Nombres premiers. Applications

Remarques d'ordre général : comme on le conseille souvent, il peut être judicieux de chercher des applications en théorie des groupes, sur les polynômes, en algèbre linéaire, ou encore d'ouvrir le sujet en considérant d'autres anneaux (théorie des nombres ou géométrie algébrique) mais il faut que cela reste marginal. Il ne faut pas perdre de vue que le coeur de la leçon doit être l'étude des nombres premiers ; il sera habile de proposer un questionnement sur le sujet à la manière de Ribenboim.

Table des matières

1. Définitions, familles et formules

1.1. Définition. —

Définition 1.1.1. — Un entier $p > 1$ est dit premier [1] si ses seuls diviseurs sont $\pm 1, \pm p$.

Théorème 1.1.2. — ***(Factorialité de*** $\mathbb{Z}$***)*** *Tout entier $n \geq 2$ s'écrit de manière unique sous la forme*

$$n = p_1^{n_1} \cdots p_r^{n_r},$$

où les n_i sont des entiers naturels non nuls, et où les p_i sont des nombres premiers.

Nous noterons alors $\mathcal{P}$ l'ensemble des nombres premiers ; la question naturelle est alors de savoir si $\mathcal{P}$ est fini ou pas.

Théorème 1.1.3. — ***(Euclide)*** *L'ensemble $\mathcal{P}$ des nombres premiers est infini.*

1. Pour ceux qui préfèrent une définition plus imagée, selon Paul Erdös, « un nombre premier est un nombre qui ne se casse pas quand on le laisse tomber par terre »

Preuve : Il existe de nombreuses preuves de ce résultat ; nous proposons ici celle de Thue qui utilise le résultat précédent. On raisonne par l'absurde et notons k le cardinal de $\mathcal{P} = \{p_1, \cdots, p_k\}$; on choisit alors n suffisamment grand tel que $(n+1)^k < 2^n$. D'après le théorème précédent tout entier $1 \leq m \leq 2^n$ s'écrit de manière unique sous la forme $\prod_{i=1}^k p_i^{e_i}$ avec $0 \leq e_i \leq n$ de sorte que $2^n \leq (n+1)^r < 2^n$ d'où la contradiction. □

Remarque : la preuve d'Euclide procède comme suit : par l'absurde supposons que $p_1, \cdots, p_r = n$ sont les seuls nombres premiers ; soit alors $N = n! + 1$, (ou bien $N = (\prod_{p \leq n} p) + 1$). Comme $N > n$ alors N n'est pas premier et possède donc un diviseur premier p qui est donc $\leq n$ de sorte que $p | n!$ et donc aussi $N - n! = 1$ d'où la contradiction. Dans la même veine, Kummer propose de raisonner comme suit : on a $N := p_1 \cdots p_r > 2$ et $N - 1 > 1$ est alors divisible par un premier p_i lequel divise $N - (N-1) = 1$ ce qui est absurde.

Remarque : on peut se demander s'il l'ensemble des premiers de la forme $n! \pm 1$ ou $(\prod_{\mathcal{P} \ni q \leq p} q) \pm 1$ est infini : à ce jour le résultat n'est pas connu.

1.2. Familles. — Nous avons vu que l'ensemble $\mathcal{P}$ des nombres premiers est infini mais il n'est pas si simple d'en exhiber, d'où ce paragraphe.

1.2.1 — Nombres de Fermat : comme -1 est racine du polynôme $X^{2n+1} + 1$ celui-ci est divisible par $X + 1$ (le quotient étant égal à $X^{2n} - X^{2n-1} + \cdots + 1)$). Soit alors $m = 2^n k$ avec k impair ; si $k > 1$, l'égalité

$$2^m + 1 = (2^{2^n})^k + 1 = (2^{2^n} + 1)((2^{2^n})^{k-1} - \cdots + 1)$$

montre que $2^{2^n} + 1$ est un diviseur propre de sorte que $2^m + 1$ n'est pas premier. Ainsi si l'on veut trouver des nombres premiers parmi la famille des $2^m + 1$, il faut prendre m de la forme 2^n. On pose alors pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$; F_n est le n-ème nombre de Fermat. On calcule $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ et l'on vérifie aisément qu'ils sont tous premiers.

