6 Nombres de Mersenne[1] - Très classique - Oral Centrale

Montrer que si $a \in \mathbb{N}, n \in \mathbb{N} \setminus \{0,1\}$ tel que $a^n - 1$ est premier, alors $a = 2$ et n est premier.

$a \notin \{0;1\}$

$a^n - 1 = a^n - 1^n = \underbrace{(a-1)}_{>0}\underbrace{(\text{qq chose d'entier})}_{a^{n-1}+a^{n-2}+a^{n-3}+\dots+1}$

$\left(\sum_{k=0}^{n-1} a^k = \frac{a^n-1}{a-1} \text{ (avec } a \neq 1)\right)$

Comme $a^n - 1$ premier, $a - 1 \in \{1, a^n - 1\}$ ie $a = 2$ ou $\underbrace{a^{n-1} = 1}_{\text{exclu avec } a \geq 2}$

Donc $a = 2$ et $a^n - 1 = 2^n - 1$ premier.

Soit d diviseur >0 de n but : $d \in \{1, n\}$.

On a $k \in \mathbb{N}$ tel que $n = d \times k$.

$\underbrace{2^n - 1}_{\text{premier}} = 2^{dk} - 1 = (2^d)^k - 1^k = (2^d - 1)m$ où $m \in \mathbb{N}$.

donc $\left| \begin{array}{l} 2^d - 1 = 1 \\ \text{ou} \\ 2^d - 1 = 2^n - 1 \end{array} \right.$ donc $\left| \begin{array}{l} 2^d = 2 \\ \text{ou} \\ 2^d = 2^n \end{array} \right.$ donc $d \in \{1; n\}$ (décomp. primaire)

donc n premier.

$F_2 = 2^4 + 1 = 17$ $\quad F_4 = 2^{16} + 1 = 65537$

$F_3 = 2^8 + 1 = 257$

7 Nombres de Fermat[2] - Très classique - Oral Mines

1. Soient $a, n \in \mathbb{N}^*$, $a \geqslant 2$. Montrer que si $a^n + 1$ est premier, a est pair et n est une puissance de 2. On appelle nombres de Fermat les nombres $F_n = 2^{2^n} + 1$. Ils sont premiers pour n de 2 à 4, mais ne le sont pas pour n de 5 à 32 (contrairement à ce que conjectura Fermat).
2. Démonstration de 1734 d'Euler du fait que F_5 n'est pas premier.
   (a) Comparer $5^4 + 2^4$ et $1 + 5 \times 2^7$ (sans calculatrice !).
   (b) En déduire que $5^4 \times 2^{28} \equiv 1$ [641].
   (c) Conclure que 641 divise F_5.
3. Montrer que pour tout $n \in \mathbb{N}$, $F_{n+1} = (F_n - 1)^2 + 1$ et en déduire que F_n et F_{n+1} sont premiers entre eux.
4. Pour $n \in \mathbb{N}$, établir que $F_{n+1} = \prod_{k=0}^{n} F_k + 2$. En déduire que les F_n sont premiers entre eux deux à deux. Retrouver le fait que le nombre de nombres premiers est infini.

$F_5 = 2^{32} + 1 = 4\,294\,967\,297$

Prendre 1 div. premier pour chaque F_n.

récurrence simple...

$\forall k \in [\![0; n]\!]$, $F_k \wedge F_{n+1} = 1$ comme en 3).

7) 1 Si $a^n + 1$ premier but : a pair, $n = 2^m$ avec $m \in \mathbb{N}$.

- Soit $a^n + 1 = 2$ et alors $a^n = 1$ donc $a = 1$ non.

  Soit $a^n + 1$ impair, $a^n + 1 \equiv 1\ [2]$ donc $a^n \equiv 0\ [2]$ donc $a \equiv 0\ [2]$

  car $\mathbb{Z}/2\mathbb{Z}$ corps donc intègre

  (ou $a \equiv 0\ [2]$ ~~ou $a \equiv 1\ [2]$~~)

  Donc a est pair.

- Soit d diviseur premier de n. But : $d = 2$

  $\boxed{\text{Si } d \text{ est impair,}}$ $n = d \times k$ avec $k \in \mathbb{N}$

  $\underbrace{a^n + 1}_{\text{premier}} = a^{d \times k} + 1 = a^{dk} - (-1)^d$ car d impair.

