PROBLEMES ET RESULTATS EN THEORIE DES NOMBRES

Conférence de Paul ERDÖS à l'Université de Limoges le 21 Octobre 1986

rédigé par François MORAIN

Notations :

Dans tout ce qui suit, p et q désigneront toujours des nombres premiers.

Le i-ème nombre premier sera noté π_i ($\pi_1 = 2, \pi_2 = 3, \ldots$).

1. Partie quadratique d'un nombre :

Définition 1.1 :

Soit $m \in \mathbf{N}^*$: $m = \prod_{i=1}^{i=k} p_i^{\alpha_i}$, $\alpha_i \geq 1$, $k \geq 1$.

On pose : $Q(m) = \prod_{\alpha_i \geq 2} p_i^{\alpha_i}$

$$NQ(m) = \prod_{\alpha_j = 1} p_j$$

$Q(m)$ (respectivement $NQ(m)$) est appelé partie quadratique (respectivement non quadratique) de m.

On définit, pour $n \geq 1$, $k \geq 1$, le nombre

$$M(n,k) = n(n+1)\ldots(n+k-1)$$

et $$E(n) = \text{Max}\{ k \mid Q(M(n,j)) > NQ(M(n,j)),\ 1 \leq j \leq k \}.$$

Si $Q(n) < NQ(n)$, on pose $E(n) = 0$.

Exemples :

$E(4) = 1$; $E(5040) = 10$; $E(3) = 0$.

Proposition 1.1 :

Si $n \geq 7$, $E(n) \geq 2n \Rightarrow E(n) = +\infty$.

Démonstration :

Etudions de plus près $M(n, k)$, pour $k \geq 2n$:

$$M(n, k) = \frac{(n + k - 1)!}{(n - 1)!} = \frac{(n - 1 + k)!}{(n - 1)!}.$$

Soit $m \in \mathbf{N}^*$: on pose $v_p(m) = \text{Max}\{i \geq 0 ; p^i \mid m\}$ avec p un nombre premier quelconque.

En particulier :

$m! = \prod_{p \leq m} p^{v_p(m!)}$, le produit portant sur les nombres premiers inférieurs à m.

On sait, cf [HAR] p. 342, que :

$\forall$ p premier, $v_p(m!) = \sum_{r=1}^{\infty} \left\lfloor \frac{m}{p^r} \right\rfloor$, si $\lfloor x \rfloor$ désigne la partie entière de x.

On a donc :

$$(n - 1)! = \prod_{p \leq n-1} p^{v_p((n-1)!)}$$

$$(n - 1 + k)! = \prod_{p \leq n-1} p^{v_p((n-1+k)!)} \prod_{n \leq p \leq n-1+k} p^{v_p((n-1+k)!)}$$

D'où :

$$M(n, k) = \prod_{p \leq n-1} p^{v_p((n-1)+k)!) - v_p((n-1)!)} \times \prod_{n \leq p \leq n-1+k} p^{v_p((n-1+k)!)}$$

De l'inégalité :

$\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$, on déduit :

$v_p((n - 1 + k)!) - v_p((n - 1)!) \geq v_p(k!)$.

Remarquons alors que :

$$v_p(m!) = 1 \Leftrightarrow \frac{m}{2} < p \leq m.$$

On en tire :

- $p \leq \frac{n - 1 + k}{2} \Rightarrow p \leq \frac{k}{2} \Rightarrow v_p(k!) \geq 2.$
- $p \leq \frac{n - 1 + k}{2} \Rightarrow v_p((n - 1 + k)!) \geq 2.$

Par suite :

$$NQ(M(n, k)) = \prod_{\frac{n-1+k}{2} < p \leq n-1+k} p$$

Posons $m = n - 1 + k$ et considérons :

$$\mathcal{M} = \binom{m}{\lfloor \frac{m}{2} \rfloor} = \frac{m(m-1) \ldots (m - \lfloor \frac{m}{2} \rfloor + 1)}{\lfloor \frac{m}{2} \rfloor !}$$

Si $\lfloor \frac{m}{2} \rfloor < p \leq m$, p divise le numérateur de $\mathcal{M}$, mais pas le dénominateur.

On a donc :

$$\prod_{\lfloor \frac{m}{2} \rfloor < p \leq m} p \mid \mathcal{M} \text{ et } \prod_{\lfloor \frac{m}{2} \rfloor < p \leq m} p \leq \mathcal{M}.$$

Mais $\mathcal{M}$ apparaît au moins une fois dans le développement de $(1+1)^m$ par la formule du binôme : $\mathcal{M} < 2^m$.

Donc :

$$\prod_{\lfloor \frac{m}{2} \rfloor < p \leq m} p < 2^m.$$

Par suite : $N\,Q(M(n,k)) < 2^{n-1+k}$.

Revenons à $Q(M(n,k))$:

$$Q(M(n,k)) = \prod_{p \leq \frac{n-1+k}{2}} p^{v_p((n-1+k)!) - v_p((n-1)!)}.$$

On a :

$$v_p((n-1+k)!) \geq 2\, v_p\left(\lfloor \frac{n-1+k}{2} \rfloor !\right) = 2\, v_p\left(\lfloor \frac{m}{2} \rfloor !\right)$$

En outre :

$$\frac{m}{2} = \frac{n-1+k}{2} \geq \frac{3n-1}{2} > n-1.$$

D'où :

$$\lfloor \frac{m}{2} \rfloor \geq n-1,$$

et donc :

$$v_p((n-1+k)!) - v_p((n-1)!) \geq v_p\left(\lfloor \frac{m}{2} \rfloor !\right) + v_p\left(\lfloor \frac{m}{2} \rfloor !\right) - v_p((n-1)!).$$
$$\geq v_p\left(\lfloor \frac{m}{2} \rfloor !\right).$$