Soit p premier divisant F_5, on a alors $2^{2^5} \equiv -1 \mod p$ de sorte que $\bar{2} \in \mathbb{Z}/p\mathbb{Z}$ est d'ordre 2^6 dans $(\mathbb{Z}/p\mathbb{Z})^\times$. D'après le petit théorème de Fermat, on a $2^{p-1} = 1$ et donc 2^6 divise $p - 1$, de sorte qu'un diviseur premier de F_5 est forcément de la forme $64k+1$. Vérifions que le cas $k = 10$ est un bon candidat : déjà 641 est premier et on l'écrit sous la forme $641 = 1 + 5.2^7 = 5^4 + 2^4$. Dans le corps $\mathbb{Z}/641\mathbb{Z}$, on a $0 = 641 = 1 + 5.2^7$ soit $2^7 = -1/5$. Ainsi $F_5 = 2^3 2 + 1 = (2^7)^4 . 2^4 + 1$ car $32 = 7.4 + 4$. D'où dans $\mathbb{Z}/641\mathbb{Z}$, on a $F_5 = (-1/5)^4 . 2^4 + 1 = (2^4 + 5^4)/5^4 = 0$.

Remarque : à ce jour, malgré l'aide de l'ordinateur, on ne connaît pas d'entiers $n \geq 5$ tels que F_n est premier. Remarquons cependant que pour $n = m + r$ avec $r > 0$, F_n et F_m sont premiers entre eux ; en effet on a $2^{2^n} = (2^{2^m})^{2^r}$ et dans $\mathbb{Z}/F_m\mathbb{Z}$, on a alors $F_n \equiv (-1)^{2^r} + 1 \mod F_m$. Ainsi le pgcd de F_m et de F_n divise 2 ; or 2 ne divise pas F_n d'où le résultat. L'ensemble $\mathcal{P}$ des nombres premiers positifs contient la réunion disjointe $\coprod_n \mathcal{F}_n$ où $\mathcal{F}_n$ est le sous-ensemble de $\mathcal{P}$ des diviseurs premiers divisant F_n ; $\mathcal{F}_n$ étant non vide pour tout n car $F_n > 1$, on en déduit alors une nouvelle preuve de l'infinité de $\mathcal{P}$.

Remarque : les nombres de Fermat ont un intérêt pour les polygones réguliers constructibles à la règle et au compas. Le polygone régulier à n côté est constructible si et seulement si n est de la forme $n = 2^\alpha p_1 \cdots p_r$ où les p_i sont des nombres premiers de Fermat. Les constructions par pliage (origami) permettent eux de construire les polygones réguliers à n côtés avec $n = 2^a 3^b p_1 \cdots p_r$ où les p_i sont des nombres premiers de la forme $2^u 3^v + 1$.

1.2.2 — Nombres de Mersenne : de la factorisation $X^{pq} - 1 = (X^p - 1)(X^{p(q-1)} + \cdots + X^p + 1)$, on en déduit que si $2^n - 1$ est premier alors n est un nombre premier. Ainsi pour p premier les

nombres $M_p = 2^p - 1$ sont dits de Mersenne $M_p = 2^p - 1$; les premiers exemples sont $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$, $127 = 2^7 - 1$ qui sont premiers alors que $2047 = 2^{11} - 1 = 23 \times 89$ ne l'est pas. Comme précédemment si q est un diviseur de M_p alors l'ordre de la classe de 2 dans $\mathbb{Z}/q\mathbb{Z}$ est égale à p qui doit diviser $q - 1$ et donc $q \equiv 1 \mod p$ (on a aussi $q \equiv 1 \mod 2p$). On en déduit aussi que 2 est un carré modulo q et donc $q \equiv \pm 1 \mod 8$.
Remarque : à ce jour on connaît 45 nombres de Mersenne qui sont premiers ; le dernier trouvé cet été possède plus de 10 millions de chiffres.

1.2.3 — Premiers en lien avec le grand théorème de Fermat : dans la recherche d'une preuve du fait que pour tout $n > 2$, l'équation $x^n + y^n = z^n$ n'a pas de solutions entières, certains types de nombres premiers sont apparus.

