Exercice 1

a) Comparez deux nombres de Fermat consécutifs

$F_{n+1} = 2^{2^{n+1}} + 1 = \left(2^{2^n}\right)^2 + 1 = (F_n - 1)^2 + 1$

b) Démontrez le Lemme : $F_n - 2 = \prod_{k=0}^{n-1} F_k$

rappel : $F_0 = 3$; $F_1 = 5$ $F_1 - 2 = 5 - 2 = 3 = F_0$:
Propriété vraie pour n = 1

Hypothèse de récurrence : suppose vraie pour n

$F_{n+1} - 2 = [(F_n - 1)^2 + 1] - 2$ d'après a)

$= (F_n - 1)^2 - 1 = (F_n - 1 + 1)(F_n - 1 - 1) = F_n (F_n - 2)$

$= F_n \left(\prod_{k=0}^{n-1} F_k\right) = \prod_{k=0}^{n} F_k$ CQFD.

c) En déduire que deux nombres de Fermat distincts sont toujours premiers entre eux.

Soit n > m entiers

$F_n - 2 = \prod_{k=0}^{n-1} F_k = \left(\prod_{k=0}^{m-1} F_k\right) \times F_m \times \left(\prod_{k=m+1}^{n-1} F_k\right)$ donc il existe q entier tel que :

$F_n = q F_m + 2$ ce qui revient à dire que 2 est le reste de la division de F_n par F_m.

Le PGCD de F_n et de F_m = PGCD (F_m, 2) = 1 car F_m est impair

Donc F_n et F_m sont premiers entre eux.

Exercice 2

a) Montrer que si a s'écrit sous la forme $2^{k-1}(2^k-1)$ avec 2^k-1 premier alors a est parfait
b) Etablir la réciproque : tout nombre parfait pair est de la forme $2^{k-1}(2^k-1)$ avec 2^k-1 premier.
c) En déduire comment obtenir un nombre parfait pair.

Rappel : un nombre parfait est un nombre entier tel qu'il soit égal à la somme $\sigma'(n)$ de ses diviseurs propres (ie : tel que la somme $\sigma(n)$ de tous ses diviseurs soit égale au double du nombre)

Posons $p = 2^k-1$ premier et $n = 2^{k-1}$

- Cherchons les diviseurs de a :
  - ceux du premier facteur n : $\{1 ; 2 ; 2^2 ; \dots ; 2^{k-1}\}$
  - ceux du second facteur p : $\{1 ; p\}$
  - donc ceux du produit n avec p premier : $\{1 ; 2 ; 2^2 ; \dots ; 2^{k-1} ; p ; 2p ; 2^2p ; \dots ; 2^{k-1}p\}$

- D'où la somme de tous les diviseurs de a :

$\sigma(a) = 1 + 2 + 2^2 + \dots + 2^{k-1} + p + 2p + 2^2p + \dots + 2^{k-1}p$
$= (1+p)\ (1 + 2 + 2^2 + \dots + 2^{k-1})$ le deuxième facteur représente la somme du série géométrique

$= (1+p)\ \frac{2^k - 1}{2-1}$ $= (1+p)\ (2^k-1) = 2^k\ (2^k-1) = 2\ .\ 2^{k-1}\ (2^k-1) = 2a$

Donc a est un nombre parfait

b) n est pair. On peut donc écrire $n = 2^{k-1}.m$ avec $k \geq 2$ et m impair
Les diviseurs de n sont ceux :
- de 2 du terme 2^{k-1} : $2 ; 2^2 ; \dots 2^{k-1}$
- du terme impair : 3 ou 5 .. ou autres mais jamais 2
-

La somme des diviseurs d'un produit est égale au produit des sommes des diviseurs des facteurs à conditions que ceux ci soient premiers entre eux.
Donc $\sigma(n) = \sigma(2^{k-1}).\ \sigma(m)$

Or la somme des diviseurs d'une puissance de 2 : $\sigma(2^{k-1}) = 2^k-1$; voir a)
D'où $\sigma(n) = (2^k-1)\ \sigma(m)$ or $\sigma(n) = 2n = 2^k.m$ car n parfait
Donc $(2^k-1)\ \sigma(m) = 2^k.m$ soit $\sigma(m) = 2^k.m\ /\ (2^k-1)$

Or 2^k-1 ne divise pas 2^k donc m ; d'où $m = (2^k-1)\ M$ et M entier ; M divise m .