Alors :

$$Q(M(n,k)) \geq \prod_{p \leq \lfloor \frac{m}{2} \rfloor} p^{v_p\left(\lfloor \frac{m}{2} \rfloor !\right)} = \lfloor \frac{m}{2} \rfloor !$$

$$Q(M(n,k)) \geq \lfloor \frac{n-1+k}{2} \rfloor !.$$

D'où :

$$\frac{Q(M(n,k))}{N\,Q(M(n,k))} > \frac{\left\lfloor \frac{n-1+k}{2} \right\rfloor}{2^{n-1+k}} > \frac{r!}{2^{2r+1}} = \alpha_r .$$

$$\text{avec} \quad r = \left\lfloor \frac{m}{2} \right\rfloor .$$

On a :

$$\alpha_r = \frac{1}{2}\,\frac{r!}{4^r} .$$

On calcule alors : $\dfrac{\alpha_{r+1}}{\alpha_r} = \dfrac{(r+1)\,r!}{4^r \times 4}\,\dfrac{4^r}{r!} = \dfrac{r+1}{4}$.

La suite (α_r) est croissante dès que $r \geq 3$ et on constate aisément que $\lim_{r \to +\infty} \alpha_r = +\infty$. De plus :

$$\alpha_r \geq 1 \iff r \geq 10.$$

Retournons au problème :

$$\frac{n-1+k}{2} \geq r$$

Si $k \geq 2n$: $\dfrac{n-1+k}{2} \geq \dfrac{3n-1}{2}$.

Si $n \geq 7$: $\dfrac{n-1+k}{2} \geq 10$

et donc : $\dfrac{Q(M(n,k))}{N\,Q(M(n,k))} > 1$.

En conclusion :

pour $n \geq 7$:

$$k \geq 2n \Rightarrow \frac{Q(M(n,k))}{N\,Q(M(n,k))} > \frac{r!}{2^{2r+1}} \geq 1 \quad \text{avec} \quad r = \left\lfloor \frac{n-1+k}{2} \right\rfloor$$

et : $\lim\limits_{\substack{k \to +\infty \\ k \geq 2n}} \dfrac{Q(M(n,k))}{N\,Q(M(n,k))} = +\infty$.

Donc $E(n) = +\infty$.

Exemples :

On montre par le calcul que :

$E(24) \geq 48$; $E(48) \geq 96$.

On a donc : $E(24) = E(48) = +\infty$.

Problème :

Existe-t-il d'autres nombres n tels que $E(n) = +\infty$?

Remarque :

J.P. MASSIAS a tabulé $E(n)$, pour $n \leq 10000$. La plus grande valeur trouvée a été : $E(5040) = 10$, pour $n \neq 24, 46$.

Proposition 1. 2 [ERD - NIC] :

Soit $\varepsilon > 0$ et soit k un entier strictement positif. On écrit : $n(n+1) = U_k V_k$ avec

$$p \mid U_k \Rightarrow p \leq k, \quad p \mid V_k \Rightarrow p > k.$$

Alors : $\exists\, n_0(k, \varepsilon)$, $\forall\, n \geq n_0$, $U_k \leq n^{1+\varepsilon}$.

Conjecture 1.1 :

Quand n a pour limite $+\infty$: $Q((n+1)\ldots(n+k)) = n^{2+o(1)}$ (k fixé).

Définition 1.2 :

Un entier $m \geq 1$ est dit squarefull ("quadratiquement saturé") si : $N Q(m) = 1$.

Ceci est équivalent à dire : $\exists\, X \in \mathbf{N}^*$, $\exists\, Y \in \mathbf{N}^*$, $m = X^2 Y^3$.

Exemple :

Les nombres squarefull inférieurs à 120 sont :

1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 72, 81, 100, 108.

Proposition 1.3 :

Il existe une infinité de n pour lesquels n et $n+1$ sont simultanément squarefull.(On peut condidérer les solutions de l'équation de Pell : $X^2 - 8Y^2 = 1$, à savoir les nombres que l'on obtient en écrivant : $(3 + \sqrt{8})^m = X + Y\sqrt{8}$, soit (3, 1), (17, 6), (99, 35), ...).

Problème :

Existe-t-il trois nombres squarefull consécutifs ?

On observe par le tableau ci-dessous que 119 ne peut pas s'écrire comme somme de trois nombres squarefull.

m, n	119 - m	119 - m - n
108	11	2, 3, 7
100	19	3, 10, 11, 15
81	38	2, 6, 11, 13, 22, 29, 30, 34
72	47	11, 15, 20, 22, 31, 38, 39, 43
64	55	6, 19, 23, 28, 30, 39, 46, 47, 51
49	70	6, 21, 34, 38, 43, 45, 54, 61, 62, 66
36	83	2, 19, 34, 47, 51, 56, 58, 67, 74, 75, 79
32	87	6, 23, 38, 51, 55, 60, 62, 71, 78, 79, 83
27	92	11, 28, 43, 56, 60, 65, 67, 76, 83, 84, 88
25	94	13, 30, 45, 58, 62, 67, 69, 78, 85, 86, 90
16	103	3, 22, 39, 54, 67, 71, 76, 78, 87, 94, 95, 99
9	110	2, 10, 29, 46, 61, 74, 78, 83, 85, 94, 101, 102, 106
8	111	3, 11, 30, 47, 62, 75, 79, 84, 86, 95, 102, 103, 107
4	115	7, 15, 34, 51, 66, 79, 83, 88, 90, 99, 108, 107, 111

Conjecture 1.2. :

Tout nombre supérieur à 120 peut s'écrire comme somme de trois nombres squarefull.

Récemment, HEATH-BROWN a montré le théorème suivant :

Théorème 1.1 :

Il existe des constantes effectives p_0 et n_0 telles que : tout $n \geq n_0$ est représentable par l'une des trois formes suivantes : $x^2 + y^2 + z^2$, $x^2 + y^2 + 8z^2$, $x^2 + y^2 + p^3 z^2$, où $p \leq p_0$ est un nombre premier avec $p \equiv 5$ modulo 8.

