Titre II
Premiers pas de l'Horloger

II.1 Approche générale

II.1.1 Axiomes retenus

Nous retenons, ici et ensuite, les axiomes de la Théorie élémentaire des Nombres Entiers. Et par conséquent, nous nous limitons à l'ensemble $\mathbb{Z}$ des nombres relatifs.

Nous avons cependant une hésitation vis-à-vis du « zéro ». Ce « zéro » qui est peut-être la plus grande trouvaille de l'Arithmétique, doit-il, comme le précise **Peano**, être uniquement considéré comme un nombre ?

La propriété des nombres est en effet de dénombrer ; or le signal « zéro » signifie qu'il n'y a rien à dénombrer ou bien plus rien à dénombrer.

Lorsqu'il s'agit du signal de position, « zéro » signifie, en effet, que la base de comptage que nous utilisons est dépassée et que le décompte se poursuit en utilisant les chiffres de la base choisie ajoutés aux puissances de 10 de ladite base selon :

$$a10^{\alpha} + b10^{\beta} + ... + z10^{0} = ab...z\,.$$
$$2014 = 2\times10^{3} + 0\times10^{2} + 10^{1} + 4 \text{ en base } 10$$
$$= 31024 = 3\times5^{4} + 5^{3} + 0\times5^{2} + 2\times5 + 4 \text{ en base } 5$$

Il apparaît que les puissances de 10 ou 5 jouent le rôle de cliquets, tels les échappements d'une horloge. Notons que l'utilisation d'exposants négatifs permet d'exprimer les nombres fractionnaires. Mais ce décompte ne permet pas d'atteindre le continuum du temps.

II.1.2 Rappels élémentaires

Rappelons qu'un nombre entier est premier si et seulement s'il n'est divisible que par 1 et par lui-même.

Lorsque l'on veut désigner un nombre pair quelconque, on écrit $2k$.

Lorsque l'on veut désigner un nombre impair quelconque, on écrit $2k+1$ ou encore $2k+\eta$ $(\eta = \pm 1)$; un tel nombre est premier par rapport à 2, car il n'est pas divisible par 2. Il est caractérisé par le paramètre $\boldsymbol{k}$ qui en permet les manipulations analytiques.

Sous son écriture en base arithmétique 10, il s'exprime en fait en base 2.

Les nombres premiers constituent un sous ensemble des nombres impairs et peuvent s'écrire $p_x = 2k+1$, le paramètre k devant être tel que le nombre premier de rang x ne soit pas composé.

II.1.3 Nombres impairs composés

Tout nombre impair composé peut s'écrire, en fonction de l'un de ses facteurs premiers p_i :

$$2k+1=(2q+1)\,p_i = p_i \bmod 2p_i \qquad (2.1)$$

en utilisant ainsi l'arithmétique modulaire des horloges où $a \bmod b = minutes \bmod(60)$, b désignant les heures pleines et a la quantité de minutes qui ne suffisent pas à constituer une heure entière.

Tel est le rouage de base de l'Horloge des Nombres.

II.1.4 Nombres impairs premiers par rapport à p_i

De tels nombres ne sont divisibles ni par 2 ni par p_i.

L'expression (2.1) devient donc, en retenant le reste r par excès ou par défaut de la division par $2p_i$:

$$2k+1 = 2p_i q \pm r$$

où r est un nombre impair (donc $\neq 0$ et 2) compris entre 1 inclus et $\frac{p_i}{2}$; (r est donc premier avec p_i) ; ce qui s'écrit encore :

$$2k+1 \equiv \eta\, r \bmod 2p_i \text{ , avec les mêmes conditions pour } r.$$

Inversement, toute expression $2p_i q \pm r$ représente un nombre premier par rapport à 2 et à p_i si et seulement si $0 < r < p_i$; en effet, $2p_i q$ étant divisible par 2 et par p_i, mais r ne l'étant pas, ladite expression n'est divisible ni par 2 ni par p_i. $2p_i$ constitue en fait la base implicite des nombres premiers par rapport à 2 et à p_i.

II.1.5 Nombres strictement premiers

Si nous envisageons tous les nombres premiers $p_i \leq \sqrt{2q+1}$, les nombres strictement premiers inférieurs ou égaux à $2q+1$ peuvent alors s'écrire :

$$2q+1 \equiv \eta\, r_i \bmod 2p_i \quad | \quad r_i \neq \eta\, p_i \quad \forall p_i \leq \left\lfloor \sqrt{2q+1} \right\rfloor$$

ηr_i étant le reste de la division de $2q+1$ par $2p_i$

II.1.6 Utilisation de différentes bases

- **En base** 2**,** comme déjà vu, $2q+1$ exprime l'ensemble des nombres impairs
- **En base** 4**,** l'expression $4q+r$ avec $r=\pm 1$ exprime aussi l'ensemble des nombres impairs
- **En base** 6**,** l'expression $6q+r$ avec $r=\pm 1$ exprime l'ensemble des nombres impairs premiers par rapport à 2 et à 3. Les nombres premiers 2 et 3 se trouvent exclus de cette représentation.

- Plus généralement, la base $\prod_{i=1}^{k} p_i$ permet l'écriture $q\prod_{i=1}^{k} p_i + r$ de tous les nombres premiers jusqu'en p_k **,** avec les conditions suivantes **:** le reste $r < \prod_{i=1}^{k} p_i$ ne doit comporter aucun facteur premier compris entre 2 et p_k inclus, il peut donc être égal à 1 **;** au contraire la factorisation du coefficient q ne doit comporter que des nombres premiers compris entre 2 et p_k inclus. Les nombres premiers de 2 à p_k échappent donc à cette écriture.

II.2 Nombres premiers par rapport à 2 et à 3

II.2.1 Leur écriture $6q+\eta$ avec $(\eta = \pm 1)$ exprime l'ensemble des nombres premiers avec 2 et 3, depuis 5 jusqu'à l'infini $\aleph_0$.

Cet ensemble est particulièrement intéressant, d'une part par la simplicité de sa formulation**,** d'autre part parce que les multiples de 2×3 constituent le plus important sous ensemble de nombres composés impairs après ajout de l'unité relative ± 1**.**

Nous exploiterons aussi loin qu'il nous sera possible les développements auxquels conduit l'écriture si simple

$$6q+\eta$$

où q, **paramètre** de ces nombres, va nous permettre une recherche analytique sur les nombres premiers.

