Les nombres absolument premiers

Daniel PERRIN

1 Premiers résultats

1.1 Définition

1.1 Définition. *Soit $N = a_{n-1}\dots a_1a_0$ un entier non nul écrit dans le système décimal (les a_i sont donc des entiers compris entre 0 et 9, avec $a_{n-1} \neq 0$). On dit que N est* **absolument premier** [1] *s'il est premier et si tous les nombres obtenus en permutant ses chiffres le sont aussi.*

1.2 *Exemples.* Les nombres premiers à un chiffre $2, 3, 5, 7$ sont évidemment absolument premiers. Il est facile de faire la liste des nombres absolument premiers à deux chiffres : 11, 13, 17, 31, 37, 71, 73, 79, 97. Il y a des nombres absolument premiers à trois chiffres, comme par exemple 113. Le but de ce texte [2], est de faire le bilan ce qu'on peut dire de manière élémentaire sur ces nombres.

Pour $N > 2$, on note déjà que les seuls chiffres possibles de N sont $1, 3, 7, 9$. En effet, si N a un chiffre pair, il suffit de le mettre en chiffre des unités pour obtenir un nombre pair. Le raisonnement est identique si N admet le chiffre 5.

1.2 Les récidivistes repunits

Les **repunits** (mot forgé à partir de l'anglais *repeated units*) sont les nombres dont tous les chiffres sont égaux à 1. On a le résultat suivant :

1.3 Proposition. *Si le repunit r_n à n chiffres est premier, le nombre de chiffres n est premier.*

Démonstration. On montre que si $n = pq$, r_p divise r_n. Pour cela on utilise le lemme facile suivant, qui résulte du calcul de la somme d'une suite géométrique :

1. Ils sont aussi appelés nombres premiers permutables.

2. Très largement inspiré d'un papier de Claude Deschamps, écrit en vue des olympiades ? Voir le site `euler.ac-versailles.fr`

1.4 Lemme. *On a* $r_n = \dfrac{10^n - 1}{9}$.

Posons $s_n = 9r_n = 10^n - 1$. Modulo s_p on a $10^p \equiv 1$, donc aussi $10^n = (10^p)^q \equiv 1$. Il en résulte que s_p divise s_n, c'est-à-dire qu'on a $s_n = 9r_n = ks_p = 9kr_p$ d'où $r_n = kr_p$. Si p n'est égal ni à 1 ni à n, on a ainsi un diviseur strict de r_n, qui n'est donc pas premier.

1.5 *Remarque.* La condition précédente n'est pas suffisante : on a $111 = 3\times37$ bien que son nombre de chiffres soit premier. On n'a pas de critère pour affirmer qu'un repunit est premier. On conjecture qu'il y en a une infinité. Les plus petits r_n premiers connus correspondent à $n = 2, 19, 23, 317, 1031$. On a cependant la proposition suivante :

1.6 Proposition. *Soient n et p des nombres premiers, avec $p > 3$. On suppose que n est l'ordre $\omega(p)$ de 10 modulo p. Alors p divise r_n. Si p n'est pas un repunit, r_n n'est pas premier. Réciproquement, si p divise r_n, on a $\omega(p) = n$.*

Démonstration. On a $10^n \equiv 1 \pmod p$, donc p divise $10^n - 1 = 9r_n$. Comme p est distinct de 3, il divise r_n.

Pour la réciproque, on a $10^n \equiv 1 \pmod p$, de sorte que $\omega(p)$ divise n et comme n est premier ils sont égaux.

1.7 Corollaire. *Les repunits r_n sont non premiers pour $n = 3$, 5, 7, 11, 13, 17.*

Démonstration. Pour $n = 3$ cela a été vu. Ensuite, on a $\omega(37) = 3, \omega(41) = 5$, $\omega(239) = 7$ ou $\omega(4649) = 7$, $\omega(21649) = \omega(513239) = 11$, $\omega(53) = \omega(79) = \omega(265371653) = 13$, $\omega(2071723) = 17$.