Cela entraîne que tout nombre $n \geq n_0$ est somme de trois nombres squarefull.

2. Suites primitives :

Définition 2.1 :

Une suite strictement croissante d'entiers positifs $(a_i)_{i \in \mathbf{N}}$ est dite primitive si et seulement si :

$$\forall\, i<j \ , \ a_i \mid a_j.$$

Exemples :

1. $\{ \pi_1, \pi_2, \ldots \}$

2. $\{ \pi_j \pi_{j+1}, \pi_j \pi_{j+2}, \dots \}$.

Théorème 2.1 [ERD] :

Si (a_i) est une suite primitive, alors :

$$\sum_{i=1}^{\infty} \frac{1}{a_i \log a_i} < +\infty.$$

Remarque :

Pour démontrer ce théorème, on montre en fait que :

$\sum_{n=1}^{\infty} \frac{1}{a_n} \prod_{p \leq P_n} \left(1 - \frac{1}{p}\right) \leq 1$, où P_n est le plus grand facteur premier de a_n.

Conjecture 2.1 :

Pour toute suite primitive (a_i), on a :

$$\sum_{i=1}^{+\infty} \frac{1}{a_i \log a_i} \leq \sum_{i=1}^{+\infty} \frac{1}{\pi_i \log \pi_i}.$$

3. Problèmes faisant intervenir d(n) :

On rappelle que $d(n)$ est le nombre de diviseurs de n :

si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, $d(n) = (\alpha_1 + 1) \dots (\alpha_k + 1)$.

Théorème 3.1 [SPI] :

Il existe une infinité de n pour lesquels

$d(n) = d(n + 5040)$.

Théorème 3.2 [HEA 1] :

Il existe une infinité de n pour lesquels

$d(n) = d(n + 1)$.

Proposition 3.1 :

Soient $q_1, \dots, q_8$ huit nombres premiers impairs distincts. Alors :

$2520 \mid \text{ppcm}(q_j - q_i)_{1 \leq i < j \leq 8}$.

Démonstration :

Rappelons le principe des tiroirs de Dirichlet : si on range $k + 1$ objets dans k boîtes, il y a au moins une boîte qui contient deux objets.

Pour $m \in \{5, 7, 8, 9\}$, on va chercher dans quelles classes modulo m, on peut trouver

des nombres premiers $p > 7$.

m	classes
5	1, 2, 3, 4
7	1, 2, 3, 4, 5, 6
8	1, 3, 5, 7
9	1, 2, 4, 5, 7, 8

On en déduit que, pour chaque $m \in \{5, 7, 8, 9\}$, il y a au moins deux nombres parmi les $q_1, \ldots, q_8$ qui sont congrus modulo m. Donc :

$$\forall\ m \in \{5, 7, 8, 9\}, \quad m \mid \text{ppcm}\,(q_j - q_i)_{1 \le i < j \le 8}.$$

Par suite :

$$2520 = 2^3 \times 3^2 \times 5 \times 7 \mid \text{ppcm}\,(q_j - q_i)_{1 \le i < j \le 8}.$$

Théorème 3.3 [MOR] :

Pour tout octuplet de nombres premiers $q_1, \ldots q_8$, on a

$$5040 \mid \text{ppcm}\,(q_j - q_i)_{1 \le i < j \le 8}.$$

Pour démontrer le théorème 3.2, l'auteur considère des k - uplets de nombres $n_1 < \ldots < n_k$ vérifiant :

$$(*)\quad \forall\ i < j\ ,\ n_j - n_i \mid n_i.$$

Proposition 3.2 :

Pour tout $k > 1$, il existe un k - uplet vérifiant $(*)$.

Démonstration :

. $k = 2$: si p est premier : $\{p, 2p\}$ convient.

. soit $\{n_1, \ldots, n_{k-1}\}$ vérifiant $(*)$. On définit :

$$m_k = \text{ppcm}\,(n_1, \ldots, n_{k-1})$$

$$m_i = m_k - n_{k-i}\ ,\ 1 \le i \le k - 1.$$

Il est facile de voir que $\{m_1, \ldots, m_k\}$ vérifient $(*)$.

Exemple : voici les plus petites suites (ordre sur n_1) d'ordre k.

k								
2	1	2						
3	2	3	4					
4	6	8	9	12				
5	36	40	42	45	48			
6	210	216	220	224	225	240		
7	14 976	14 980	14 994	15 000	15 008	15 015	15 120	
8	552 720	552 825	552 960	553 000	553 014	553 140	553 280	554 400

Remarques :

1. Les plus grands nombres de ces suites sont hautement composés.

(i.e : n est hautement composé si : $\forall\, m < n,\ d(m) < d(n)$, cf. [RAM]).

2. La suite pour $k = 6$ a été trouvée par BALOG.

Les suites pour $k = 7$ et $k = 8$ ont été trouvées par le rédacteur en utilisant la démarche suivante.

Soit $n_1 < \ldots < n_k$ une suite vérifiant $(*)$. On pose :

$$n_j = n_1 + a_j\ , \quad 2 \le j \le k.$$

La condition $(*)$ s'écrit :

(1) $\forall\ j \in 2 \ldots k,\ a_j \mid n_1$.

(2) $\forall\ 2 \le i < j \le k, \quad a_j - a_i \mid n_1 + a_i = n_i$.

On définit alors le graphe suivant :

$G = (V, E)$ avec :

$V = \{d, d \mid n_1\} = \{d_1, \ldots, d_k\}$, $K = d(n_1)$.

$(d_i, d_j) \in E \Leftrightarrow |d_j - d_i| \mid n_1 + d_i$.