Cela fait 3 diviseurs au moins de m connus : 1 ; M et m si $M \neq 1$.
Leur somme $s = 1+ m + M = 1 + m + \frac{m}{2^k-1} = 1 + \frac{m(2^k-1)+m}{2^k-1} = 1 + \frac{m.2^k}{2^k-1} = 1+\sigma(m)$:
Impossible ; donc M=1 d'où $m = 2^k-1$ et m premier (car n'a que 2 diviseurs 1 et m) et $n = 2^{k-1}\ (2^k-1)$

Remarque : m est un nombre de Mersenne premier.

c) En pratique, si on trouve un nombre de Mersenne premier 2^k-1, il suffit de le multiplier par 2^{k-1} pour obtenir un nouveau nombre parfait et on trouve ainsi tous les nombres parfaits pairs.

Exercice 3

- ***Soit p un entier naturel premier. On note Ep l'ensemble {1 ; 2 ; .... ; p-1}.***
  a : Montrez que tout élément de Ep est premier avec p.
  b : Montrez que pour tout a de Ep , il existe b unique dans Ep tel que ab ≡1 [p].
  c : Déterminez les a éléments de Ep tels que a^2 ≡1 [p].
  d : Montrez que 1*2*3...*(p-1) ≡(p -1) [p]
  e : Déduisez-en que pour tout p entier naturel premier, (p -1)! + 1 est divisible par p.
  (Ce résultat ainsi que sa réciproque est le théorème de Wilson)

a: Evident car tout si a et p , avec a dans Ep ont un diviseur d ≥ 1commun alors d est inférieur à a donc strictement inférieur à p et comme p est premier, la seule valeur possible pour d est 1.

b: Si a est dans Ep, comme a et p sont premiers entre eux, on sait d'après le théorème de Bezout, qu'il existe deux entiers naturels u et v tels que au+pv=1.
Soit u = qp + b la division euclidienne de u par p. On a b dans {1;2;...;p-1}.
Effectivement, si b = 0 alors au + pv est divisible par p , ce qui contredit l'égalité au+pv=1.
Alors au + pv = a(qp+b) + pv
= ab + (aq+v)p
= 1
On a donc ab ≡1 [p]. L'existence de b est donc assurée.
Pour l'unicité, supposons qu'il existe un autre entier c dans Ep tel que ac ≡1 [p]
Alors a(b-c) est divisible par p. Comme a est premier avec p, on a donc (b-c) divisible par p.
Or, (b-c) est compris entre -(p-1) et (p-1) donc il ne peut pas être divisible par p.
D'où l'unicité de b.

c: a^2 ≡ 1 [p] si et seulement si (a-1)(a+1) est divisible par p.
a = 1 et a = (p-1) sont deux solutions évidentes.
Si a est dans {2;3;...;p-2} alors (a-1) et (a+1) sont dans {1;2;...;p-1}, donc premiers avec p.
Dans ce cas (a-1)(a+1) ne pas être divisible par p (car p premier).
Les seules solutions sont donc 1 et (p-1).

d: Pour p = 2,le résultat est évident car dans ce cas (p-1)! = 1! = 1 = (p-1) [p].
Pour p > 2 et premier:
Pour k compris strictement entre 1 et (p-1), il existe un k' unique distinct de k compris strictement entre 1 et (p-1) tel que kk' ≡1 [p] d'après 2)
Dans le produit 1×2×3×...× (p-2) × (p-1), on regroupe alors les facteurs compris entre 2 et (p-2) deux par deux tels que le produit de ces facteurs soit identique à 1.
On a donc 1×(aa') ×(bb') ×(cc') ×.....(dd') ×(p-1) = 1×2×3×...× (p-1) d'après 3).
ce qui s'écrit 1×(p-1) ≡1×2×3×...×(p-1) [p] d'où 1×2×3×...×(p-1) ≡(p-1) [p].

e: Comme (p-1) ≡-1 [p], on en déduit que 1×2×3×...× (p-1) +1 ≡0 [p]
ou encore (p-1)! + 1 ≡0 [p], c'est à dire (p-1)! + 1 est divisible par p.

Exercice 4

Montrer que p est un nombre premier si et seulement si le plus petit entier dont le carré ajouté à p donne un carré parfait est $\frac{p-1}{2}$ **.**

En déduire un test de primalité pour reconnaître si un nombre impair, non carré, est premier.

(Solution d'après « exercices d'arithmétique de J.Fitz-Patrick »)

- Soient a et b 2 nombres entiers tels que $p + a^2 = b^2$. On en déduit :

$P= b^2-a^2 = (b+a)(b-a)$ comme p est premier on a p = a+b et b-a = 1

D'où a = $\frac{p-1}{2}$ et b = $\frac{p+1}{2}$ on remarque que p étant impair ces expressions sont bien entières

- Si p n'est pas premier, bornons nous au cas p impair.