II.2.2 Aînés, cadets et jumeaux

Nous baptisons **'aînés'** les nombres du type $6q+1$; nous baptisons **'cadets'** les nombres du type $6q-1$.

$6q-1$et $6q+1$ sont jumeaux ; ils sont '**premiers jumeaux**' lorsqu'ils sont tous deux premiers.

L'écriture $6q+\eta$ sera utilisée pour désigner indifféremment aînés ou cadets premiers en *2* et *3*.

Nous sommes ainsi amenés à employer deux types d'écriture pour les nombres premiers p_j qui font nécessairement partie du sous ensemble des nombres premiers par rapport à 2 et à 3:

- p_j , étant, selon l'écriture traditionnelle, le nombre premier de rang ou d'ordinal j,
- $p_{i,\eta}$, indiquant que l'on a recours à l'écriture paramétrique $6q\pm 1$ avec $q=i$ et $\eta = \pm 1$, écriture pour laquelle $p_{i,\eta}$ est égal au nombre premier particulier $6i+\eta$.

Le plus petit nombre $p_{i,\eta} = 6i+\eta$ est $p_3 = 6\times 1-1 = 5 = p_{1,-1}$.

Réciproquement, on trouvera, par exemple, que $p_{11,1} = 6\times 11+1 = 67 = p_{19}$

Les cadets premiers par rapport à 2 et à 3 s'écrivent sous la forme modulaire $-1 \bmod 6$

Les aînés premiers par rapport à 2 et à 3 s'écrivent sous la forme modulaire $+1 \bmod 6$.

Les écarts successifs entre nombres premiers par rapport à 2 et 3 sont :

2 entre jumeaux,

4 entre aîné et cadet consécutifs,

6 entre cadets ou aînés successifs,

$2a + 4b$ entre deux premiers quelconques par rapport à 2 et 3

II.2.3 Primalité relative des nombres jumeaux

Si un couple de jumeaux $(p,\ p+2)$ avait en commun un facteur premier $p_k > 2$, l'écriture

$$p = p_k \times a, \quad p+2 = p_k \times b$$

entraînerait $2 = p_k (b-a)$ ce qui serait absurde.

Il sera parfois intéressant de recourir au théorème de **Bachet de Méziriac** (si deux nombres a et b ont un PGCD égal à c, il existe au moins deux entiers relatifs x et y tels que l'on ait $xa + yb = c$) ; la réciproque n'étant vraie que si et seulement si $c = 1$.

Qu'ils soient premiers ou seulement premiers par rapport à 2 et à 3**,** aînés et cadets jumeaux vérifient la relation

$$3q(6q+1) - (3q+1)(6q-1) = 1 \qquad (2.2)$$

laquelle révèle un PGCD égal à 1, avec $x = 3q, \quad y = -(3q+1)$

L'expression (2.2) montre que non seulement les jumeaux $6q-1$ et $6q+1$ n'ont d'autre facteur commun que l'unité, mais qu'il en est de même des couples

$$(3q, 3q+1), (3q, 6q-1), (3q+1, 6q+1).$$

Dans la relation de **Bachet** de **Méziriac**, les coefficients x, y ne sont pas uniques ; il existe des jeux x', y' , en quantité illimitée et qui sont liés à x, y par les relations

$$x' = x + kb$$
$$y' = y - ka$$

Par convention implicite, on choisit les coefficients x, y issus de l'algorithme d'Euclide, lequel algorithme permet la démonstration du théorème de **Bachet**.

Les jumeaux $6q-1$ et $6q+1$ sont premiers entre eux.

II.2.4 Remarque sur les nombres premiers par rapport à 2,3 et 5 exprimés en base 6

Les nombres premiers par rapport à 2 et à 3, mais multiples de 5 ne peuvent se terminer par 0 puisqu'ils sont impairs ; ils se terminent donc par 5.

Pour être également premiers par rapport à 5 les cadets $6q-1$ devront donc être tels que $6q$ ne se termine pas par 6 ; autrement dit, q ne devra se terminer ni par 1, ni par 6.

De même, pour être premiers par rapport à 5, les aînés $6q+1$ devront être tels que $6q$ ne se termine pas par 4 ; autrement dit, q ne devra se terminer ni par 4, ni par 9.

En ce qui concernent les jumeaux, pour qu'ils soient simultanément premiers par rapport à 2, 3 et 5, il faut que q ne se termine pas par 1, 4, 6 ou 9 et donc que q^2 ne se termine ni par 1 ni par 6. Mais ce n'est pas suffisant.

II.3 Infinitudes

II.3.1 Infinitude des 'cadets premiers'

Cette infinitude résulte du théorème de la progression arithmétique dû à **Dirichlet :** parmi les nombres de la progression arithmétique $a \bmod b$, il existe une quantité illimitée de nombres premiers à condition que a et b soient premiers entre eux ; dans le cas contraire, cette progression ne comporte, au plus, qu'un seul nombre premier.

Ainsi, $6q-1$ peut aussi s'écrire $6(q-1)+5$ et comme 6 et 5 sont premiers entre eux, il y a une infinité de premiers de la forme $6q-1$.

On trouve même une expression du nombre des cadets d'après une extension du théorème de **Dirichlet** : soit en effet une progression arithmétique $aq+b$, où a et b sont premiers entre eux ; on démontre que la quantité ainsi produite de nombres premiers inférieurs à un nombre donné n, quantité que l'on baptise $\pi_{a,b}(n)$, tend vers $\dfrac{n}{\varphi(a)\ln n}$ lorsque n augmente indéfiniment, $\varphi(a)$ étant la fonction indicatrice d'Euler. Rappelons que cette fonction $\varphi(a)$ a pour valeur la quantité de nombres inférieurs à a et n'ayant aucun facteur premier avec a. Pour $a=6$, cette fonction a donc pour valeur 2, seuls 1 (par convention) et 5 n'ayant aucun diviseur commun avec 6.

