EXERCICE 1:

Montrer par récurrence que $\forall n \in IN\ ,\ \forall k > 1$ *on a :* $2^{2^{n+k}} - 1 = \left(2^{2^n} - 1\right) \times \prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right)$.

2. On pose $F_n = 2^{2^n} + 1$ *. Montrer que pour* $m \neq n$ *,* F_n *et* F_m *sont premiers entre eux.*

3. En déduire qu'il y a une infinité de nombres premiers.

CORRECTION :

1. Fixons n et montrons par récurrence sur k > 1.
La formule est vraie pour k = 1.
Supposons la formule vraie au rang k. Alors

$$\left(2^{2^n} - 1\right) \times \prod_{i=0}^{k} \left(2^{2^{n+i}} + 1\right) = \left(2^{2^n} - 1\right) \times \prod_{i=0}^{k-1} \left(2^{2^{n+i}} + 1\right) \times \left(2^{2^{n+k}} + 1\right)$$

$$= \left(2^{2^{n+k}} - 1\right) \times \left(2^{2^{n+k}} + 1\right) = \left(\left(2^{2^{n+k}}\right)^2 - 1\right)$$

$$= \left(2^{2^{n+k+1}} + 1\right)$$

Nous avons utilisé l'hypothèse de récurrence dans ces égalités. Nous avons ainsi montré la formule au rang $k+1$ *. Et donc par le principe de récurrence elle est vraie.*

2. Écrivons $m = n + k$ *, alors l'égalité précédente devient* $F_m + 2 = \left(2^{2^n} - 1\right) \times \left(2^{2^n} - 1\right) \times \prod_{i=n}^{m-1} F_i$.

Soit encore : $F_n \times \left(2^{2^n} - 1\right) \times \left(2^{2^n} - 1\right) \times \prod_{i=n+1}^{m-1} F_i - F_m = 2$.

Si d est un diviseur de F_n *et* F_m *alors d divise 2 (ou alors on peut utiliser le théorème de Bézout). En conséquent* $d = 1$ *ou* $d = 2$*. Mais* F_n *est impair donc d = 1. Nous avons montré que tous diviseurs de* F_n *et* F_m *est 1, cela signifie que* F_n *et* F_m *sont premiers entre eux.*

3. Supposons qu'il y a un nombre fini de nombres premiers. Nous les notons alors $\{p_1, ..., p_N\}$ *. Prenons alors* $N+1$ *nombres de la famille* F_i *, par exemple* $\{F_1, ..., F_{N+1}\}$ *. Chaque* F_i *,* $i = 1, ..., N+1$ *est divisible par (au moins) un facteur premier* p_j *,* $j = 1, ..., N$ *. Nous avons* $N+1$ *nombres* F_i *et seulement* N *facteurs premiers* p_j *. Donc par le principe des tiroirs il existe deux nombres distincts* F_k *et* $F_{k'}$ *(avec* $1 \leq k$ *,* $k' \leq N+1$ *) qui ont un facteur premier en commun. En conséquent* F_k *et* $F_{k'}$ *ne sont pas premiers entre eux. Ce qui contredit la question précédente. Il existe donc une infinité de nombres premiers.*

EXERCICE 2:

1. Montrer que le reste de la division euclidienne par 8 *du carré de tout nombre impair est* 1 *.*
2. Montrer de même que tout nombre pair vérifie $x^2 \equiv 0[8]$ *ou* $x^2 \equiv 4[8]$*.*
3. Soient a, b, c trois entiers impairs.
Déterminer le reste modulo 8 *de* $a^2 + b^2 + c^2$ *et celui de* $2(ab + bc + ca)$ *.*
4. En déduire que ces deux nombres ne sont pas des carrés puis que $ab + bc + ca$ *non plus.*

CORRECTION :

1. Soit n un nombre impair, alors il s'écrit $n = 2p + 1$ *avec* $p \in IN$ *.*

Maintenant $n^2=(2p+1)^2=4p^2+4p+1=4p(p+1)+1$ *. Donc* $n^2\equiv 1\ [8]$.

2. Si n est pair alors il existe $p\in IN$ *tel que* $n=2p$ *. Et* $n^2=4p^2$ *. Si p est pair alors* p^2 *est pair et donc* $n^2=4p^2$ *est divisible par* 8 *, donc* $n^2\equiv 0\ [8]$. *Si p est impair alors* p^2 *est impair et donc* $n^2=4p^2$ *est divisible par* 4 *mais pas par* 8 *, donc* $n^2\equiv 4\ [8]$.

3. Comme a est impair alors d'après la première question $a^2\equiv 1\ [8]$, *de même* $b^2\equiv 1\ [8]$ *et* $c^2\equiv 1\ [8]$. *Donc* $a^2+b^2+c^2\equiv 1+1+1\ [8]\equiv 3[8]$ *. Pour l'autre reste, écrivons* $a=2p+1, b=2q+1b$ *et* $c=2r+1$, *alors* $2ab=2(2p+1)(2q+1)=8pq+4(p+q)+2$ *. Alors* $2(ab+bc+ca)=8pq+8qr+8pr+8(p+q+r)+6$, *donc* $2(ab+bc+ca)\equiv 6[8]$.