- *premiers ordinaires* : ce sont ceux tels que l'anneau des entiers $\mathbb{Z}[\zeta_p]$ de l'extension cyclotomique $\mathbb{Q}[\zeta_p]$ pour $\zeta_p = e^{2i\pi/p}$ est principale (ou de manière équivalente pour les corps de nombres, factorielle). Ce sont exactement les $p \leq 19$ pas de quoi leur donner un nom. *Remarque :* plus généralement Montgomery en 1976 a prouvé que $\mathbb{Z}[\zeta_n]$ est principal si et seulement si $n = 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84$.
- *premiers réguliers* : p est dit régulier s'il ne divise pas le nombre des classes d'idéaux de $\mathbb{Z}[e^{2i\pi/p}]$. Dans cette situation Kummer a réussi à raisonner « comme si », cet anneau était principal et a alors prouvé le théorème de Fermat. Pour l'instant on ne sait pas s'il existe une infinité de tels nombres premiers : ceux ≤ 163 sont $37, 59, 67, 101, 103, 131, 149, 157$. Par contre Jensen a prouvé en 1905 qu'il y avait une infinité de nombres premiers irréguliers ;
- *les premiers de Sophie Germain* : ce sont les p tels que $2p + 1$ est premier. Pour ceux-ci Sophie Germain a prouvé le premier cas du théorème de Fermat, i.e. quand x, y, z ne sont pas divisibles par p. On ne sait toujours pas s'il y a ou non une infinité de tels nombres.
- *les premiers de Wieferich* : ce sont les p tels que $2^{p-1} \equiv 1 \mod p^2$. Dans ce cas il a réussi à montrer que si le premier cas du théorème de Fermat était faux pour p alors p vérifiait cette congruence. Lehmer a montré si $p < 6.10^9$ était de Wieferich alors $p = 1093$ ou 3511. En 1910 *Mirimanoff* a prouvé que si le premier cas du théorème de Fermat était faux pour p alors $3^{p-1} \equiv 1 \mod p^2$. Le résultat a été ensuite étendu en remplaçant 2 et 3 par tous les $p \leq 89$ ce qui prouve le premier cas du théorème de Fermat pour tous les $p \leq 714591416091389$: enfin tout cela est désormais inutile puisque le théorème de Fermat a été prouvé en toute généralité.

1.2.4 — D'autres familles : d'après le théorème de Wilson $W(p) := \frac{(p-1)!+1}{p}$ est un entier ; pour $p = 5, 13$, $W(p)$ est premier, on peut se demander si l'ensemble des $W(p)$ premiers est infini ou pas : la réponse n'est pas connue. Nous avons vu que les facteurs premiers des nombres de Fermat était de la forme $k2^n + 1$: d'après le théorème de Dirichlet, on sait qu'il existe une infinité de k pour lesquels $k2^n + 1$ est premier. Erdös et Odlyzko ont alors montré qu'il existe une constante C telle que si $N(x)$ désigne le nombre de $1 \leq k \leq x$ tels qu'il existe n avec $k2^n + 1$ premier, alors $N(x) \geq Cx$.

1.3. Quelques formules. — Notons tout d'abord qu'il ne peut pas exister de polynômes de $\mathbb{Z}[X]$ non constant ne prenant sur $\mathbb{N}$ que des valeurs premières : en effet soit $P(X) = a_n X^n + \cdots + a_0$ de sorte qu'en particulier $a_0 \in \mathcal{P}$. Comme $P(n)$ tends vers l'infini quand n tends vers l'infini, il existe une valeur n_0 à partir de laquelle $|P(n)| > a_0$. Ainsi pour k assez grand, on a $|P(ka_0)| > a_0$ alors que $P(ka_0)$ est divisible par a_0.

Remarque : pour des polynômes du second degré donnant pour les premières valeurs de n des nombres premiers, citons les résultats suivant :

- spirales d'Ulam : il s'agit des premiers p pour lesquels n^2+n+p est premier pour $n=0,\cdots,n-2$: on remarquera en effet que p divise $(p-1)^2+(p-1)+p$, cf. aussi l'exercice 6.1. Heegner a montré que les seuls p qui conviennent sont $2,3,5,16$ et 41. On conjecture que pour tout A, il existe B tel que n^2+n+B soit premier pour tout $n=0,\cdots,A$. Pour $A=41$, B est nécessairement plus grand que 10^{18} et n'est pas connu.
- R. Ruby : $103n^2-3945n+32381$ est premier pour $n=0,1,\cdots,42$;
- G. Fung : $47n^2-1701n+10181$ est premier pour $n=0,1,\cdots,42$;
- R. Ruby : $36n^2-810n+2753$ est premier pour $n=0,1,\cdots,44$.