$6q-1$ s'écrivant encore $6(q+1)-5$, il s'ensuit que $\pi_{6,5}(n)$ tend vers $\dfrac{n}{2\ln n}$.

Les nombres cadets premiers sont en quantité illimitée et cette quantité est asymptotique à l'expression

$$\frac{n}{2\ln n} \simeq \pi(n/2)$$

II.3.2 Infinitude des 'aînés premiers'

$6q+1$ peut aussi s'écrire $6(q-1)+7$; 6 et 7 sont premiers entre eux ; il y a donc une infinité de premiers de la forme $6q+1$, d'après le théorème de la progression arithmétique.

La quantité de premiers aînés inférieurs à n, que l'on baptise $\pi_{6,7}(n)$, tend également vers $\frac{n}{2\ln n}$.

Les nombres aînés premiers sont en quantité illimitée et cette quantité est asymptotique à l'expression

$$\frac{n}{2\ln n} \simeq \pi(n/2)$$

Il est rassurant que la somme des aînés et cadets premiers tende vers l'expression $\frac{n}{\ln n}$ découverte par **Hadamard** et **La Vallée Poussin**.

II.3.3 Détermination des nombres premiers

L'informatique nous procure aujourd'hui des outils puissants :

La feuille 1 du tableur Excel prem-tableau-premiers.xlsb donne les nombres premiers jusqu'à 200 000 000, à la limite des possibilités d'Excel. Ils s'obtiennent en quelques minutes à l'aide du tableur Excel et d'un algorithme dû à John Baker (Natural Maths, John@naturalmaths.com.au). Mais il faut une bonne journée pour en sortir le tableau. Ci-dessous, un tableau limité aux 1000 plus petits nombres premiers.

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863	877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053	2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213	2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357	2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531	2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999	3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181	3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511	3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643	3659	3671	3673	3677	3691	3697	3701	3709	3719	3727
3733	3739	3761	3767	3769	3779	3793	3797	3803	3821	3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989	4001	4003	4007	4013	4019	4021	4027	4049	4051	4057
4073	4079	4091	4093	4099	4111	4127	4129	4133	4139	4153	4157	4159	4177	4201	4211	4217	4219	4229	4231
4241	4243	4253	4259	4261	4271	4273	4283	4289	4297	4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
4421	4423	4441	4447	4451	4457	4463	4481	4483	4493	4507	4513	4517	4519	4523	4547	4549	4561	4567	4583
4591	4597	4603	4621	4637	4639	4643	4649	4651	4657	4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
4759	4783	4787	4789	4793	4799	4801	4813	4817	4831	4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999	5003	5009	5011	5021	5023	5039	5051	5059	5077	5081	5087
5099	5101	5107	5113	5119	5147	5153	5167	5171	5179	5189	5197	5209	5227	5231	5233	5237	5261	5273	5279
5281	5297	5303	5309	5323	5333	5347	5351	5381	5387	5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521	5527	5531	5557	5563	5569	5573	5581	5591	5623	5639
5641	5647	5651	5653	5657	5659	5669	5683	5689	5693	5701	5711	5717	5737	5741	5743	5749	5779	5783	5791
5801	5807	5813	5821	5827	5839	5843	5849	5851	5857	5861	5867	5869	5879	5881	5897	5903	5923	5927	5939
5953	5981	5987	6007	6011	6029	6037	6043	6047	6053	6067	6073	6079	6089	6091	6101	6113	6121	6131	6133
6143	6151	6163	6173	6197	6199	6203	6211	6217	6221	6229	6247	6257	6263	6269	6271	6277	6287	6299	6301
6311	6317	6323	6329	6337	6343	6353	6359	6361	6367	6373	6379	6389	6397	6421	6427	6449	6451	6469	6473
6481	6491	6521	6529	6547	6551	6553	6563	6569	6571	6577	6581	6599	6607	6619	6637	6653	6659	6661	6673
6679	6689	6691	6701	6703	6709	6719	6733	6737	6761	6763	6779	6781	6791	6793	6803	6823	6827	6829	6833
6841	6857	6863	6869	6871	6883	6899	6907	6911	6917	6947	6949	6959	6961	6967	6971	6977	6983	6991	6997
7001	7013	7019	7027	7039	7043	7057	7069	7079	7103	7109	7121	7127	7129	7151	7159	7177	7187	7193	7207
7211	7213	7219	7229	7237	7243	7247	7253	7283	7297	7307	7309	7321	7331	7333	7349	7351	7369	7393	7411
7417	7433	7451	7457	7459	7477	7481	7487	7489	7499	7507	7517	7523	7529	7537	7541	7547	7549	7559	7561
7573	7577	7583	7589	7591	7603	7607	7621	7639	7643	7649	7669	7673	7681	7687	7691	7699	7703	7717	7723
7727	7741	7753	7757	7759	7789	7793	7817	7823	7829	7841	7853	7867	7873	7877	7879	7883	7901	7907	7919

II.4 Nombres composés premiers par rapport à 2 et à 3

II.4.1 Leur écriture

Les nombres $6q+\varepsilon$, premiers par rapport à 2 et à 3, ne sont pas strictement premiers si l'on peut trouver un nombre premier $p_{i,\eta}=6i+\eta$, avec $\eta=\pm 1$, tel que

$$6q+\varepsilon=(2k+1)\,p_{i,\eta}=(2k+1)(6i+\eta)=6i(2k+1)+\eta(2k+1)$$

Il convient donc que $(2k+1)\eta-\varepsilon$ ne soit pas divisible par 6 d'où $2k+1=(6u+\varepsilon)\eta$

Les nombres composés premiers par rapport à 2 et à 3 sont de la forme : $(6i+\eta_i)(6u+\eta_u)$

(2.3)

On notera que les nombres premiers 2 et 3 ne font partie ni des aînés, ni des cadets.

II.4.2 Cribles pour l'ensemble des nombres premiers

L'ensemble des nombres premiers est un sous-ensemble de l'ensemble des nombres premiers par rapport à 2 et 3.
La puissance de cet ensemble est réduite selon un facteur 3 par rapport à celle des nombres entiers impairs. Elle reste donc égale à $\aleph_0$.
Si l'on retranche de l'ensemble des nombres premiers par rapport à 2 et 3 les sous-ensembles des nombres composés révélés par les trois tableaux ci-dessous, on obtient donc l'ensemble des nombres premiers.