La propriété (2) traduit le fait que $(a_2, \ldots, a_k)$ est un sous-graphe complet d'ordre $k - 1$ du graphe G.

Des algorithmes sont connus pour résoudre ce problème ([BY], [KNU]).

Rechercher $n_1 < \ldots < n_k$ vérifiant $(*)$ se fait par une étude systématique du graphe correspondant.

Les calculs ont été effectués à l'aide d'un goupil G4 (compatible IBM-PC).

3. Pour d'autres propriétés de ces k - uplets, voir [HEA 2].

Proposition 3.3 :

Si $\{n_1, \ldots, n_k\}$ vérifient $(*)$, alors : $k \leq d(n_1)$, $\quad k > 3$.

Démonstration :

1) $k \leq d(n_1) + 1$:

comme $\{n_1, \ldots, n_k\}$ vérifient $(*)$:

$\forall\, j \in 2 \ldots k$: $\quad n_j - n_1 \mid n_1$.

Les valeurs possibles pour n_j $(2 \leq j \leq k)$ sont de la forme $n_1 + d$, avec $d \mid n_1$: cela fait au plus $d(n_1)$ valeurs.

2) $k \leq d(n_1)$:

Cherchons à quelle condition $n_k = 2n_1$ peut convenir pour faire partie d'une suite vérifiant $(*)$.

On a alors :

$$\forall\, j \in 2..(k-1),\ n_k - n_j \mid n_j, \quad \text{avec } n_j = n_1 + d_j,\ d_j \mid n_1.$$

Autrement dit

$$n_1 - d_j \mid n_1 + d_j \text{ , soit } \frac{n_1}{d_j} - 1 \ \Big|\ \frac{n_1}{d_j} + 1.$$

Cela n'est possible que si $d_j = \dfrac{n_1}{2}$ ou $\dfrac{n_1}{3}$.

Alors : Card $\{ j \mid 2 \leq j \leq k-1 \text{ et } 2n_1 - n_j \mid n_j \} \leq 2$.

Donc : si $k > 3$, $2n_1$ ne peut convenir : $k \leq d(n_1)$.

si $k = 3$ et si $d(n_1) = 2$, n_1 est premier : on a comme solutions :

$\{2, 3, 4\}$, $\{3, 4, 6\}$.

si $k = 2$: on a : $\forall\, n_1$, $d(n_1) \geq 2$.

Estimations de n_1, n_k :

On a : $\quad \forall\, n,\ d(n) \leq \exp\left((1 + o(1)) \dfrac{\log n}{\log 2 \log\log n} \right)$

D'où : $\quad k \leq \exp\left(\dfrac{\log n_1}{\log 2 \log_2 n_1} (1 + o(1)) \right)$,

soit $\quad \log 2 \log_2 n_1 \log k \leq \log n_1 (1 + o(1))$,

et $\quad \log_2 n_1 (1 + o(1)) \geq \log_2 k$.

Par suite : $\quad \log n_1 \geq \log 2 \log k \log_2 k \ (1 + o(1))$.

Théorème 3.4 [HEA 2] :

$\forall\ n_1 < \ldots < n_k$ vérifiant $(*)$:

$\log n_k >> k \log k.$

Enfin : on a vu que le plus grand diviseur d de n_1 tel que $n_1 + d$ soit dans la suite est strictement inférieur à n_1. Le plus grand diviseur possible est alors $\frac{n_1}{p}$ où p est le plus petit facteur premier de n_1.

En général : $\frac{n_1}{p} \leq \frac{n_1}{2}$.

Donc : $n_k \leq \frac{3n_1}{2}$.

Une fonction concernant les diviseurs premiers de n :

Soit $n > 1$: $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, $p_1 < p_2 < \ldots < p_r$: $\omega(n) = r$.

On pose : $f(n) = \sum_{1 \leq i < j \leq r} \frac{1}{p_j - p_i}$.

Problème : A-t-on toujours : $f(n) < C\ \omega(n)$?

Soit $a = \{a_1 < a_2 < m\}$ une famille définie par :

$$A(x) = \sum_{a_i \leq x} 1.$$

On suppose que a vérifie la condition suivante :

$$\exists\ c > 0,\ \forall\ t > 1,\ A(x + t) - A(x) \leq c \frac{t}{\log t} \quad (1)$$

De telles familles existent : par exemple $a = \{\pi_1, \ldots, \pi_k, \ldots\}$ et $c = 2$ (théorème de Brun - Titschmarsch).

Proposition 3.4 :

Si $\mathcal{A}(n) = \sum_{1 \leq i < j \leq n} \frac{1}{a_j - a_i}$, alors :

$$\exists\ C > 0,\quad \mathcal{A}(n) \leq C\ n \log \log n.$$

Démonstration :

On écrit :

$$\mathcal{A}(n) = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \frac{1}{a_j - a_i}$$

$$\mathcal{A}(n) = \sum_{i=1}^{n-1} \left(\frac{1}{a_{i+1} - a_i} + \sum_{j=i+2}^{n} \frac{1}{a_j - a_i} \right)$$

$$= \sum_{i=1}^{n-1} \frac{1}{a_{i+1} - a_i} + \sum_{i=1}^{n-2} \sum_{j=i+2}^{n} \frac{1}{a_j - a_i}.$$

Comme : $a_{i+1} \geq a_i + 1$, on a :

$$\sum_{i=1}^{n-1} \frac{1}{a_{i+1} - a_i} = O(n).$$

Posons : $\mathcal{B}(n) = \sum_{i=1}^{n-2} \sum_{j=i+2}^{n} \frac{1}{a_j - a_i}$.

On remarque alors que :

$$A(a_j) = \sum_{a_i < a_j} 1 = j.$$

De (1), on déduit :

$$A(a_i + (a_j - a_i)) - A(a_i) \leq \frac{c(a_j - a_i)}{\log(a_j - a_i)} \quad \text{pour} \quad j \geq i+2$$

relation valide car $a_j \geq a_{i+2} > a_{i+1} \geq a_i + 1$: $a_j - a_i \geq 2$.