1.8 *Remarque.* Bien entendu, cette proposition n'est pas très sérieuse. On l'utilise plutôt en sens inverse : en prenant les facteurs premiers des repunits on obtient de grands nombres premiers p tels que l'ordre de 10 modulo p (ce que nous avons appelé $\omega(p)$) est petit. Ces nombres sont remarquables car les développements décimaux des fractions a/p ont une petite période (précisément égale à $\omega(p)$). Ainsi, par exemple on a, avec $\omega(p) = 13$:

$$\frac{125874915}{265371653} = 0,4743444219454743444219454743444219454\ldots$$

1.3 Les huns à Sète ?

1.9 Proposition. *Un nombre N de plus de deux chiffres dont les chiffres sont tous égaux à 1 sauf un qui vaut 7 n'est pas absolument premier.*

Démonstration. Soit n le nombre de chiffres. On raisonne selon les congruences de n modulo 6. On rappelle que 111111 est multiple de 7 et de 13 et il en est évidemment de même des repunits à $n = 6k$ chiffres.

• Si n est multiple de 3 (donc $\equiv 0, 3 \pmod 6$), la somme des chiffres de N est multiple de 3 (car 7 est aussi congru à 1 modulo 3), donc N est multiple de 3.

• Si n est congru à 1 modulo 6, le nombre $111\ldots117$ est multiple de 7 car $111\ldots11$ l'est.

• Si n est congru à 5 modulo 6, on note que 11711 est multiple de 7, donc aussi $11\ldots11\,11711$.

• Si n est congru à 4 modulo 6, on utilise le nombre 7111 qui est multiple de 13.

• Enfin, si n est congru à 2 modulo 6 (et $n > 2$), c'est 11111711 qui est multiple de 13.

1.4 Pas de quatre

1.10 Proposition. *Si un nombre N possède les quatre chiffres $1, 3, 7, 9$, il n'est pas absolument premier.*

Démonstration. Écrivons $N = a_{n-1}\ldots a_5abcd$ avec $\{a, b, c, d\} = \{1, 3, 7, 9\}$, donc $N = M + abcd$. Modulo 7, le nombre M est congru à $0, 1, \ldots, 6$. Alors, il y a un permuté de N qui est multiple de 7. Pour le voir, il suffit de montrer que, pour tout k avec $0 \leq k \leq 6$, il y a un nombre permuté de 1379 qui est congru à k modulo 7. Or, on a $1379 \equiv 0$, $1793 \equiv 1$, $3719 \equiv 2$, $1739 \equiv 3$, $1397 \equiv 4$, $1937 \equiv 5$ et $1973 \equiv 6$.

1.5 Trois contre deux

1.11 Proposition. *Si un nombre N contient trois chiffres égaux à a et deux égaux à b, il n'est pas absolument premier.*

Démonstration. Bien entendu on peut supposer que a et b sont parmi $1, 3, 7, 9$. La méthode est la même que pour la proposition précédente : il suffit de montrer qu'on obtient toutes les congruences possibles modulo 7 avec les permutés de *aaabb*. Il y a 10 permutés : *aaabb*, *aabab*, *aabba*, *abaab*, *ababa*, *abbaa*, *baaab*, *baaba*, *babaa* et *bbaaa*. Comme les puissances de 10 modulo 7 sont égales à $-3, -1, 2, 3, 1$ quand l'exposant vaut $4, 3, 2, 1, 0$, les nombres précédents sont respectivement congrus modulo 7 à $-2a + 4b$, $-a + 3b$, $-3a + 5b$, $2a$, $2b$, $a + b$, $-3a + 5b$, $2a$, $3a - b$ et $-a + 3b$. On vérifie que les sept qui ne sont pas trivialement égaux sont tous distincts modulo 7. (Le plus simple pour cela est de retrancher $2b$ à chacun de ces nombres. Si l'on pose $x = a - b$, les

sept différences sont alors 0, x, $2x$, $3x$, $4x$, $5x$ et $6x$ et comme x est non nul modulo 7, elles sont bien distinctes.)

1.6 Laissez venir à moi les petits absolument premiers

1.12 Proposition. *Les seuls nombres absolument premiers à moins de* 7 *chiffres sont* 2, 3, 5, 7, 11, 13, 17, 31, 37, 71, 73, 79, 97, 113, 131, 199, 311, 337, 373, 733, 919 *et* 991.