Plus précisément, l'ensemble des aînés premiers se compose de l'ensemble $(6q+1)$ duquel on retranche les deux ensembles définis aux tableaux (I) et (III) pour ε,η tous deux positifs ou tous deux négatifs.
L'ensemble des cadets premiers se compose de l'ensemble $(6q-1)$ duquel on retranche l'ensemble défini au tableau (II) pour ε,η de signes contraires.

Il convient de préciser que les tableaux du type ci-dessous comportent plusieurs fois les mêmes nombres ; ces tableaux développés plus abondamment illustrent la rapidité d'élimination des nombres composés à partir des nombres premiers par rapport à 2 et 3. Ils constituent en fait un perfectionnement du crible d'**Eratosthène**.

u i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	49	91	133	175	217	259	301	343	385	427	469	511	553	595	637	679	721
2	91	169	247	325	403	481	559	637	715	793	871	949	1027	1105	1183	1261	1339
3	133	247	361	475	589	703	817	931	1045	1159	1273	1387	1501	1615	1729	1843	1957
4	175	325	475	625	775	925	1075	1225	1375	1525	1675	1825	1975	2125	2275	2425	2575
5	217	403	589	775	961	1147	1333	1519	1705	1891	2077	2263	2449	2635	2821	3007	3193
6	259	481	703	925	1147	1369	1591	1813	2035	2257	2479	2701	2923	3145	3367	3589	3811
7	301	559	817	1075	1333	1591	1849	2107	2365	2623	2881	3139	3397	3655	3913	4171	4429
8	343	637	931	1225	1519	1813	2107	2401	2695	2989	3283	3577	3871	4165	4459	4753	5047
9	385	715	1045	1375	1705	2035	2365	2695	3025	3355	3685	4015	4345	4675	5005	5335	5665
10	427	793	1159	1525	1891	2257	2623	2989	3355	3721	4087	4453	4819	5185	5551	5917	6283
11	469	871	1273	1675	2077	2479	2881	3283	3685	4087	4489	4891	5293	5695	6097	6499	6901
12	511	949	1387	1825	2263	2701	3139	3577	4015	4453	4891	5329	5767	6205	6643	7081	7519
13	553	1027	1501	1975	2449	2923	3397	3871	4345	4819	5293	5767	6241	6715	7189	7663	8137
14	595	1105	1615	2125	2635	3145	3655	4165	4675	5185	5695	6205	6715	7225	7735	8245	8755
15	637	1183	1729	2275	2821	3367	3913	4459	5005	5551	6097	6643	7189	7735	8281	8827	9373
16	679	1261	1843	2425	3007	3589	4171	4753	5335	5917	6499	7081	7663	8245	8827	9409	9991
17	721	1339	1957	2575	3193	3811	4429	5047	5665	6283	6901	7519	8137	8755	9373	9991	10609

(I) Aînés $(6i+1)(6u+1)$

u i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	35	65	95	125	155	185	215	245	275	305	335	365	395	425	455	485	515
2	77	143	209	275	341	407	473	539	605	671	737	803	869	935	1001	1067	1133
3	119	221	323	425	527	629	731	833	935	1037	1139	1241	1343	1445	1547	1649	1751
4	161	299	437	575	713	851	989	1127	1265	1403	1541	1679	1817	1955	2093	2231	2369
5	203	377	551	725	899	1073	1247	1421	1595	1769	1943	2117	2291	2465	2639	2813	2987
6	245	455	665	875	1085	1295	1505	1715	1925	2135	2345	2555	2765	2975	3185	3395	3605
7	287	533	779	1025	1271	1517	1763	2009	2255	2501	2747	2993	3239	3485	3731	3977	4223
8	329	611	893	1175	1457	1739	2021	2303	2585	2867	3149	3431	3713	3995	4277	4559	4841
9	371	689	1007	1325	1643	1961	2279	2597	2915	3233	3551	3869	4187	4505	4823	5141	5459
10	413	767	1121	1475	1829	2183	2537	2891	3245	3599	3953	4307	4661	5015	5369	5723	6077
11	455	845	1235	1625	2015	2405	2795	3185	3575	3965	4355	4745	5135	5525	5915	6305	6695
12	497	923	1349	1775	2201	2627	3053	3479	3905	4331	4757	5183	5609	6035	6461	6887	7313
13	539	1001	1463	1925	2387	2849	3311	3773	4235	4697	5159	5621	6083	6545	7007	7469	7931
14	581	1079	1577	2075	2573	3071	3569	4067	4565	5063	5561	6059	6557	7055	7553	8051	8549
15	623	1157	1691	2225	2759	3293	3827	4361	4895	5429	5963	6497	7031	7565	8099	8633	9167
16	665	1235	1805	2375	2945	3515	4085	4655	5225	5795	6365	6935	7505	8075	8645	9215	9785
17	707	1313	1919	2525	3131	3737	4343	4949	5555	6161	6767	7373	7979	8585	9191	9797	10403

(II) Cadets $(6i+1)(6u-1)$

u i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	25	55	85	115	145	175	205	235	265	295	325	355	385	415	445	475	505
2	55	121	187	253	319	385	451	517	583	649	715	781	847	913	979	1045	1111
3	85	187	289	391	493	595	697	799	901	1003	1105	1207	1309	1411	1513	1615	1717
4	115	253	391	529	667	805	943	1081	1219	1357	1495	1633	1771	1909	2047	2185	2323
5	145	319	493	667	841	1015	1189	1363	1537	1711	1885	2059	2233	2407	2581	2755	2929
6	175	385	595	805	1015	1225	1435	1645	1855	2065	2275	2485	2695	2905	3115	3325	3535
7	205	451	697	943	1189	1435	1681	1927	2173	2419	2665	2911	3157	3403	3649	3895	4141
8	235	517	799	1081	1363	1645	1927	2209	2491	2773	3055	3337	3619	3901	4183	4465	4747
9	265	583	901	1219	1537	1855	2173	2491	2809	3127	3445	3763	4081	4399	4717	5035	5353
10	295	649	1003	1357	1711	2065	2419	2773	3127	3481	3835	4189	4543	4897	5251	5605	5959
11	325	715	1105	1495	1885	2275	2665	3055	3445	3835	4225	4615	5005	5395	5785	6175	6565
12	355	781	1207	1633	2059	2485	2911	3337	3763	4189	4615	5041	5467	5893	6319	6745	7171
13	385	847	1309	1771	2233	2695	3157	3619	4081	4543	5005	5467	5929	6391	6853	7315	7777
14	415	913	1411	1909	2407	2905	3403	3901	4399	4897	5395	5893	6391	6889	7387	7885	8383
15	445	979	1513	2047	2581	3115	3649	4183	4717	5251	5785	6319	6853	7387	7921	8455	8989
16	475	1045	1615	2185	2755	3325	3895	4465	5035	5605	6175	6745	7315	7885	8455	9025	9595
17	505	1111	1717	2323	2929	3535	4141	4747	5353	5959	6565	7171	7777	8383	8989	9595	10201