D'où : $$j - i \leq \frac{c(a_j - a_i)}{\log(a_j - a_i)} \quad : (2).$$

Par suite : $c(a_j - a_i) \geq (j - i) \log(a_j - a_i) \geq \log 2 (j - i)$.

Si $c_1 = \frac{\log 2}{c}$, on a : $\log(a_j - a_i) \geq \log c_1 + \log(j - i)$.

De (2), on tire : $a_j - a_i \geq \frac{1}{c}(j - i)(\log c_1 + \log(j - i))$

$$a_j - a_i \geq \frac{1}{c_2}(j - i) \log(j - i).$$

Alors :

$$\frac{1}{a_j - a_i} \leq \frac{c_2}{(j - i) \log(j - i)}.$$

D'où :

$$\mathcal{B}(n) \leq \sum_{i=1}^{n-2} \sum_{j=i+2}^{n} \frac{c_2}{(j - i) \log(j - i)}.$$

$$\mathcal{B}(n) \leq \sum_{i=1}^{n-2} \sum_{k=2}^{n-i} \frac{c_2}{k \log k}.$$

$$\mathcal{B}(n) \leq \sum_{i=2}^{n-1} \sum_{k=2}^{i} \frac{c_2}{k \log k}, \text{ en changeant } i \text{ en } n-i.$$

On pose ensuite :

$$B(i) = \sum_{k=2}^{i} \frac{1}{k \log k}.$$

La fonction $x \to \frac{1}{x \log x}$ est décroissante pour $x \geq 2$. On en déduit la majoration :

$$B(i) \leq \frac{1}{2 \log 2} + \int_2^i \frac{dx}{x \log x}$$

$$B(i) \leq \frac{1}{2 \log 2} + [\log \log x]_2^i$$

$$B(i) \leq \log \log i + c_3.$$

D'où : $\mathcal{B}(n) \leq c_2 \sum_{i=2}^{n-1} B(i) \leq c_2 \left(c_3 (n-2) + \sum_{i=2}^{n-1} \log \log i \right)$.

Il est facile de voir que : $\sum_{i=2}^{n-1} \log \log i = O(n \log \log n)$.

On en déduit donc :

$$\mathcal{B}(n) = O(n \log \log n).$$

$$\mathcal{A}(n) = O(n \log \log n).$$

Remarque :

Il n'est pas vrai que :

$$\mathcal{A}(n) < Cn \text{ pour tout } a.$$

Rusza a donné le contre - exemple suivant :

$$a = \bigcup_{k=0}^{\infty} \left\{ \sum_{i=0}^{k} \varepsilon_i 2^i \text{ , avec } \varepsilon_i \in \{0,1\} \text{ et } i = 2^r \Rightarrow \varepsilon_i = 0 \right\}.$$

D'où :

$$a = \{0, 1, 8, 9, 32, 33, 40, 41, 64, 65, 72, 73, 96, 97, 104, 105, \ldots\}.$$

On pose, pour $k \neq 2^a$:

$$a_k = \{ x \in a \ ; \ 2^k \leq x < 2^{k+1} \}$$

Alors :

$$a = \bigcup_{\substack{k=0 \\ k \neq 2^a}}^{\infty} a_k.$$

Soit $k \neq 2^a$ et soit $a \in \mathbf{N}$ défini par $2^a < k < 2^{a+1}$ on voit que

$$\text{card}\ \partial_k = 2^{k-a} > 2^k / k$$

et

$$\sum_{\substack{j \le k \\ j \neq 2^a}} \text{card}\ \partial_j = 2^{k-a+1} \le 4\, 2^k / k$$

Nous montrons :

Proposition 3.5 :

Il existe des constantes effectives c_1 et $c_2 > 0$ telles que, pour $x \ge 2$, on ait :

$$c_1 \frac{x}{\log x} < A(x) < c_2 \frac{x}{\log x}.$$

Démonstration :

On définit k par $2^k \le x < 2^{k+1}$. On a alors :

si $k - 1 \neq 2^a$, $\quad A(x) \ge \text{card}\ \partial_{k-1} \ge 2^{k-1} / k - 1$

si $k - 1 = 2^a$, $\quad A(x) \ge \text{card}\ \partial_{k-2} \ge 2^{k-2} / k - 2$

dans les deux cas,

$$A(x) \ge \frac{1}{8} \frac{2^{k+1}}{k+1}$$

et comme la fonction $t \to 2^t / t$ est croissante et que $k + 1 \ge \dfrac{\log x}{\log 2}$,

$$A(x) \ge \frac{\log 2}{8} \frac{x}{\log x}.$$

Pour la majoration de $A(x)$, on a :

si $k \neq 2^a$,

$$A(x) \le \sum_{\substack{j \le k \\ j \neq 2^a}} \text{card}\ \partial_j \le 4\, 2^k / k$$

si $k = 2^a$

$$A(x) \le \sum_{\substack{j \le k-1 \\ j \neq 2^a}} \text{card}\ \partial_j \le 4\, 2^{k-1} / k - 1$$

Dans les deux cas, on a, pour $k \ge 2$:

$$A(x) \le 4 \frac{2^k}{k} \le 4 \log 2 \frac{x}{\log x}.$$

La formule est encore valable pour $2 \le x < 4$, soit $k = 1$, puisque $A(x) = 2$.

Cela démontre la proposition avec $c_1 = \dfrac{\log 2}{8}$ et $c_2 = 4 \log 2$.

