $z = vw$.

**1. a)** Montrer que $4+5i$ divise $14-3i$ mais ne divise pas $14+3i$.
**b)** Vérifier que $N(4+5i)$ divise $N(14-3i)$ dans $\mathbb{Z}$.

**2. a)** Démontrer que pour tous $z$ et $z'$ de $\mathbb{Z}[i]$, $N(zz') = N(z)N(z')$.
**b)** En déduire que si $z$ divise $z'$ dans $\mathbb{Z}[i]$, alors $N(z)$ divise $N(z')$ dans $\mathbb{Z}$.
La réciproque est-elle vraie ?

**3.** Déterminer les entiers de Gauss de norme égale à 1. On les appelle « unités de $\mathbb{Z}[i]$ ».

**4.** Dire qu'un élément $z$ de $\mathbb{Z}[i]$ est entier de Gauss premier signifie que $z$ n'est pas une unité et que les seuls diviseurs de $z$ dans $\mathbb{Z}[i]$ sont les unités et les produits de $z$ par une unité.
**a)** Justifier que 2 n'est pas entier de Gauss premier et que 3 l'est.
**b)** $p$ est un nombre premier dans $\mathbb{Z}$. On suppose qu'il n'existe pas $a$ et $b$ dans $\mathbb{N}$ tels que $p = a^2 + b^2$.
Démontrer que $p$ est un entier de Gauss premier.
**c)** Démontrer que si $N(z)$ est premier dans $\mathbb{Z}$, alors $z$ est un entier de Gauss premier.
La réciproque est-elle vraie ?