(III) Aînés $(6i-1)(6u-1)$

II.5 Ordonnancement des nombres premiers

II.5.1 Critère de primalité

Lorsque les nombres premiers par rapport à 2 et à 3 ne sont pas strictement premiers, ils peuvent s'écrire d'après (2.3)

$$6q+\varepsilon=(6k+\eta)\,p_i,$$

où p_i est un nombre premier et k un nombre supérieur ou égal à 1, d'où le critère de primalité qui n'est qu'une autre présentation du crible d'**Eratosthène** :

$$p_n \neq (6k+\eta)\,p_i \quad \forall\,(p_{i<n}\,,k\neq 0) \quad \text{ou encore} \quad p_n \neq \eta\,p_i \bmod 6\,p_i \quad \forall\ p_{i<n} \tag{2.4}$$

Un nombre composé qui contient p_i en facteur, apparaît

- d'abord composé avec des nombres cadets successifs $6k-1$, ce qui s'écrit encore $-p_i \bmod 6\,p_i$ et se développe

$$5p_i, 11p_i, 17p_i, ..., (6k-1)\,p_i, ... \tag{2.5}$$

  par exemple, pour $p_i=5$: $\quad 25, 55, 85, 115, ..., -5+30k, ... \equiv -5 \bmod 30$

- puis avec des nombres aînés successifs $6k+1$, ce qui s'écrit cette fois ci $+p_i \bmod 6\,p_i$ et se développe

$$7p_i, 13p_i, 19p_i, ..., (6k+1)\,p_i, ... \tag{2.6}$$

par exemple, pour $p_i=5$: $\quad 35, 65, 95, 125, ..., 5+30k, ... \equiv 5 \bmod 30$

Ces progressions arithmétiques fournissent tous les nombres composés divisibles par le facteur premier p_i

Dans de telles suites, on rencontrera les produits successifs $6k+\eta = p_i^g\,p_j^h\,p_i^l ...$ des puissances de plusieurs nombres premiers.

II.5.2 Raréfaction des nombres premiers

On constate que la densité des nombres $6q+\eta$, lorsqu'ils sont premiers, est une fonction décroissante de q, décroissante de façon discontinue selon les apparitions successives des nombres premiers p_i, décroissante de façon atténuée par suite de l'augmentation de la valeur du module $6\,p_i$.

II.5.3 Cadence des nombres premiers

Ainsi bat l'horloge qui retire de la suite des nombres premiers par rapport à 2 et à 3, ceux qui ne sont pas strictement premiers. Les nombres premiers occupent les vides laissés par les rouages qui assemblent les nombres composés

L'expression (2.4) développée à titre d'exemple selon (2.5) et (2.6) caractérise l'ordonnancement des nombres premiers.

II.5.4 Quantités comparées des nombres premiers cadets et aînés.

D'après le critère de primalité (2.4) les nombres composés s'écrivent

$$c = (6k + \eta)\, p_i \qquad (2.7)$$

Le facteur p_i apparaîtra à nouveau dans une expression telle que

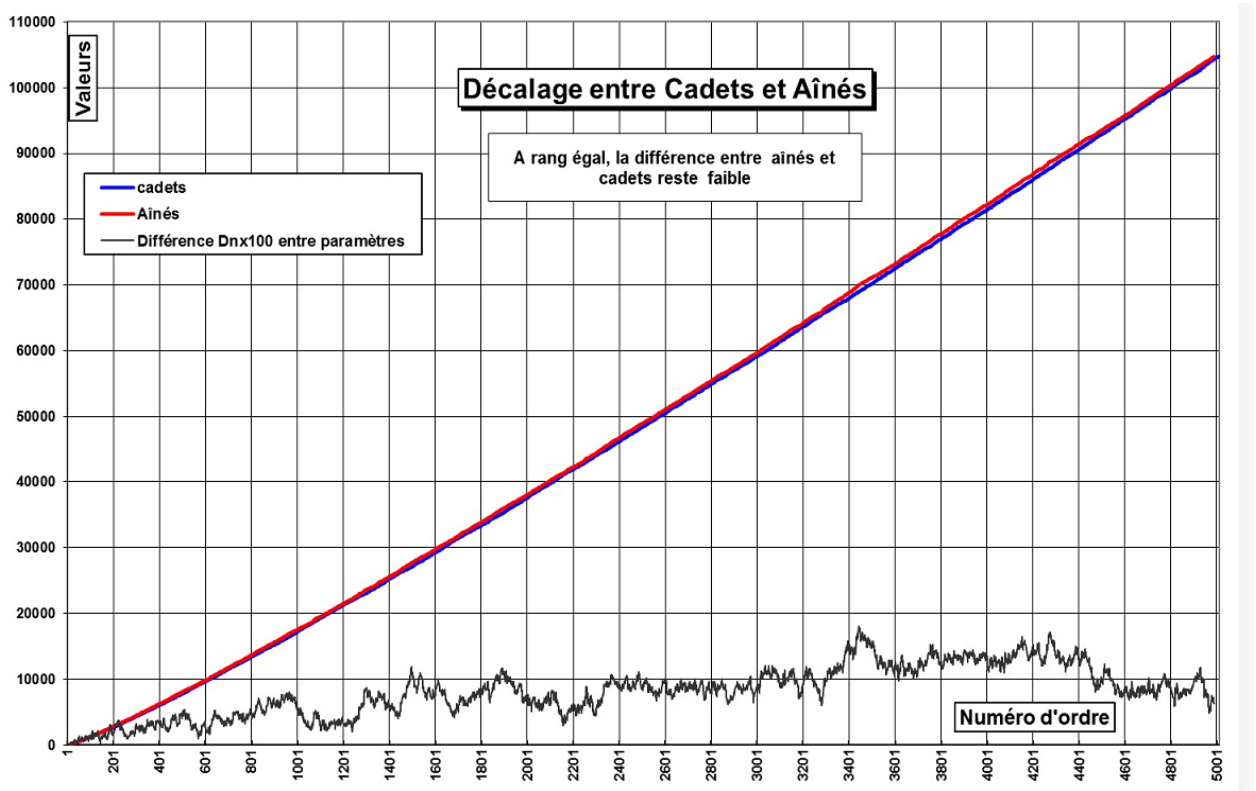
$$c = p_i\left(p_j\left(6k' + \eta'\right)\right) = p_j\left(p_i\left(6k' + \eta'\right)\right)$$