Démonstration. Le mieux est d'écrire un petit programme qui fasse le tour de ces nombres.

Pour les nombres à trois chiffres, on peut montrer que ceux qui admettent trois chiffres distincts recèlent un multiple de 7. En effet, on a abc, avec a, b, c égaux à $1, 3, 7, 9$ donc à $0, 1, 2, 3$ modulo 7 et comme $1, 10, 100$ valent $1, 3, 2$ modulo 7, il suffit de noter qu'on a les congruences suivantes à 0 : $3.2 + 1.1 + 0.3$, $2.3 + 1.1 + 0.2$, $3.1 + 2.2 + 0.3$ et $3.3 + 2.2 + 1.1$. Pour les nombres admettant des répétitions il faut procéder à un examen direct. On a $111 = 3 \times 37$, 117 relève de 1.9 (multiple de 13), 119 est multiple de 7, de même que 133. Bien sûr, 339, 771 et 993 sont multiples de 3. Les plus difficiles sont 737 et 979 (multiples de 11) et surtout $779 = 19.41$.

Cela montre qu'il va y avoir des difficultés à exhiber des règles générales.

2 Un premier théorème

2.1 Le résultat

2.1 Théorème. *Tout nombre N absolument premier est soit un repunit, soit permuté d'un nombre de la forme $B_n(a, b) = aaa \dots aab$ avec $n - 1$ chiffres a et un chiffre b, $a, b \in \{1, 3, 7, 9\}$, distincts.*

Démonstration. On commence par montrer le lemme suivant :

2.2 Lemme. *Si un nombre absolument premier est de la forme :*

$$N = c_1 c_2 \dots c_{n-6} aaaaab$$

avec a, b distincts, l'entier $c_1 c_2 \dots c_{n-6}$ est multiple de 7.

Démonstration. Comme les puissances de 10 modulo 7 sont égales à $-2, -3, -1, 2, 3, 1$ quand l'exposant vaut $5, 4, 3, 2, 1, 0$ et que leur total est nul, les congruences modulo 7 des nombres obtenus par permutation à partir de $aaaaab$ sont $b - a$, $3b - 3a$, $2b - 2a$, $a - b$, $3a - 3b$, $2a - 2b$, c'est-à-dire

$b-a$ multiplié par $1, 3, 2, -1, -3, -2$. Comme $b-a$ est non nul modulo 7, ces valeurs sont distinctes et distinctes de 0. On obtient donc par permutation les six classes non nulles de restes modulo 7. Si $M = c_1c_2\dots c_{n-6}$ n'est pas multiple de 7, il y a donc une permutation des derniers chiffres dont la congruence modulo 7 est opposée à celle de M, donc qui rend N multiple de 7 et c'est absurde.

On peut alors prouver le théorème. On peut supposer que N a au moins 7 chiffres qui sont parmi $1, 3, 7, 9$ et qu'on n'a pas ces quatre chiffres à la fois. Si on a un seul chiffre on est dans le cas d'un repunit (les autres cas ne donnent évidemment pas des nombres premiers). Si on a deux chiffres et si le nombre n'est pas un $B_n(a, b)$ il y a au moins deux chiffres de chaque sorte et, comme il y a au moins cinq chiffres, cela contredit 1.11.

Si on en a trois, disons a, b, c, il ne peut y en avoir deux, disons b, c, qui soient répétés deux fois. En effet, si l'un est répété trois fois cela contredit 1.11, sinon, a est répété $n-4 \geq 3$ fois et cela contredit encore 1.11.

Le nombre contient donc deux chiffres b, c qui apparaissent une seule fois et le chiffre a présent $n-2 \geq 5$ fois. Il y a donc des permutés de N qui sont de la forme $aa\dots acaaaaab$, de sorte que les nombres $aa\dots ac$ et $aa\dots ca$ avec $n-7$ chiffres a sont tous deux multiples de 7 en vertu de 2.2. Si n est égal à 7, cela signifie qu'on a $c = 7$ et sinon, on voit que c'est impossible car les nombres $\overline{ac} = 10a + c$ et $\overline{ca} = 10c + a$ ne sont pas égaux modulo 7. Le cas $n = 7$, $c = 7$ est impossible lui aussi car le même raisonnement montre que b devrait lui aussi être égal à 7.

