L'été, revenir à des calculs simples (Denise Vella-Chemla, 12.8.18)

1) Plusieurs fonctions en une, à la recherche d'une fonction simple qui permettrait de caractériser les nombres premiers

En calculant la somme modulaire (selon n) des entiers inférieurs à $n/2$, on réalise que le calcul modulaire transforme une fonction quadratique en plusieurs fonctions affines.

On calcule par programme dans $\mathbb{Z}/n\mathbb{Z}$ la somme des $n/2$ premiers nombres $h(n) = \sum_{x=1}^{n/2} x \ (mod\ n)$.

n	$h(n)$	n	$h(n)$	n	$h(n)$	n	$h(n)$	n	$h(n)$
$s(1)$	0	$s(21)$	13	$s(41)$	5	$s(61)$	38	$s(81)$	10
$s(2)$	1	$s(22)$	0	$s(42)$	21	$s(62)$	0	$s(82)$	41
$s(3)$	1	$s(23)$	20	$s(43)$	16	$s(63)$	55	$s(83)$	31
$s(4)$	3	$s(24)$	6	$s(44)$	33	$s(64)$	16	$s(84)$	63
$s(5)$	3	$s(25)$	3	$s(45)$	28	$s(65)$	8	$s(85)$	53
$s(6)$	0	$s(26)$	13	$s(46)$	0	$s(66)$	33	$s(86)$	0
$s(7)$	6	$s(27)$	10	$s(47)$	41	$s(67)$	25	$s(87)$	76
$s(8)$	2	$s(28)$	21	$s(48)$	12	$s(68)$	51	$s(88)$	22
$s(9)$	1	$s(29)$	18	$s(49)$	6	$s(69)$	43	$s(89)$	11
$s(10)$	5	$s(30)$	0	$s(50)$	25	$s(70)$	0	$s(90)$	45
$s(11)$	4	$s(31)$	27	$s(51)$	19	$s(71)$	62	$s(91)$	34
$s(12)$	9	$s(32)$	8	$s(52)$	39	$s(72)$	18	$s(92)$	69
$s(13)$	8	$s(33)$	4	$s(53)$	33	$s(73)$	9	$s(93)$	58
$s(14)$	0	$s(34)$	17	$s(54)$	0	$s(74)$	37	$s(94)$	0
$s(15)$	13	$s(35)$	13	$s(55)$	48	$s(75)$	28	$s(95)$	83
$s(16)$	4	$s(36)$	27	$s(56)$	14	$s(76)$	57	$s(96)$	24
$s(17)$	2	$s(37)$	23	$s(57)$	7	$s(77)$	48	$s(97)$	12
$s(18)$	9	$s(38)$	0	$s(58)$	29	$s(78)$	0	$s(98)$	49
$s(19)$	7	$s(39)$	34	$s(59)$	22	$s(79)$	69	$s(99)$	37
$s(20)$	15	$s(40)$	10	$s(60)$	45	$s(80)$	20	$s(100)$	75

On note que $h(n)$ est égal à :
- k pour les $8k$ (soit $n/8$) ;
- k pour les $8k+1$;
- $4k+1$ pour les $8k+2$ (soit $n/2$) ;
- $3k+1$ pour les $8k+3$;
- $6k+3$ pour les $8k+4$ (soit $3n/4$) ;
- $5k+3$ pour les $8k+5$;
- 0 pour les $8k+6$;
- et $7k+6$ pour les $8k+7$.

La fonction $h(n)$ qui vaut $\frac{1}{4}n^2 + \frac{1}{2}n$ quand on la calcule sur l'ensemble des nombres entiers $\mathbb{N}$ s'est transformée dans $\mathbb{Z}/n\mathbb{Z}$ en une sorte d'agrégat de 8 fonctions affines différentes. On peut effectuer un traitement similiaire avec la somme des nombres compris entre $n/2$ et n [*]. Enfin, si on calcule la somme des nombres compris entre 1 et $n-1$, la fonction résultante est :

- Id pour les $8k, 8k+2$ et $8k+4$;
- $\frac{n-1}{2}$ pour les $8k+1, 8k+3$ (en fait, $4k$ pour les $8k+1$ et $4k+1$ pour les $8k+3$) ;
- $n + \frac{n-1}{2}$ pour les $8k+5, 8k+7$ (en fait, $12k+7$ pour les $8k+5$ et $12k+10$ pour les $8k+7$) ;
- et 0 pour les $8k+6$.