Alors on peut trouver un diviseur d (impair) de p différent de 1 tel que le quotient q de p par d soit au plus égal à d. p = qd

Posons **b-a = d et b+a = q**

Alors b = $\frac{d+q}{2}$ et a = $\frac{q-d}{2}$

d et q étant impairs b et a sont bien entiers.

On a alors $\frac{q-d}{2} < \frac{p-1}{2}$ puis que d>1 et q<p

Vérifions: $p + \left(\frac{q-d}{2}\right)^2 = qd + \frac{q^2+d^2-2qd}{4} = \frac{4qd+q^2+d^2-2qd}{4} = \left(\frac{q+d}{2}\right)^2$

Corollaire : pour reconnaître si un nombre impair, non carré, est premier, on lui ajoute successivement les carrés des $\frac{n-1}{2}$ premiers nombres 1,2,3…, $\frac{p-1}{2}$; jusqu'à ce qu'on obtienne un total qui soit carré parfait d'un nombre entier. Si le premier total remplissant cette condition est $p + \left(\frac{p-1}{2}\right)^2$ alors le nombre est premier.

Exercice 5

a) Soit n un entier naturel. Montrer que 30 | n^5 - n

- Décomposons 30 en produit de facteurs premiers; il vient 30 = 5.3.2

  Comme chaque nombre premier intervenant dans la décomposition de 30 a une valuation de 1, il suffit de montrer que chaque nombre premier divise n^5 - n, pour que leur produit qui est alors 30, le divise.

- Montrons que 2 | n^5 - n

  On a n^5 - n = n.(n^4 - 1)

  - Si n est pair, on a 2 | n, donc 2 | n.(n^4 - 1) d'où 2 | n^5 - n.

  - Sinon, n est impair et alors n^4 aussi donc n^4 - 1 est pair. Il vient donc 2 | n^4 - 1, soit 2 | n^5 - n.

  Finalement, dans tous les cas 2 | n^5 - n

- Montrons que 3 | n^5 - n

  On a n^5 - n = n.(n^4 - 1) = n.(n^2 - 1).(n^2 + 1) = (n^3 - n).(n^2 + 1)

  3 étant un nombre premier, alors, d'après le petit théorème de Fermat

  $\forall$ n $\in$N, $n^3 \equiv$ n [3] ; soit 3 | n^3 - n et **alors 3 | n^5 - n**

- Montrons que 5 | n^5 - n

  5 étant un nombre premier, alors, d'après le petit théorème de Fermat,

  $\forall$ n $\in$N, $n^5 \equiv$ n [5] ; **d'où 5 | n^5 - n**

- Finalement, comme 2, 3 et 5 sont premiers deux à deux, leur produit divise n^5 - n

  D'où 30 | n^5 - n

b) Un entier naturel ne contient que les facteurs premiers 5 et 7. Le nombre des diviseurs (positifs) de n^2 est le triple de celui de n. Trouver n.

Par hypothèse : $n = 5^{\alpha} \times 7^{\beta}$; d'où $n^2 = 5^{2\alpha} \times 7^{2\beta}$. Désignons par $\tau(n)$ le nombre de diviseurs de n.

$$\begin{cases} \tau(n) = (\alpha+1)(\beta+1) \\ \tau(n^2) = (2\alpha+1)(2\beta+1) \end{cases}$$

Par hypothèse : $(2\alpha+1)(2\beta+1) = 3(\alpha+1)(\beta+1)$

Ce qui donne : $4\alpha\beta+2\alpha+2\beta+1=3\alpha\beta+3\alpha+3\beta+3$ d'où $\alpha\beta - \alpha - \beta - 2 = 0$

Ou encore : $\alpha\beta - \alpha - \beta + 1 = 3$ ce qui donne : $(\alpha-1)(\beta-1) = 3$. Donc $(\alpha-1)$ et $(\beta-1)$ sont des diviseurs de 3 ; donc $(\alpha-1) = 1$ et $(\beta-1) = 3$, ou $(\alpha-1) = 3$ et $(\beta-1) = 1$. Ce qui conduit pour le **couple $(\alpha,\beta) = (1,3)$** ou **(3,1)**. On obtient donc les solutions **n = 60025 ou n = 30625**. Dans les deux cas on a 15 diviseurs pour n et 45 diviseurs pour n^2 .