  $= (a^k)^d - (-1)^d = (a^k - (-1)) \times l$ où $l \in \mathbb{N}$

  donc $\left| \begin{array}{l} a^k + 1 = 1 \\ \text{ou} \\ a^k + 1 = a^n + 1 \end{array} \right.$ avec $a \geq 2$, donc $k = n$ donc $d = 1$ $\boxed{\text{contradiction}}$

  2 seul div premier de n : n est une puissance de 2

ou : si d div. impair de n alors $d=1$.
Donc le seul div. premier de n est 2.

$F_n = 2^{2^n}+1$

3) $F_{n+1} = \underbrace{(F_n-1)^2}_{=(2^{2^n})^2 = 2^{2\times 2^n} = 2^{2^{n+1}}} + 1 = F_n^2 - 2F_n + 2$

$a \wedge b = 1$

But : $F_n \wedge F_{n+1} = 1$

$\boxed{au + bv = 1}$ Seul div >0 commun 1.

$F_{n+1} + F_n(2-F_n) = 2$

Si d div. commun >0 à F_n et F_{n+1}, alors $d \mid 2$ donc $d \in \{1,2\}$.

Or F_n (et F_{n+1}) sont impairs donc $d \neq 2$ donc $d=1$

$F_n \wedge F_{n+1} = 1$.

8 En s'inspirant de la démonstration sur l'infinité des nombres premiers, montrer qu'il existe une infinité de nombres premiers de la forme $4k-1$[3].

Sinon $p_1, \dots, p_k$ ces nb premiers.

Soit $N = 4p_1 \times \dots \times p_k - 1 \geq 2$.

$p \equiv \begin{cases} 0 \\ 1 \\ 2 \end{cases} [4]$ Soit p diviseur premier de N alors $p \notin \{p_1, \dots, p_k\}$ car sinon $p \mid 1$.

donc p n'est pas de la forme $4k-1$ donc soit de la forme $\cancel{4k}$ non premier, $4k+1$, $\cancel{4k+2}$

Tous les div. premiers de N sont de la forme $4k+1$.

N impair

Par décomp. primaire : $N = \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} p^{v_p(n)} \equiv 1 \ [4]$

Or $N = 4p_1 \cdots p_k - 1 \equiv -1 \ [4]$ contradiction.

9 Justifier l'existence de 1000 entiers consécutifs sans nombre premier.

$\cancel{n+1}$
$n+2$
$n+3$
$\vdots$
$n+999$
$n+1000$
$n+1001$

$n=2\times$
$n=3\times$
$n=999\times$

$\cancel{n=999!}$

$\boxed{n=1001!}$

$\pi(n) = \{\text{nb premiers} \leq n\}$

$\sim \frac{n}{\ln n}$ (difficile).

proportion de nb premiers $\frac{\pi(n)}{n} \sim \frac{1}{\ln n} \to 0$.

$\forall k \in [\![2; 1001]\!]$,

$n+k = \underbrace{k}_{\geq 2} \times \underbrace{\left[\underbrace{\frac{1001!}{k}}_{\in \mathbb{N}} + 1\right]}_{\geq 2}$ non premiers

10 Formule de Legendre - Très classique - Oraux divers

Combien y a-t-il de zéros à la fin de 100!? De 1000!? De 2021!?

Montrer que $\underbrace{v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor}$ pour p premier et $n \in \mathbb{N}^*$.

aper $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ $\quad (p^k \xrightarrow[k \to +\infty]{} +\infty)$

100 !: nb de zéros finals = (nb de facteurs 10)

ie le + gd k tq $10^k \mid 100!$

$100! = 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times \overset{10}{\cdots} \times 100$

beaucoup de facteurs 2 que de facteurs 5 !

Le nb de facteurs 10 est donc celui de facteurs 5.

ie $v_5(100!)$

- Dans les multiples de 5 entre 2 et 100 : il y en a $\frac{100}{5} = 20$] fournit un 5.
- Dans les multiples de $5^2 = 25$: il y en a $\frac{100}{25} = 4$] fournit un 5 supplémentaire
- ——— $5^3 = 125$: ——— 0] idem.