Il apparaît que chaque nombre premier p_i engendre la 'disparition' de $6k + \eta$ nombres premiers aux facteurs près p_j contenus dans chaque coefficient $6k + \eta$.
Et finalement, chaque premier permet de rayer de la liste des nombres premiers un nombre égal de cadets et d'aînés premiers par rapport à 2 et 3.

Le nombre de cadets et d'aînés premiers inférieurs à un nombre n est donc le même à un déphasage près $2p_i$ dû à la présence de ηp_i dans l'expression (2.7), laquelle s'écrit aussi $\eta p_i + 6kp_i$. Ce déphasage ne peut affecter que les nombres compris entre $p_i(6\times1-1) = 5p_i$ et $p_i(6\times1+1) = 7p_i$.

On peut donc conclure que la différence des quantités de cadets et d'aînés inférieurs à n est égale à la quantité de nombres premiers p_i tels que $5p_i < n < 7p_i$. Lorsque n est grand, cette différence devient négligeable.

Les nombres premiers aînés et cadets inférieurs à un nombre donné n sont en quantité égale à quelques unités près.



Les deux courbes indiquant la valeur des aînés ou cadets en fonction de leur rang se superposent pratiquement, ce qui est conforme à l'assertion ci-dessus.

Le cadet premier de rang $32\ 000$ a pour valeur $799\ 031$ tandis que l'aîné premier de rang $32\ 000$ a pour valeur $802\ 159$ d'où un écart absolu de $3\ 128$ et un écart relatif de $0{,}0039$.

II.6 Exploitation analytique des cribles définis en II.4.2

II.6.1 Analyse générale

Soit un nombre premier par rapport à 2 et 3 : $p_{q,\eta}$

$6q+\eta$ sera premier, si et seulement si l'on ne peut trouver aucun couple d'entiers i et j non nuls tels que

$$6q+\eta_q = (6i+\eta_i)(6j+\eta_j) \tag{2.8}$$

d'où

$$q = 6ij+\eta_i j+\eta_j i \quad \forall i,j \qquad \text{avec} \qquad \eta_i\eta_j = \eta_q \tag{2.9}$$

ou encore

$$j = \frac{q-\eta_j i}{6i+\eta_i}, \tag{2.10}$$

qui signifie que $q-\eta_j i$ n'est divisible par aucun nombre premier $6i+\eta_i$ lorsque $6q+\eta_q$ est premier.

II.6.2 Cas des nombres aînés premiers par rapport à 2 et à 3

Pour un aîné $6q+1$, η_i et η_j devront être égaux, d'où l'écriture du paramètre q des aînés composés avec $6i+\eta$

$$q = i\eta + j(6i+\eta) \quad \forall i,j \qquad 6i+\eta \text{ étant premier}$$

soit

$$q \equiv i\eta \bmod (6i+\eta) \tag{2.11}$$

Les nombres $6q+1$ sont premiers si et seulement si leur paramètre q est tel que $q-\eta i$ ne soit divisible par aucun nombre $6i+\eta$.

Il est à noter que les valeurs successives de i entraînent l'élimination de tous les paramètres $\boldsymbol{q}$ tels que

$q = i\eta + j(6+\eta)$, soit $q=-1+5j$ et $q=1+7j$ pour $i=1$

$q = i\eta + j(12+\eta)$, soit $q=-2+11j$ et $q=2+13j$ pour $i=2$

$q = i\eta + j(18+\eta)$, soit $q=-3+17j$ et $q=3+19j$ pour $i=3$

$q = i\eta + j(24+\eta)$, soit $q=-4+23j$ et $q=4+25j$ pour $i=4$

$q = i\eta + j(30+\eta)$, soit $q=-5+29j$ et $q=5+31j$ pour $i=5$

II.6.3 Cas des nombres cadets premiers par rapport à 2 et à 3

Pour un cadet $6q-1$, η_i et η_j sont opposés, d'où l'écriture du paramètre q des cadets composés :

$$q = -i\eta + j(6i+\eta) \quad \forall i,j, \quad 6i+\eta \text{ étant premier}$$

soit

$$q = -i\eta \bmod (6i+\eta) \tag{2.12}$$

Les nombres $6q-1$ sont premiers si et seulement si leur paramètre q est tel que $q+\eta i$ ne soit jamais divisible par $6i+\eta$, d'où un système d'élimination du même type que le précèdent.

II.6.4 Critère de primalité généralisé.