4. Montrons par l'absurde que le nombre $a^2+b^2+c^2$ *n'est pas le carré d'un nombre entier. Supposons qu'il existe* $n\in IN$ *tel que* $a^2+b^2+c^2=n^2$ *. Nous savons que* $a^2+b^2+c^2\equiv 3[8]$. *Si n est impair alors* $n^2\equiv 1[8]$ *(et si n est pair alors* $n^2\equiv 0\ [8]$ *ou* $n^2\equiv 4\ [8]$. *Dans tous les cas* n^2 *n'est pas congru à* 3 *modulo* 8 *. Donc il y a une contradiction. La conclusion est que l'hypothèse de départ est fausse donc* $a^2+b^2+c^2$ *n'est pas un carré. Le même type de raisonnement est valide pour* $2(ab+bc+ca)$. *Pour* $ab+bc+ca$ *l'argument est similaire : d'une part* $2(ab+bc+ca)\equiv 6[8]$ *et d'autre part si, par l'absurde, on suppose* $ab+bc+ca=n^2$ *alors selon la parité de n nous avons* $2(ab+bc+ca)\equiv 2n^2\equiv 2[8]$ *ou* $2(ab+bc+ca)\equiv 2n^2\equiv 0[8]$.
Dans les deux cas cela aboutit à une contradiction.
Nous avons montré que $ab+bc+ca$ *n'est pas un carré.*

EXERCICE 3:

Soient a; b des entiers supérieurs ou égaux à 1. Montrer que :

1. $(2^a-1)\,|\,(2^{ab}-1)$
2. *Si* (2^p-1) *est premier alors* p *est premier ;*
3. $pgcd(2^a-1;2^b-1)=2^{pgcd(a;b)}-1$

CORRECTION :

1. Nous savons que : $(x^b-1)=(x-1)(x^{b-1}+\cdots+x+1)$

pour $x=2^a$ *nous obtenons :* $(2^{ab}-1)=(2^a-1)(2^{a(b-1)}+\cdots+2^a+1)$

donc $(2^a-1)\,|\,(2^{ab}-1)$

2. Montrons cette propriété par la contraposée. Supposons que p ne soit pas premier. Donc il existe a et b des entiers tels que $p=ab$ *avec* $1<p\,;q<a$. *Par la question précédente 2-*$(2^a-1)\,|\,(2^p-1)$

(et $1<2^a-1<2^p-1$*) Donc* 2^p-1 *n'est pas un nombre premier.*

3. Nous supposons $a\geq b$. *Nous allons montrer que faire l'algorithme d'Euclide pour le couple* $(2^a-1;2^b-1)$ *revient à faire l'algorithme d'Euclide pour* $(a\,;b)$. *Tout d'abord rappelons la formule qui est à la base de l'algorithme d'Euclide :* $pgcd(a;b)=pgcd(a-b;b)$. *Appliqué à* $(2^a-1;2^b-1)$ *cela donne directement* $pgcd(2^a-1;2^b-1)=pgcd(2^a-2^b;2^b-1)$

Mais $2^a-2^b=2^b(2^{a-b}-1)$ *d'où* $pgcd(2^a-1;2^b-1)=pgcd(2^b(2^{a-b}-1);2^b-1)$

$=pgcd(2^{a-b}-1;2^b-1)$

La dernière égalité vient du fait que : 2^b *et* 2^b-1 *sont premiers entre eux (deux entiers consécutifs sont toujours premiers entre eux).*

Nous avons montré : $pgcd\left(2^a-1;2^b-1\right)=pgcd\left(2^{a-b}-1;2^b-1\right)$.

Cette formule est à mettre en parallèle de $pgcd\left(a;b\right)=pgcd\left(a-b;b\right)$. *En itérant cette formule nous obtenons que si* $a=bq+r$ *alors :* $pgcd\left(2^a-1;2^b-1\right)=pgcd\left(2^{a-bq}-1;2^b-1\right)$

$$=pgcd\left(2^r-1;2^b-1\right)$$

à comparer avec $pgcd\left(a;b\right)=pgcd\left(a-b;b\right)$

$$=pgcd\left(r;b\right).$$

Nous avons notre première étape de l'algorithme d'Euclide. En itérant l'algorithme d'Euclide pour $\left(a;b\right)$, *nous nous arrêtons au dernier reste non nul :* $pgcd\left(a;b\right)=pgcd\left(b;r\right)=pgcd(r_n;\ 0)=r_n$. *Ce qui va donner*

$$pgcd\left(2^a-1;2^b-1\right)=pgcd\left(2^b-1;2^r-1\right)$$

$$=pgcd\left(2^{r_n}-1;2^0-1\right)=2^{r_n}-1$$

$$(r_n=pgcd(a,b)\ )$$

Bilan : $pgcd\left(2^a-1;2^b-1\right)=2^{pgcd(a,b)}-1$