Exercice 15

Soit $(m,a)\in\mathbb{N}^2$. On suppose que a^m+1 est premier.

On veut montrer que $m=2^n$, pour un certain $n\in\mathbb{N}$.

Raisonnons par l'absurde, et supposons que m n'est pas de la forme cherchée.

Cela signifie que dans la décomposition de m en facteurs premier, il y a au moins un autre nombre premier que 2. C'est à dire un nombre premier impair, q

On peut donc écrire $m=qk$ avec q premier impair ($q\neq 1$)
$k\in\mathbb{N}$.

Alors $a^m+1 = (a^p)^q+1$
$= (a^p+1)(a^{p(q-1)}-a^{p(q-2)}+\dots+1)$ d'après la formule indiquée (appliquée en prenant $x=a^p$ et $l=q$)

Ceci prouve : $\exists K\in\mathbb{Z},\ a^m+1=(a^p+1)K$.

Ainsi $a^p+1 \mid a^m+1$. Or a^m+1 est premier, par hypothèse.

Nécessairement, on a donc $a^m+1=a^p+1$ (les seuls diviseurs de a^m+1 sont lui même et 1).

c'est-à dire $p=m$. Or $m=pq$ donc $q=1$.

Absurde! On avait supposé $q\neq 1$

Donc l'hypothèse de départ était fausse, et donc : $\exists n\in\mathbb{N},\ m=2^n$.

Exercice 16

Soient $a,n\in\mathbb{N}$, $a,n\geq 2$.

1) On suppose que a^n-1 est premier. Montrons que $a=2$.

On sait que $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\dots+a+1)$ (puisque $1+a+\dots+a^{n-1}=\frac{a^n-1}{a-1}$ formule vue et revue...)

Donc $a-1\mid a^n-1$.

Or a^n-1 est premier : donc $a-1=1$ ou $a-1=a^n-1$. Mais $n\geq 2$. Donc $a-1\neq a^n-1$

d'où $a-1=1$ et $\boxed{a=2}$.

2) Supposons $M_n=2^n-1$ premier. Montrons que n est premier.

Soit p un diviseur (positif) de n. Il s'agit de montrer que $p=n$ ou $p=1$.

$p\mid n \Rightarrow \exists k\in\mathbb{N},\ n=kp$.

donc $2^n-1=2^{kp}-1=(2^p)^k-1=(2^p-1)((2^p)^{q-1}+\dots+2^p+1)$ (par la même formule qu'au

donc $2^p-1\mid 2^n-1$, et 2^n-1 est premier.

donc $2^p-1=2^n-1$ ou $2^p-1=1$

càd $p=n$ ou $p=1$. et donc $\boxed{n \text{ est premier}}$

Ainsi, si M_n est premier, alors n aussi.

La réciproque est fausse : si n est premier, M_n ne l'est pas nécessairement.

Contre exemple $n=11$ est premier, mais $M_{11}=2^{11}-1=2047=23\times 89$ ne l'est pas

Exercice 17

1) Soit p premier et $k\in\{1,2,\dots p-1\}$. $\binom{p}{k}=\frac{p!}{k!(p-k)!}=\frac{p(p-1)\dots(p-k+1)}{k!}$

donc $p(p-1)\dots(p-k+1)=k!\binom{p}{k}$. C'est à dire, il existe $K\in\mathbb{N}$ tel que $k!\binom{p}{k}=Kp$. donc $p\mid k!\binom{p}{k}$

or $p\wedge 2=1$, $p\wedge 3=1$ ... $p\wedge k=1$ (car p premier, $p>k$)

donc, par l'exercice 12, 1), $p\wedge(2\times 3\times\dots\times k)=1$. c'est à dire $p\wedge k!=1$ Donc par le lemme de Gauss, $\boxed{p\mid\binom{p}{k}}$

2) Par la formule du binôme de Newton

$(a+b)^p=\sum_{k=0}^{p}\binom{p}{k}a^kb^{p-k}$ Donc $(a+b)^p=b^p+\sum_{k=1}^{p-1}\binom{p}{k}a^kb^{p-k}+a^p$.

D'où $(a+b)^p-a^p-b^p=\sum_{k=1}^{p-1}a^kb^{p-k}\binom{p}{k}$. Or, $p\mid\binom{p}{k}$ pour $k=1,\dots,p-1$. donc $p\mid\sum_{k=1}^{p-1}a^kb^{p-k}\binom{p}{k}=(a+b)^p-a^p-b^p$

en prenant $b=1$, on en déduit que $\boxed{p\mid(a+1)^p-(a^p+1)}$.

3) Soit, $\forall a\in\mathbb{N}\setminus\{0\}$ $\mathcal{P}(a)$ la propriété : $p\mid a^p-a$. Démontrons que $\mathcal{P}(a)$ est vraie quelle que soit a, par récurrence

- Initialisation.
  Comme $p\mid 0=a^p-a$, $\mathcal{P}(1)$ est vraie.
- Supposons $\mathcal{P}(a)$ vraie au rang a fixé. Et Montrons $\mathcal{P}(a+1)$.
  $(a+1)^p-(a+1)=(a+1)^p-a^p-1+a^p-a$ (on fait apparaître a^p ... pour utiliser $\mathcal{P}(a)$)
  par hypothèse de récurrence $p\mid a^p-a$
  par la question 2) $p\mid(a+1)^p-a^p-1$. Donc p divise la somme des 2, càd $p\mid(a+1)^p-(a+1)$ et $\mathcal{P}(a+1)$ est encore vraie.

Donc $\mathcal{P}(a)$ est vraie, quelque soit a : Donc $p\mid a^p-a$.

Si de plus $p\wedge a=1$, alors, comme $p\mid(a^{p-1}-1)a$ par lemme de Gauss $\boxed{p\mid a^{p-1}-1}$.