Du développement ci-dessus (II.6.1,2,3), il ressort que tout nombre $6q+\eta$ premier par rapport à 2 et à 3 sera strictement premier si et seulement si pour i non nul :

$$q \equiv r_{i\eta} \bmod(6i+\eta) \quad \forall(6i+\eta) < \sqrt{6q+1} \text{ avec } r_{i\eta} \neq (\pm i) \tag{2.13}$$

En effet si $r_{i\eta} = \pm i = \varepsilon i$,

$$6q+\varepsilon\eta = (6\varepsilon i + \varepsilon\eta) \bmod(6i+\eta) = \varepsilon(6i+\eta) \bmod(6i+\eta)$$

Une démonstration et une réciproque identiques s'appliquent aux paramètres q des nombres $(2q+1)$ premiers car

$$2q+\varepsilon\eta = \varepsilon(2i+\eta) + 2k(2i+\eta) = (2k+\varepsilon)(2i+\eta)$$

II.6.5 Hyperboles associées aux nombres premiers par rapport à 2 et à 3

Les équations établies en **II.6.1** décrivent dans le domaine des nombres réels les hyperboles

$$6xy = q + \frac{\eta_i\eta_j}{6} \quad \text{avec} \quad x = i + \frac{\eta_i}{6} \quad \text{et} \quad y = j + \frac{\eta_j}{6} \tag{2.14}$$

Cela signifie que pour que $6q+\varepsilon$ reste premier, l'hyperbole $xy = h$ de paramètre $h = \frac{q}{6} + \varepsilon\frac{\eta_i\eta_j}{36}$ ne doit passer par aucun point x, y tel que i, j soient tous deux entiers.

Ci-dessous, nous avons tracé les quatre hyperboles correspondant à une certaine valeur de q ; soit $q = 100$.

Les deux courbes des aînés se caractérisent par le fait que $\eta_i = \eta_j$; leur équation commune s'écrit :

$$j = \frac{q-\eta i}{6i+\eta} \text{ ou encore } 6xy = q + \frac{1}{6} \text{ (avec une origine décalée de } x, y = \eta/6) \tag{2.15}$$

Les deux courbes des cadets sont symétriques l'une par rapport à l'autre ; elles sont comprises entre les deux précédentes qu'elles rejoignent asymptotiquement, l'une en j et l'autre en i.

Elles se caractérisent par le fait que $\eta_i = -\eta_j$, et leur équation commune s'écrit :

$$j = \frac{q+\eta i}{6i+\eta} \text{ ou encore } 6xy = q - \frac{1}{6} \tag{2.16}$$

Les points situés sur la bissectrice sont caractérisés par les valeurs ci-dessous de $i = j$, extrapolées dans le domaine des nombres réels :

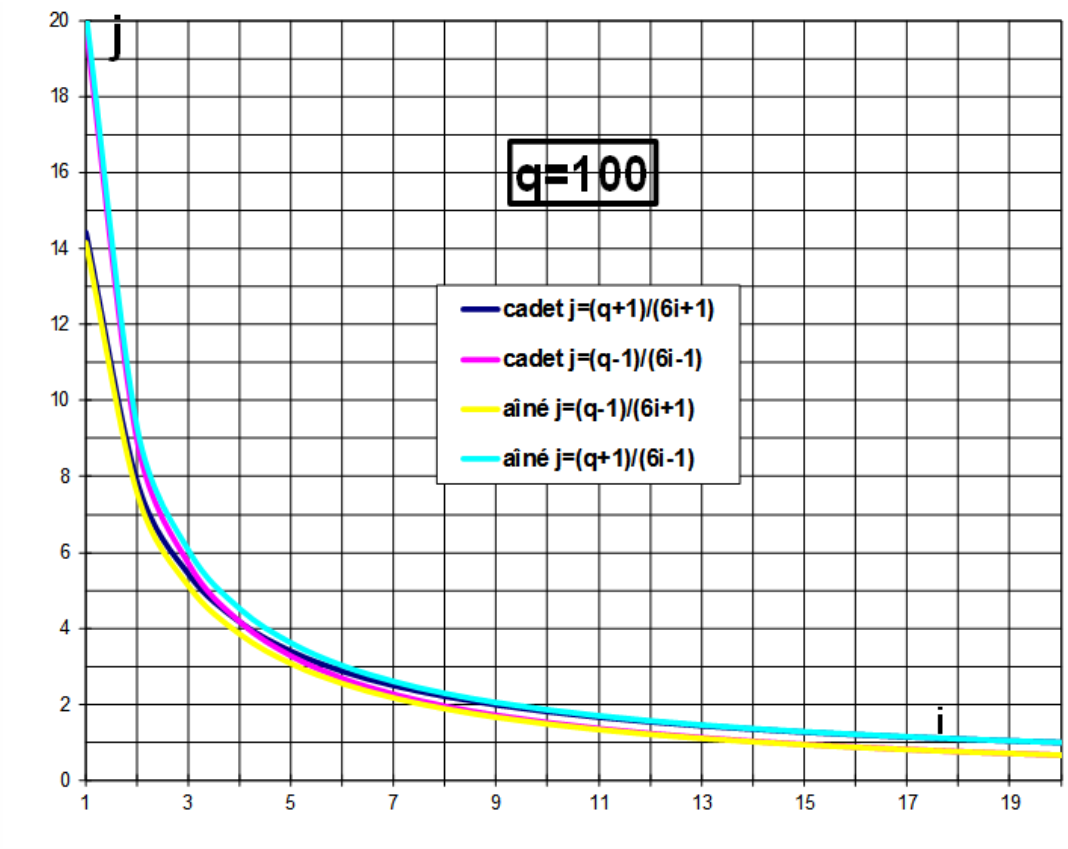
aînés : $i = j = \frac{\pm 1 + \sqrt{6q+1}}{6}$ cadets : $i = j = \sqrt{\frac{q}{6}}$

En ce qui concerne les deux hyperboles aînées, les coordonnées de ces deux points restent donc distantes d'une valeur constante et égale à $1/3$.