Les doubles de nombres premiers sont soit de la forme $8k+6$ (doubles de nombres premiers de la forme

∗. Les $8k$ ont pour image $6k$, les $8k+1$ ont pour image $3k$, les $8k+2$ ont pour image $4k+1$, les $8k+3$ ont pour image k, les $8k+4$ ont pour image $2k+1$, les $8k+5$ ont pour image $7k+4$, les $8k+6$ ont pour image 0 et les $8k+7$ ont pour image $5k+4$.

$4k+3$) soit de la forme $8k+2$ (doubles de nombres premiers de la forme $4k+1$).

Les résultats ci-dessus ne permettent pas de différencier les nombres premiers (resp. ou les doubles de nombres premiers) des nombres impairs composés (resp. des doubles de nombres impairs composés).

Pour voir si un autre élément permettrait de caractériser les nombres premiers, on calcule par programme dans $\mathbb{Z}/n\mathbb{Z}$ pour n pair le produit des $n/2$ nombres compris entre 1 et $n/2$, $k(n) = \prod_{x=1}^{n/2} x \ (mod\ n)$.

$k(n)$ est nul pour les nombres pairs. Voyons dans le tableau ci-dessous sa valeur pour les nombres impairs.

n	$k(n)$	n	$k(n)$	n	$k(n)$	n	$k(n)$	n	$k(n)$
$k(1)$	1	$k(21)$	0	$k(41)$	9	$k(61)$	11	$k(81)$	0
$k(3)$	1	$k(23)$	1	$k(43)$	42	$k(63)$	0	$k(83)$	1
$k(5)$	2	$k(25)$	0	$k(45)$	0	$k(65)$	0	$k(85)$	0
$k(7)$	6	$k(27)$	0	$k(47)$	46	$k(67)$	66	$k(87)$	0
$k(9)$	6	$k(29)$	12	$k(49)$	0	$k(69)$	0	$k(89)$	34
$k(11)$	10	$k(31)$	1	$k(51)$	0	$k(71)$	1	$k(91)$	0
$k(13)$	5	$k(33)$	0	$k(53)$	23	$k(73)$	27	$k(93)$	0
$k(15)$	0	$k(35)$	0	$k(55)$	0	$k(75)$	0	$k(95)$	0
$k(17)$	13	$k(37)$	31	$k(57)$	0	$k(77)$	0	$k(97)$	22
$k(19)$	18	$k(39)$	0	$k(59)$	1	$k(79)$	78	$k(99)$	0

Cette "moitié de factorielle" † de n est non-nulle pour les nombres premiers (sauf les nombres 1 et 9 ‡) tandis qu'elle est nulle pour les nombres composés.

Elle est égale à 1 ou $p-1$ pour les premiers $4k+3$ et à un nombre différent de 1 ou $p-1$ pour les premiers $4k+1$.

2) Nombre de puissances pures

On a trouvé à Noël passé une caractérisation des nombres premiers et de leurs puissances qu'on résume dans le tableau ci-dessous en terme de nombre de solutions de l'équation $x^{10} \equiv 1 \ (mod\ n)$ § :

	premiers ou puissances de premiers	*composés*
dernier chiffre 1	10 *solutions*	*autre chose que* 10
dernier chiffre 3, 5, 7	2 *solutions*	*autre chose que* 2

Comme la possibilité ci-dessus ne permet pas de distinguer les nombres premiers de leurs puissances pures, on voulait avoir à l'esprit le nombre de telles puissances pures de premiers jusqu'à un nombre donné (si elles étaient très peu nombreuses par rapport au nombre de premiers, le nombre de solutions ci-dessus pourrait servir à caractériser les premiers et peut-être à les compter, avec une faible erreur ¶).