Théorème 3.5 :

$$\exists\ c > 0,\ \forall\ t > 1,\quad A(x + t) - A(x) \le c \frac{t}{\log t}.$$

Démonstration :

Soient x et t deux entiers plus grands que 1. On cherche à compter les a dans $\mathcal{A}$ tels que :

$$x < a < x + t.$$

On décompose a comme suit : $a = a_1 + a_2$, avec :

$$a_1 = \sum_{j \leq \lfloor \frac{\log t}{\log 2} \rfloor} \varepsilon_j 2^j \ , \ a_2 = \sum_{j > \lfloor \frac{\log t}{\log 2} \rfloor}^{K} \varepsilon_j 2^j.$$

Posant : $T = \lfloor \frac{\log t}{\log 2} \rfloor$, on voit que :

$$a_1 < 2^{T+1} < 2t.$$

et $\quad a_2 = 2^T m$, m entier.

Comme : $\quad x - 2t < x - a_1 < a_2 < x + t,$

on a : $\quad x - 2t < 2^T m < x + t.$

Comme $\frac{t}{2} < 2^T \leq t$, m ne peut prendre au plus qu'un nombre fini de valeurs.

D'autre part, le nombre de choix possibles pour a_1 est borné a :

$$A(2^{T+1} - 1) << \frac{2^T}{T} << \frac{t}{\log t}.$$

D'où on conclut que :

$$A(x + t) - A(x) < c \frac{t}{\log t}.$$

Retour à $\mathcal{A}(n)$:

Proposition 3.6 :

$$\exists \ c > 0 \ , \ \exists \ N_0, \ N \geq N_0 \Rightarrow \mathcal{A}(N) \geq c \ N \log\log N.$$

Démonstration : (cette démonstration nous a été communiquée par Mr RUSZA lui-même).

Nous cherchons à estimer :

$\mathcal{A}(n) = \sum_{1 \leq i < j \leq N} \frac{1}{a_j - a_i}$, avec $N = 2^{n - r(n)}$, si $2^{r(n)} \leq n < 2^{r(n+1)}$. Tous les a_i sont dans $[0, 2^n[$.

Soit k un entier positif. On définit la fonction F_k par :

$$F_k(a, b) = \begin{cases} 1 \ \text{s'il existe } m \text{ tel que, } (a, b) \in ([m2^k \ , \ (m+1)2^k [ )^2 \\ 0 \ \text{sinon.} \end{cases}$$

Si $b - a \geq 2^k$, alors $F_k(a, b) = 0$.

Montrons le lemme suivant :

Lemme :

Supposons $a < b$. Alors :

$$\sum_{k=0}^{+\infty} 2^{-k} F_k(a,b) \leq \frac{2}{b-a}. \qquad (\S)$$

Démonstration :

Il existe un unique $K \geq 0$ tel que : $2^K < b-a \leq 2^{K+1}$.

Alors : $\sum_{k=0}^{+\infty} 2^{-k} F_k(a,b) \leq \sum_{k=K+1}^{\infty} 2^{-k} \times 1 = 2^{-K} \leq \frac{2}{b-a}$.

Estimons maintenant : $S_k(N) = \sum_{i<j\leq N} F_k(a_i, a_j)$, pour k fixé, $k \geq 2$.

Tous les a_i sont dans $2^{(n-r(n))-(k-r(k))}$ intervalles de longueur 2^k, avec $2^{k-r(k)}$ nombres dans chacun de ces intervalles. Alors :

$$S_k(N) = 2^{(n-r(n))-(k-r(k))} \sum_{1\leq i<j\leq 2^{k-r(k)}} 1,$$

$$= 2^{(n-r(n))-(k-r(k))} \binom{2^{k-r(k)}}{2} > 2^{(n-r(n))+(k-r(k))-2}.$$

Avec (§), on obtient :

$$\mathcal{A}(N) = \sum_{1\leq i<j\leq N} \frac{1}{a_j - a_i} \geq \sum_{1\leq i<j\leq N} \frac{1}{2} \sum_{k=0}^{+\infty} 2^{-k} F_k(a_i, a_j)$$

$$\geq \frac{1}{2} \sum_{k=2}^{n} 2^{-k} \cdot S_k(N).$$

D'où :

$$\mathcal{A}(N) \geq \sum_{k=2}^{n} 2^{n-r(n)-r(k)-3} = \frac{N}{8} \sum_{k=2}^{n} 2^{-r(k)}.$$

Par suite :

$$\mathcal{A}(N) \geq \frac{N}{8} \sum_{k=2}^{n} \frac{1}{k} > c\, N \log\log N,$$

ce qui démontre le résultat.

Quelques fonctions faisant intervenir les diviseurs de n :

On rappelle que $d(n) = \sum_{d \mid n} 1$: n a $d(n)$ diviseurs : $d_1 < d_2 < \ldots < d_{d(n)}$.

On définit : $g(n) = \sum_{1\leq i\leq d(n)-1} \frac{1}{d_{i+1} - d_i}$.

Proposition 3.7 :

1) $g(n) \leq \exp\left(\frac{c \log n}{\log_2 n}\right)$, où $\log_2 n = \log\log n$.

2) Pour tout $\varepsilon > 0$, l'inégalité

$$g(n) > \exp\{(\log n)^{\frac{1}{2}-\varepsilon}\}$$

est vraie pour une infinité de nombres n.

Démonstration :

1) $g(n) \leq \sum_{1 \leq i \leq d(n)-1} 1 = d(n) - 1.$

Or, d'après [ROB] :

$$\forall\ n \geq 3, \quad \frac{\log d(n)}{\log 2} \leq 1,5379\ \frac{\log n}{\log_2 n}.$$

On a bien : $g(n) \leq \exp\left(c\ \frac{\log n}{\log_2 n} \right)$.

2) Considérons le problème d'optimisation en nombres réels :

$$\left| \begin{array}{l} \text{Min} \sum_{i=1}^{M} \frac{1}{a_i} \\ \sum_{i=1}^{M} a_i = C, \ M \text{ étant fixé et } C \text{ une constante.} \end{array} \right.$$

La solution de ce problème est : $\forall i,\ a_i = \frac{C}{M}$.