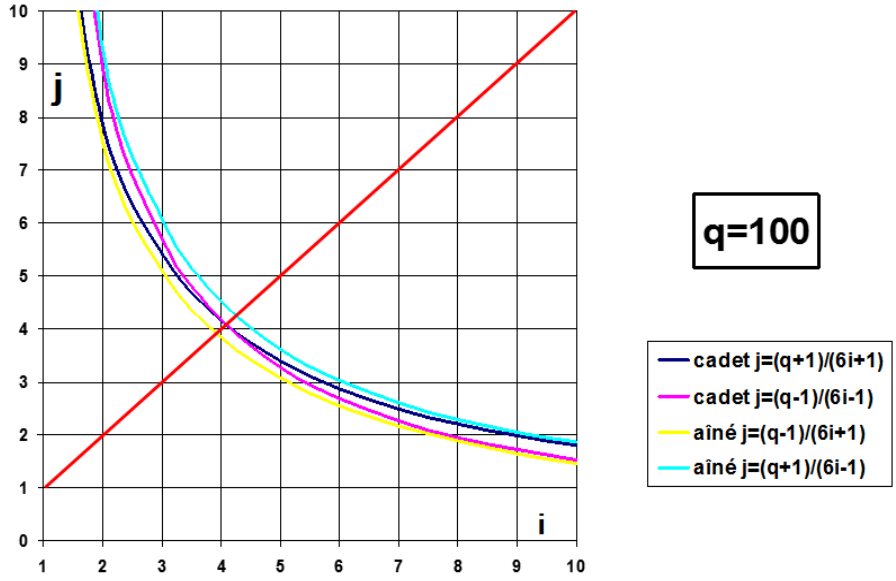
La distance entre l'origine des axes et le sommet des hyperboles cadettes est égale à $\sqrt{q/3}$; cette distance s'accroît selon un gradient égal à $\frac{1}{2\sqrt{3q}}$.

La distance entre sommets de cadets de paramètres successifs $q, q+1$ est $\sqrt{q/3}\left[\sqrt{1+1/q}-1\right]$; lorsque q devient grand, elle est équivalente à $\dfrac{1}{2\sqrt{3q}}$ et devient infinie.

Les hyperboles tracées pour $q=100$ ne passent par aucun 'point' (i, j) entier car $p=6q+\varepsilon=599$ ou 601 sont tous deux premiers.



AGRANDISSEMENT¶



II.7 Les nombres premiers jusqu'en p_k

En **II.1.6** nous avons défini les nombres en base $\prod_{i=1}^{k} p_i$ qui sont premiers jusqu'en p_k ; ils s'écrivent

$$p_x = q\prod_{i=1}^{k} p_i + r$$

Le reste impair r n'étant divisible par aucun des nombres premiers $(2,..., p_k)$ et q étant compris entre 2 et p_k inclus.

La notion de cadet, d'aîné, de jumeaux perdure.

Par exemple, si l'ensemble des premiers p_i comporte un nombre pair de cadets et si r est un aîné, alors p_x désigne un aîné. Plus généralement, cadets et aînés sont le résultat de quatre combinaisons possibles de p_i et r**.**

II.7.1 Crible suffisant pour nombres strictement premiers.

Si les nombres $p_x = q\prod_{i=1}^{k} p_i + r$ sont inférieurs à p_{k+1}^2, alors ces nombres sont strictement premiers car ils sont premiers par rapport à $2,..., p_i,..., p_k$, mais aussi par rapport à p_{k+1} ; en effet un nombre composé qui serait inférieur à p_{k+1}^2 comporterait au moins un facteur inférieur à p_{k+1} (crible d'Eratosthène) ; il ne pourrait donc pas être premier jusqu'en p_k .

Pour que les nombres p_x premiers jusqu'en p_k soient strictement premiers, il suffit donc qu'ils vérifient la relation :

$$-p_{k+1}^2 < p_x = q\prod_{i=1}^{k} p_i + r < p_{k+1}^2 \qquad (2.17)$$

Les nombres premiers jusqu'en p_k au moins et qui sont inférieurs en valeur absolue à p_{k+1}^2**,** carré du nombre premier suivant, sont strictement premiers

Exemple: $p_k = 13$,

$$2n = 9\prod_{1}^{13} p_i = 270\,270 \ ,$$

$$p_{k+1}^2 = (17)^2 = 289$$

$$p_a = 2n - r \ .$$

Sur le tableau ci-dessous extrait du fichier Excel prem-tableau2.xlsb feuille 2, les nombres r successifs compris entre $270\ 270$ -289 et $270\ 270$ +289 sont retranchés de $2n = 270270$; toutes les fois que le résultat n'est divisible par aucun des nombres $p_k = 2, 3, 5, 7, 11, 13$, ledit résultat p_a est un nombre strictement premier.

Nbr. r	Fact. r	p_a	Nbr. r	Fact. r	p_a	Nbr. r	Fact. r	p_a
269981	269981	289						
						270131	270131	139
						270133	270133	137
269987	269987	283	270059	270059	211			
269989	37 * 7297	281						
						270139	151 * 1789	131
269993	109 * 2477	277						
						270143	270143	127
269999	83 * 3253	271	270071	270071	199			
270001	270001	269	270073	270073	197			
			270077	29 * 67 * 139	193			
270007	193 * 1399	263	270079	17 * 15887	191			
						270157	270157	113
270013	71 * 3803	257				270161	19 * 59 * 241	109
						270163	270163	107
			270089	23 * 11743	181			
270019	29 * 9311	251	270091	163 * 1657	179	270167	270167	103
						270169	43 * 61 * 103	101
			270097	270097	173	270173	73 * 3701	97
270029	270029	241						
270031	270031	239	270103	31 * 8713	167			
						270181	17 * 23 * 691	89
			270107	257 * 1051	163			
270037	270037	233						
						270187	271 * 997	83
270041	31 * 31 * 281	229	270113	17 * 15889	157			
270043	23 * 59 * 199	227				270191	270191	79
270047	19 * 61 * 233	223	270119	313 * 863	151			
			270121	270121	149			

Suite			Suite		
270197	157*1721	73			
270199	19 * 14221	71			
270203	47 * 5749	67			
270209	270209	61			
270211	37 * 67 * 109	59	270287	270287	-17
			270289	31 * 8719	-19
270217	270217	53	270293	89 * 3037	-23
270223	270223	47	270299	270299	-29
			270301	137 * 1973	-31
270227	23 * 31 * 379	43			
270229	270229	41			
			270307	270307	-37
270233	181 * 1493	37			
			270311	270311	-41
			270313	19 * 41 * 347	-43
270239	270239	31			
270241	270241	29	270317	17 * 15901	-47
270247	53 * 5099	23	270323	270323	-53
270251	29 * 9319	19			
270253	131 * 2063	17	270329	270329	-59
			270331	83 * 3257	-61
			270559	41 * 6599	-289