Rappelons comment calculer le nombre $PP(n)$ de puissances pures de nombres premiers inférieures à n

†. La présente note fait suite à deux notes écrites à l'été 2017 http://denise.vella.chemla.free.fr/valpadiquefacto.pdf et http://denise.vella.chemla.free.fr/facto.pdf.

‡. car il n'y a pas au moins 2 multiples de 3 inférieurs à la moitié de 9.

§. A ce moment-là, on avait d'abord découvert par programme que seuls les nombres premiers $n = p$ et leurs puissances $n = p^k$ sont tels que $x^2 \equiv 1 \ (mod\ n)$ a exactement deux racines. Pour les nombres composés, cette même équation modulaire a 2^k solutions avec k le nombre de nombres premiers différents de la factorisation de n. On avait alors également vérifié par programme (c'est un résultat qui doit être déduisible des Recherches arithmétiques) que pour les $p = 4k+3$ et leurs puissances, l'équation $x^4 \equiv 1 \ (mod\ n)$ a toujours 2 solutions ; concernant les $p = 4k+1$ et leurs puissances, la même équation modulaire a toujours 4 solutions mais c'est également le cas pour les nombres composés qui ont un nombre pair de premiers de la forme $4k+3$ dans leur factorisation ; c'est ce défaut de caractérisation des premiers qui nous a fait envisager l'équation $x^5 \equiv 1 \ (mod\ n)$, puis $x^{10} \equiv 1 \ (mod\ n)$. Se reporter à http://denise.vella.chemla.free.fr/racinesdixiemesde1.pdf

¶. tout ça est bien connu, mais j'essaie d'imaginer quels ont pu être les cheminements des pensées.

(i.e. qui ne sont pas des nombres premiers). On a :

$$\begin{aligned} PP(n) &= \#\{p^k \ / \ p^k \leq n, p \leq \sqrt{n}, 1 < k < log_p n\} \\ &= \sum_{k=2}^{log_p n} \Pi(\sqrt[k]{n}) \end{aligned}$$

Note : On note aussi $\sqrt[k]{n}$ par $n^{\frac{1}{k}}$. $\Pi(n)$ désigne le nombre de nombres premiers inférieurs ou égaux à n.

Il y a "très peu" de puissances pures parmi les nombres (voici les 10 puissances pures inférieures à 100 : 49, 25, 9, 27, 81, 4, 8, 16, 32 et 64). Ci-dessous un tableau qui fournit quelques-uns de leur nombre (en troisième colonne, on note le pourcentage d'erreurs que l'on ferait si l'on confondait les puissances pures de nombres premiers avec des nombres premiers, sous prétexte qu'elles partageraient une caractéristique avec eux par exemple, comme le nombre de solutions de l'équation modulaire $x^{10} \equiv 1$) :

n	$PP(n)$	$\%$ *d'erreur*
10^2	10	10 *pour* 100
10^3	25	2 *pour* 100
10^4	51	5 *pour* 1000
10^5	108	1 *pour* 1000
10^8	1404	1 *pour* 100000
10^{12}	80070	8 *pour* 10^8

3) Somme des exposants des factorisations

Dans ce paragraphe, il s'agit de présenter une fonction qui rappelle le logarithme. On fournit dans le tableau ci-dessous pour chaque entier n sa factorisation $f(n) = \prod p_i^{\alpha_i}$ et la somme des exposants des différentes puissances des nombres premiers contenues dans sa factorisation $s(n) = \sum \alpha_i$.