2.2 Une application

2.3 Proposition. *Soit p un nombre premier ≥ 7. On suppose que 10 est d'ordre $p-1$ dans $(\mathbf{Z}/p\mathbf{Z})^*$. Alors, si n est $\geq p-1$ et si $B_n(a, b) = aaa\dots aab$ est absolument premier, n est multiple de $p-1$.*

Démonstration. Comme 10 est d'ordre $p-1$ modulo p, il suffit de montrer qu'on a $10^n \equiv 1 \pmod{p}$. En particulier, on peut supposer $n \geq p$.

Soit N_i le nombre permuté de $B_n(a, b)$ obtenu en mettant b en i-ième position. On a donc : $N_i = (b-a)10^i + a(1 + 10 + \dots + 10^{n-1}) = (b-a)10^i + \dfrac{10^n - 1}{9}$. On en déduit $9N_i = 9(b-a)10^i + 10^n - 1$.

Comme 10 est d'ordre $p-1$ modulo p, les classes 10^i pour i variant de 0 à $p-1$ décrivent tout le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ et *a fortiori* les 10^i pour i de 0 à $n-1$ puisque n est $\geq p$. Comme 9 et $b-a$ sont premiers à p (car on a $p \geq 7$), il en est de même des $9(b-a)10^i$. Si $10^n - 1$ n'est pas multiple de p, il existe donc un i tel que $9(b-a)10^i$ soit égal à $-(10^n - 1)$ modulo p. Mais alors $9N_i$

est multiple de p, donc aussi N_i, et B_n n'est pas [3] absolument premier, ce qui est absurde.

2.4 *Remarque.* Les nombres premiers p auxquels on peut appliquer cette proposition sont ceux dont le développement décimal de l'inverse est de période maximale, c'est-à-dire $p-1$, et ils sont très nombreux. C'est par exemple le cas de 7, 17, 19, 23, 29, 47, 59, 61, 97, etc.

2.5 Corollaire. *Soit N un nombre absolument premier qui n'est pas un repunit et qui contient $n \geq 4$ chiffres. Alors, n est multiple de* 11088.

Démonstration. On a vu que si B_n est absolument premier n est multiple de $7-1=6$. On commence par montrer qu'il n'y a pas de nombre B_n absolument premier [4] avec 6 ou 12 chiffres et on peut donc supposer $n \geq 18$. On note qu'on a $11088 = 2^4 \times 3^2 \times 7 \times 11$. On applique la proposition précédente avec $p = 17$ (c'est possible car on a $n > 16$). On voit que n doit être multiple de 16 et donc au moins égal à 32. On peut alors appliquer encore la proposition avec 19, de sorte que n est multiple de 18, donc de 9, avec 23, on voit que n est multiple de 22, donc de 11 et avec 29 et on voit que n est multiple de 7. En définitive, il est multiple de 11088.

2.6 Corollaire. *Soit N un nombre absolument premier qui n'est pas un repunit et qui contient $n \geq 4$ chiffres. Alors, n est multiple de* 258849360 *et bien plus encore ...*

Démonstration. Maintenant qu'on sait que N a au moins 11088 chiffres on peut appliquer la proposition avec tous les nombres premiers pour lesquels 10 est un générateur. Ici, on s'est limité aux nombres premiers plus petits que 100.

2.7 Conjecture. *Il n'y a pas de nombre absolument premier $N \geq 10^3$ autre que les repunits.*

Démonstration. S'il y a une infinité de p tels que 10 engendre $(\mathbf{Z}/p\mathbf{Z})^*$ ce doit être clair. Sauf que ça c'est la conjecture d'Artin et qu'on ne sait toujours pas si c'est vrai ...

3. Car B_n est $> n$ (donc $> p$) comme on le vérifie aisément.

4. Pour $n = 6$, en dehors des cas triviaux, on a $111113 = 23 \times 4831$, $111911 = 17 \times 29 \times 227$, $333313 = 149 \times 2237$, $333373 = 389 \times 857$, $777773 = 709 \times 1097$, $777779 = 113 \times 6883$, $999991 = 17 \times 59 \times 997$ et enfin $999997 = 757 \times 1321$.