D'où : $\forall\ (a_i)_{1 \leq i \leq M},\ \sum_{i=1}^{M} \frac{1}{a_i} \geq \frac{M^2}{C}$.

Revenons à notre problème et posons :

$$G_n(x) = \sum_{\substack{1 \leq i < d(n) \\ d_i \leq x}} \frac{1}{d_{i+1} - d_i}.$$

Choisissons désormais n de la forme $n_k = \pi_1 \ldots \pi_k$.

On définit, pour tout entier $m \geq 2$: $P(m) = \max_{\substack{p \text{ premier} \\ p \mid m}} p$ (et $P(1) = 1$).

Alors $d \mid n_k \Leftrightarrow \left\{ \begin{array}{l} P(\leq \pi_k \\ \text{et } d \text{ est squarefree. (i. e. : } p \mid d \Rightarrow p^2 \nmid d) \end{array} \right.$

Pour $x \geq 0$, on définit :

$$\psi_1(x, y) = \text{Card}\ \{ d \leq x,\ P(d) \leq y \text{ et } d \text{ squarefree} \}.$$

Pour les estimations de ψ_1, voir [IV - TEN].

Reportons n_k dans G :

$$G_{n_k}(x) = \sum_{\substack{1 \leq i < d(n_k) \\ d_i \leq x}} \frac{1}{d_{i+1} - d_i}.$$

Le nombre de termes dans la somme est :

$$\sum_{\substack{1 \leq i < d(n_k) \\ d_i \leq x}} 1 = \psi_1(x, \pi_k).$$

D'autre part :

$$\sum_{\substack{1 \leq i < d(n_k) \\ d_i \leq x}} (d_{i+1} - d_i) = d_h - 1,$$

où d_h est le diviseur de n_k vérifiant $d_{h-1} \leq x < d_h$. Comme $P(n_k) \ \pi_k$, on en déduit que :

$d_h \leq \pi_k \ d_{h-1} \leq \pi_k x$.

Comparant avec le problème d'optimisation, on trouve :

$$G_{n_k}(x) \geq \frac{\psi_1(x, \pi_k)^2}{\pi_k x}.$$

Nous allons maximiser cette dernière expression en x.

Alors :

1) $\exists\ x_0(\varepsilon),\ \forall\ x \geq x_0(\varepsilon),\ \forall\ y,\ \log^{2+\varepsilon} x < y \leq x,\ \beta(x, y) \geq \frac{1}{2} + \frac{\varepsilon}{6}$.

2) $\psi_1(x, y) \geq \frac{1}{\zeta(2\beta)}\ \psi(x, y)\ (1 + o(1))$, uniformément pour $0 < \varepsilon < 1$, où ζ est la fonction de Riemann et ψ la fonction de De Bruijn [BRU] : $\psi(x, y) = \sum_{\substack{n \leq x \\ P(n) \leq y}} 1$.

Proposition 3.8 : [IV - TEN]

On pose : $u = \frac{\log x}{\log y}$ pour $2 \leq y \leq x$. On définit $\xi = \xi(u)$ comme étant l'unique racine positive de : $e^{\xi} = 1 + u\xi$ si $u > 1$ et $\xi(1) = 0$. On définit également la fonction :

$$\beta = \beta(x, y) = 1 - \frac{\xi(u)}{\log y}.$$

Soit ε un réel vérifiant $0 < \varepsilon < 1$.

D'après [CAN - ERD - POM], on a :

$$\forall\ x \geq 10,\ \forall\ y \geq \log^{1+\varepsilon} x,\ \psi(x, y) \geq \frac{x}{u(1 + o(1))}.$$

Par suite, si $y = \pi_k$, on en déduit qu'il existe $\delta > 0$ tel que :

$$\psi(x, \pi_k) \geq \frac{x}{y \cdot u^{u(1+\delta)}}.$$

On en déduit :

$$G_{n_k}(x) \geq C\ \frac{x}{y \cdot u^{2u(1+\delta)}}.$$

On pose : $f(x, y) = \frac{x}{u^{2u(1+\delta)}}$ et on cherche à maximiser f pour y fixée ($u = \pi_k$).

On a : $x = y^u$, $\log f(x, y) = u(\log y - 2(1 + \delta) \log u)$.

On trouve :

$$\log u - 2(1 + \delta) \log u - 2(1 + \delta) = 0,$$

soit :

$$u_0 = \frac{y^{\frac{1}{2(1+\delta)}}}{e},$$

et donc :

$$\log x = \frac{1}{e}\, y^{\frac{1}{2(1+\delta)}} \log y.$$

Par suite,

$$f(x, y) \leq \exp\left[\frac{2(1+\delta)}{e}\, y^{\frac{1}{2(1+\delta)}}\right].$$

On en déduit :

$$G_{n,k}(x) \geq \frac{C}{y} \exp\left\{\frac{2(1+\delta)}{e}\, y^{\frac{1}{2(1+\delta)}}\right]$$

$$\geq \exp\left[\frac{2(1+\delta)}{e}\, y^{\frac{1}{2(1+\delta)}} - \log y\right].$$

Or $y = \pi_k \sim \log n_k$. Donc pour k assez grand : $g(n_k) \geq G_{n_k}(x) \geq \exp\{(\log n_k)^{\frac{1}{2}-\varepsilon}\}$.

Soit $\zeta_k(n) = \{ a \mid n,\ a = t(t+1) \ldots (t+k-1) \}$.

Théorème 3.6 [ERD - HAL] :

Pour tout k fixé, tout $A < e^{1/k}$ fixé, on a : $\tau_k(n) > (\log n)^A$ pour une infinité de n.