n	$f(n)$	$s(n)$	n	$f(n)$	$s(n)$	n	$f(n)$	$s(n)$	n	$f(n)$	$s(n)$	n	$f(n)$	$s(n)$
$s(1)$	1	1	$s(21)$	3.7	2	$s(41)$	41	1	$s(61)$	61	1	$s(81)$	3^4	4
$s(2)$	2	1	$s(22)$	2.11	2	$s(42)$	2.3.7	3	$s(62)$	2.31	2	$s(82)$	2.41	2
$s(3)$	3	1	$s(23)$	23	1	$s(43)$	43	1	$s(63)$	$3^2.7$	3	$s(83)$	83	1
$s(4)$	2^2	2	$s(24)$	$2^3.3$	4	$s(44)$	$2^2.11$	3	$s(64)$	2^6	6	$s(84)$	$2^2.3.7$	4
$s(5)$	5	1	$s(25)$	5^2	2	$s(45)$	$3^2.5$	3	$s(65)$	5.13	2	$s(85)$	5.17	2
$s(6)$	2.3	2	$s(26)$	2.13	2	$s(46)$	2.23	2	$s(66)$	2.3.11	3	$s(86)$	2.43	2
$s(7)$	7	1	$s(27)$	3^3	3	$s(47)$	47	1	$s(67)$	67	1	$s(87)$	3.29	2
$s(8)$	2^3	3	$s(28)$	$2^2.7$	3	$s(48)$	$2^4.3$	5	$s(68)$	$2^2.17$	3	$s(88)$	$2^3.11$	4
$s(9)$	3^2	2	$s(29)$	29	1	$s(49)$	7^2	2	$s(69)$	3.23	2	$s(89)$	89	1
$s(10)$	2.5	2	$s(30)$	2.3.5	3	$s(50)$	2.5^2	3	$s(70)$	2.5.7	3	$s(90)$	$2.3^2.5$	4
$s(11)$	11	1	$s(31)$	31	1	$s(51)$	3.17	2	$s(71)$	71	1	$s(91)$	7.13	2
$s(12)$	$2^2.3$	3	$s(32)$	2^5	5	$s(52)$	$2^2.13$	3	$s(72)$	$2^3.3^2$	5	$s(92)$	$2^2.23$	3
$s(13)$	13	1	$s(33)$	3.11	2	$s(53)$	53	1	$s(73)$	73	1	$s(93)$	3.31	2
$s(14)$	2.7	2	$s(34)$	2.17	2	$s(54)$	2.3^3	4	$s(74)$	2.37	2	$s(94)$	2.47	2
$s(15)$	3.5	2	$s(35)$	5.7	2	$s(55)$	5.11	2	$s(75)$	3.5^2	3	$s(95)$	5.19	2
$s(16)$	2^4	4	$s(36)$	$2^2.3^2$	4	$s(56)$	$2^3.7$	4	$s(76)$	$2^2.19$	3	$s(96)$	$2^5.3$	6
$s(17)$	17	1	$s(37)$	37	1	$s(57)$	3.19	2	$s(77)$	7.11	2	$s(97)$	97	1
$s(18)$	2.3^2	3	$s(38)$	2.19	2	$s(58)$	2.29	2	$s(78)$	2.3.13	3	$s(98)$	2.7^2	3
$s(19)$	19	1	$s(39)$	3.13	2	$s(59)$	59	1	$s(79)$	79	1	$s(99)$	$3^2.11$	3
$s(20)$	$2^2.5$	3	$s(40)$	$2^3.5$	4	$s(60)$	$2^2.3.5$	4	$s(80)$	$2^4.5$	5	$s(100)$	$2^2.5^2$	4

On $f(ab) = f(a) + f(b)$. Un texte qui en explique très pédagogiquement la raison, en présentant la factorisation d'un point de vue ensembliste, peut être trouvé ici :

$$http://denise.vella.chemla.free.fr/Laisant1.pdf.$$

Pour résumer, en utilisant le calcul modulaire dans les corps premiers, grâce à la cyclicité que celui-ci apporte, on sait bien tout compter mais les demi-factorielles présentées ici n'apportent rien que n'apportait déjà le théorème de Wilson.