Algèbre et Arithmétique 1

Feuille n^o 4 : nombres premiers

Exercices à savoir faire

Exercice 1

Les entiers suivants sont-ils premiers 211, 287 et 561 ?

Exercice 2

1. Montrer que 59 est premier.
2. Résoudre sur $\mathbb{Z}$, l'équation $x^2 + 59 = y^2$.
3. Résoudre sur $\mathbb{Z}$, l'équation $x^2 + 6x = y^2 + 50$.

Exercice 3

On appelle nombres premiers jumeaux, deux nombres premiers qui comme 11 et 13, diffèrent de 2. À l'aide du crible d'Ératosthène, déterminer deux nombres premiers jumeaux, compris entre 200 et 250.

Exercice 4

Soit p un nombre premier strictement plus grand que 3. Montrer que $p-1$ ou $p-5$ est divisible par 6.

Exercice 5

Soit p un nombre premier. Quels sont les restes possibles de la division Euclidienne de p par 4 ? Par 6 ? En déduire que si $p \geqslant 5$ alors 24 divise $p^2 - 1$.

Exercice 6

1. Montrer que si p et $8p-1$ sont premiers alors $8p+1$ est composé.
2. Montrer que si est p premier et différent de 3 alors $8p^2+1$ est composé. On pourra utiliser une congruence modulo 3.

Exercice 7

Soit $n = 792$. Trouver le plus entier naturel p tel que np soit le carré d'un entier.

Exercice 8

Décomposer 1536, 1001, 1155 en facteurs premiers. Calculer le pgcd de 1536 et 1001, puis de 1001, 1155, et enfin de 1155 et 1536.

Pour les 4 exos qui suivent, diviseurs signifient diviseurs positifs.

Exercice 9

Trouver tous les entiers m dont la décomposition en facteurs premiers est de la forme $2^x 3^y 5^2$ et qui ont 12 diviseurs.

Exercice 10

Trouver le plus petit entier qui possède 24 diviseurs.

Exercice 11

1. Montrer que le nombre de diviseur d'un carré est impair.
2. Inversement, montrer que si le nombre de diviseur d'un nombre est impair alors celui-ci est un carré.

Exercice 12

Combien 15! possède-t-il de diviseurs ? *On pourra commencer par factoriser* 15! *en produit de nombres premiers.*

Exercice 13

Soit p un nombre premier impair.

1. Montrer que p est congru à 1 ou -1 modulo 4.
2. Donner deux exemples de chaque cas.
3. Soit N un nombre congru à -1 modulo 4, montrer que l'un des facteurs premiers de N est congru à -1 modulo 4.
4. En déduire qu'il existe une infinité de nombres premiers congrus à -1 modulo 4. On pourra utiliser le nombre $N = 4 \cdot 3 \cdot 5 \cdot 7 \cdots p - 1$ où p est un nombre premier.

Exercice 14

Montrer que pour tout entier $n \in \mathbb{N}$, on a 42 divise $n^7 - n$.

Exercice 15

1. Décomposer 546 en facteurs premiers.
2. Montrer que $a^{13} - a$ est divisible par $a^6 - 1$ et $a^6 + 1$.
3. Démontrer que $a^{13} - a$ est divisible par 546 quelque soit $a \in \mathbb{N}$.

Exercice 16

On veut montrer le théorème de Wilson :

Soit p un entier supérieur ou égale à 2 ; p est premier si et seulement si p divise $(p-1)! + 1$.

1. Montrer que si $p = ab$ avec $1 < a < b < p$ alors p divise $(p-1)!$.
2. Montrer que si $p = a^2$ alors p divise $(p-1)!$.
3. En déduire, le « sens facile » du théorème de Wilson.
4. Supposons à présent p premier. Montrer que pour tout $a \in \{1, \ldots, p-1\}$, il existe un unique $u \in \{1, \ldots, p-1\}$ tel que $au \equiv 1 \quad [p]$.
5. Montrer que $a = u$ si et seulement si $a = 1$ ou -1.
6. En déduire que $(p-1)! \equiv -1 \quad [p]$

Exercices pour aller plus loin

Exercice 17

1. Trouver tous les nombres x tel que 13 divise $x^2 + x + 1$. On commencera par remarquer que 3 répond à la question.
2. Trouver tous les nombres x tel que 17 divise $x^2 - 2x + 2$. On commencera par remarquer que 5 répond à la question.

Exercice 18

Soient $p_1, ..., p_n$ les n premiers nombres premier. On pose $a = p_1 p_2 \cdots p_n$ et $N = a^2 + 1$. Soit q un diviseur premier de N.

1. Soit b un entier. Montrer que $(b^2 + 1) \wedge (b + 1) = (b^2 + 1) \wedge (b - 1) = 1$ ou 2.
2. Montrer que q est différent de 2.
3. Montrer que $a \not\equiv 1$ ou -1 $[q]$.
4. Montrer que $a^2 \equiv -1$ $[q]$.

5. Montrer que la suite a^l modulo $[q]$ pour tout $l \in \mathbb{N}$ est périodique de période 4. Attention, il faut bien montrer que la période est exactement 4.
6. Montrer que $a^{q-1} \equiv 1\ [q]$.
7. En déduire que q est congru à 1 modulo 4.
8. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Exercice 19

1. Soient a, b des entiers avec $a \geqslant b$. On note r le reste de la division euclidienne de a par b. Montrer que le reste de la division euclidienne de $2^a - 1$ par $2^b - 1$ est $2^r - 1$.
2. En déduire que si $2^n - 1$ est premier alors n est premier.

Exercice 20

On introduit la fonction $\sigma(x)$ la somme des diviseurs (positifs) de x.

1. Montrer que si p est premier alors $\sigma(p) = p + 1$.
2. Montrer que $\sigma(p^k) = p^{k+1} - 1$.
3. Montrer que si $a \wedge b = 1$ alors $\sigma(ab) = \sigma(a)\sigma(b)$

Exercice 21

Un nombre est dit *parfait* lorsque la somme de ces diviseurs stricts est égale à lui-même.

1. Montrer que 6 et 28 sont parfaits.
2. Montrer que ce sont les plus petits nombres parfaits.
3. Soit p un nombre premier tel que $2^p - 1$ est premier. Montrer que $n = 2^{p-1}(2^p - 1)$ est un nombre parfait pair.
4. Réciproquement, soit n un nombre parfait pair. Soit q le plus grand nombre tel que 2^q divise n. On pose $p = q - 1$ et on a donc $n = 2^{p-1}m$ pour un certain m. Montrer que $\sigma(n) = (2^p - 1)\sigma(m)$.
5. En déduire que $2^p - 1$ divise m.
6. Montrer que par l'absurde que m est premier.
7. En déduire que $m = 2^p - 1$ et que p est premier.

On ne sait pas s'il existe une infinité de nombres premiers p tel que $2^p - 1$ est premier. Donc on ne sait pas s'il existe une infinité de nombres parfaits pairs. On ne sait pas non plus s'il existe ne serait-ce qu'un seul nombre parfait impair (s'il existe le plus petit nombre parfait impair est plus grand que 10^{150}).

Exercice 22

Ce nombre s'écrit avec 8 chiffres en base 2 et avec 6 chiffres en base 3. Quel est-il ? Ah, oui, j'oubliais, c'est un nombre premier.

Exercice 23

1. Vérifier que, si n est le numéro de votre jour de naissance, alors $P(n) = 2n^2 - 20n + 79$ est premier.
2. Le nombre $P(n)$ est-il premier pour tout $n \in \mathbb{N}$?