Remarque :

Pour $k = 2$, $e^{1/k} = 1,649\ldots$

Conjecture 3.1 :

Dans le cas $k = 2$, le théorème précédent est vrai pour tout $A > 1$. G. Tenenbaum m'a signalé avoir montré cette conjecture avec Balog.

On pose : $f(n) = \sum_{\substack{d_i \mid n \\ (d_i, d_{i+1}) = 1}} 1.$

Proposition 3.9 :

$\forall\ n,\ f(n) \geq \omega(n)$.

Démonstration :

En effet, si p premier divise n, le diviseur de n immédiatement inférieur à p est premier avec p.

Théorème 3.7. (Erdös et Tenenbaum, [ERD - TEN]) :

$$\forall\ \varepsilon > 0,\ \exists\ x_0(\varepsilon),\ x \geq x_0 \Rightarrow \operatorname{Max}_{n \leq x} f(n) > \exp\left(\frac{c \log x}{(\log\log x)^2}\right)$$

avec $c = \frac{1}{2} (\log 2)^2 - \varepsilon$.

Théorème 3.8. [ERD - TEN] :

$\forall \varepsilon > 0, \quad f(n) < (\log n)^{\log 2 - \frac{1}{2} + \varepsilon}$ pour presque tout n.

Problème :

On ne sait presque rien sur :

$$\sum_{\substack{d_i, d_i+1, d_i+2 \\ \text{premiers entre eux deux à deux} \\ d_j \mid n}} 1.$$

Théorème 3.9. [MAI - TEN] :

Si $E(n) = \inf_{\substack{d \mid n,\ d' \mid n \\ d < d'}} \log \frac{d'}{d}$, et si $\xi(n)$ est n'importe quelle fonction tendant vers $+\infty$ avec n,

on a : pour presque tout n : $E(n) \leq (\log n)^{1 - \log 3} \exp \{ \xi(n) \sqrt{\log \log n} \}$.

Corollaire :

Pour presque tout n, il existe $d < d'$, $d \mid n$, $d' \mid n$ et :

$$d < d' \leq 2d.$$

Remerciements :

Je tiens à remercier J.L. Nicolas pour m'avoir incité à rédiger cette conférence et pour son aide durant ce travail. D'autre part, je remercie G. Tenenbaum pour les remarques qu'il m'a faite après lecture de la version préliminaire.

François Morain
Département de Mathématiques
Université de Limoges
123 Avenue Albert Thomas
F - 87060 LIMOGES CEDEX

Bibliographie

[BRU] N. G. DE BRUIJN. - On the Number of Positive integers $\leq y$ and free of prime factors $> y$, II -. Nederl. Akad. Wetensch. Proc. Ser 169 (1966), p. 239 - 247.

[BY] E. BALAS - C.S. YU. - Finding a maximum clique in an arbitrary graph - SIAM J. ; Comput, V15, 4, (Nov. 1986), p. 1054 - 1068.

[CAN -ERD-POM] E.R. CANFIELDS- P. ERDÖS - C. POMERANCE. - On a Problem of Oppenheim concerning "Factorisatio Numerorum" -. J. of N. Theory 17, (1883) p. 1 - 28.

[ERD] Paul ERDÖS. - Note on sequences of integers no one of which is divisible by any other -. J. London Math. Soc. 10 (1935) p. 126 - 128.

[ERD - HAL] P. ERDÖS - R. R. HALL. - On some unconventionnal problems on the divisors of integers -. J. Austral. Math. Soc. (Series A) 25 (1978) p. 479 - 485.

[ERD - TEN] P. ERDÖS - G. TENENBAUM. - Sur les fonctions arithmétiques liées aux diviseurs consécutifs -. J. of Number Theory ; à paraître.

[ERD - NIC] P. ERDÖS - J.L. NICOLAS. - Sur la fonction : nombre de facteurs premiers de N -. L'enseignement mathématique, II^{è} série, T. XXVII, fasc. 1 - 2 (1981) p. 3 - 27.

[HAR - WRI] G.H. HARDY-E.M. WRIGHT. - An introduction to the theory of numbers -. 4^{è} éd. (Clarendon Press, Oxford, 1960).

[HEA 1] D.R. HEATH - BROWN. - The divisor function at consecutive integers -. Mathematika 31 (1984), p. 141 - 149.

[HEA 2] D.R. HEATH - BROWN. - Consecutive almost primes. - (à paraître).

[HIL] A. HILDEBRAND. - Même titre -. (à paraître).

[IV-TEN] A. IVIC - G. TENENBAUM. - Local densities over integers free of large prime factors -. Quart. J. Math, Oxford (2), 37, (1986), p. 401-417.

[KNU] D.E. KNUTH. - The Art of Computer Programming VIII, Sorting and Searching -. ex 23 p. 10.

[MAI - TEN] H. MAIER - G. TENENBAUM. - On the set of divisors of an integer -. Inventiones Math. 76, (1984) p. 121 - 128.

[MOR] F. MORAIN. - On the lim of the differences of eight primes -. à paraître dans Mathematics of Computation.

[RAM] S. RAMANUJAN. - Highly composite numbers. - Proc. London Math. Soc. Série 2, 14 (1915), p. 347 - 400, Collected papers, 78 - 128, Chelsea.

[RID] D. RIDOUT. - Rationnal approximations to algebraic numbers -. Mathematika, 2 (1955), p. 1 - 20.

[ROB] G. ROBIN. - Thèse, - Grandes valeurs de fonctions arithmétiques et problèmes d'optimisation en nombres entiers - Limoges, (1983) -.

[SCH] W.M. SCHMIDT. - Approximation to algebraic numbers -. Enseignement Mathématique, 17 (1971), p. 187 - 253 et Monographies de l'Enseignement Mathématique n°19, 1972.

[SPI] C. A. SPIRO. - Thesis University of Illinois at Urbana , - The frequency with which an integral-valued, prime-independent, multiplicative or additive function of n divides a polynomial function of n. Urbana 1981 -.