100! se termine par $24 = v_5(100!)$ zéros.

$$1000! : \underbrace{\frac{1000}{5}}_{\text{multiples de 5}} + \underbrace{\frac{1000}{25}}_{\text{mult. de 25}} + \frac{1000}{125} + \left\lfloor \frac{1000}{625} \right\rfloor = 249$$

$1 \leq 125k \leq 1000$

ie $1 \leq k \leq \left\lfloor \frac{1000}{125} \right\rfloor$

13 Oral Centrale Déterminer le chiffre des unité de 1587^{413}.

On cherche à réduire 1587^{413} modulo 10

$1580 + 7 = 1587 \equiv 7 \ [10]$

donc $1587^{413} \equiv \underbrace{7^{413} \ [10]}$

$7^2 \equiv 9 \ [10]$

$7^3 \equiv 7^2 \times 7 \ [10]$

$\equiv -1 \times 7 \ [10]$

$\equiv 3 \ [10]$

$7^4 \equiv 21 \ [10]$

$\boxed{7^4 \equiv 1 \ [10]}$

Thm d'Euler : $7 \wedge 10 = 1$, $\quad 7^{\varphi(10)} \equiv 1 \ [10]$

$\varphi(10) = \varphi(5 \times 2) = \varphi(5)\varphi(2) = 4 \times 1 = 4.$

1es entre eux

$413 = 412 + 1 \equiv 1 \ [4]$ donc $7^{413} = 7^{4k+1} = (7^4)^k \times 7 \equiv 1^k \times 7 \ [10]$

$\equiv 7 \ [10]$.

chiffre des unités

Critères de divisibilité : $n = \overline{a_p \cdots a_2 a_1 a_0}^{10} = \sum_{k=0}^{p} a_k 10^k$

$2 \mid n \Leftrightarrow 2 \mid a_0 \Leftrightarrow a_0 \in \{0, 2, 4, 6, 8\}$

$3 \mid n \Leftrightarrow 3 \mid \sum_{k=0}^{p} a_k$

$4 \mid n \Leftrightarrow 4 \mid \overline{a_1 a_0}^{10}$

$5 \mid n \Leftrightarrow 5 \mid a_0 \Leftrightarrow a_0 \in \{0, 5\}$

$6 \mid n \Leftrightarrow 2 \mid n$ et $3 \mid n$

$8 \mid n \Leftrightarrow 8 \mid \overline{a_2 a_1 a_0}^{10}$

$9 \mid n \Leftrightarrow 9 \mid \sum_{k=0}^{p} a_k$

$10 \mid n \Leftrightarrow 2 \mid n$ et $5 \mid n \Leftrightarrow a_0 = 0$

$11 \mid n \Leftrightarrow 11 \mid \sum_{k=0}^{p} (-1)^k a_k$

$n \mid m(m+1)\dots(m+n-1)$

15 Oral Mines

Soit $p \geqslant 5$ un nombre premier. Montrer que 24 divise p^2-1.

$p^2-1 = \underbrace{(p-1)}_{\text{pair}}\underbrace{(p+1)}_{\text{pair}}$ donc $4 \mid p^2-1$

$3 \mid \underbrace{(p-1)\ p\ (p+1)}_{\text{3 nb consécutifs}}$ $\quad 3 \nmid p$ car $\begin{cases} p \text{ premier} \\ p \neq 3 \text{ car } p \geqslant 5 \end{cases}$

et 3 premier donc $3 \mid (p-1)(p+1)$

donc $3 \mid p^2-1$

$(p-1), \cancel{p}, (p+1), \cancel{(p+2)}$ consécutifs donc l'un est divisible par 4

impairs

C'est $p-1$ ou $p+1$.

donc $2 \times 4 = 8 \mid (p-1)(p+1)$

Or $8 \wedge 3 = 1$ donc $8 \times 3 = 24 \mid p^2-1$.

Pour demain

16, 17 thm chinois

18 $\mathbb{Z}/13\mathbb{Z}$ corps $\longrightarrow$ pivot de Gauss.

21 $\mathbb{Z}/17\mathbb{Z}$ corps

25