Définition 1.3.1. — Un ensemble S est dit diophantien s'il existe un polynôme P dans $\mathbb{Z}[X_1,\cdots,X_n,Y_1,\cdots,Y_m]$ tel que $(x_1,\cdots,x_n)\in S$ si et seulement si il existe des entiers positifs $y_1,\cdots,y_m$ tels que

$$P(x_1,\cdots,x_n,y_1,\cdots,y_m)=0$$

.

Remarque : pour $n=1$, il est aisé de voir qu'un ensemble S d'entiers positifs est diophantien si et seulement s'il existe un polynôme $Q\in\mathbb{Z}[X_1,\cdots,X_m]$ tel que

$$S=\{Q(x_1,\cdots,x_m)\geq 1:\ x_1\geq 1\cdots x_m\geq 1\}$$

En effet pour $P=Q(X_1,\cdots,X_m)-X\in\mathbb{Z}[X,X_1,\cdots,X_m]$ on voit bien qu'un tel S est diophantien et réciproquement prendre $Q=X(1-P^2)$.

Théorème 1.3.2. — *L'ensemble des nombres premiers est diophantien.*

Remarque : des polynômes explicites ont étés construits, par exemple on trouvera p.148 de [**?**] un exemple en 26 variables de degré total 25. On ne connaît pour l'instant pas le nombre minimal de variables nécessaires (on sait qu'il est compris entre 3 et 10) ni le degré minimal (on sait qu'il est ≤ 5). Expérimentalement on note que lorsque le nombre de variables (resp. le degré) diminue le degré (resp. le nombre de variables) augmente.

En utilisant le théorème de Wilson, lequel affirme que p est premier si et seulement si $(p-1)!\equiv -1 \mod p$, on montre facilement que la fonction

$$f(n)=2+2(n!) \mod n+1$$

produit tous les nombres premiers exclusivement mais plusieurs fois. En 1947 W. Mills établit l'existence d'une constante A telle que pour tout $n>1$,

$$\lfloor A^{3n}\rfloor\in\mathcal{P},\qquad A\simeq 1,306377883863...$$

cependant le calcul de cette constante nécessite la connaissance de $\mathcal{P}$ ce qui convenons le n'est pas très honnête. L'escroquerie est du même genre que la suivante : posons

$$L=0,2,003000050000007000000011...$$

le n-ème nombre premier étant placé en position n^2. On vérifie alors aisément que

$$\lfloor L\times 10^{n^2}\rfloor-\lfloor L\times 10^{(n-1)^2}\rfloor 10^{2n-1}$$

est égal au n-ème nombre premier p_n.

On s'interdit désormais d'utiliser des nombres pouvant cacher une infinité d'informations. Le premier exemple du à Roland Yéléhada repose sur la formule suivante

$$t(n) = 2 + n\lfloor \frac{1}{1 + \sum_{p=2}^{m+1} \lfloor \frac{n+2}{p} - \lfloor \frac{n+1}{p} \rfloor \rfloor} \rfloor$$

laquelle tous les nombre premiers. Le principe est très élémentaire : si $n+2$ est un multiple de p alors $(n+2)/p$ est un entier q et donc $(n+1)/p = q - 1/p$ et donc $\lfloor \frac{n+2}{p} - \lfloor \frac{n+1}{p} \rfloor \rfloor$ est égal à 1 alors qu'il est nul si p n'est pas un diviseur. Autrement dit la somme compte le nombre de diviseurs de $n+2$ compris entre 2 et $n+1$; ainsi si $n+2$ est premier on obtient $t(n) = n+2$ qui est premier alors que si $n+2$ n'est pas premier on a $t(n) = 2$. Ainsi la formule ne donne que des nombres premiers mais très lentement, 2 apparaissant très souvent. En utilisant la formule de Wilson, Minac simplifie la formule précédente :

$$t(n) = 2 + n\lfloor \frac{(n+1)! + 1}{n+2} - \rfloor \frac{(n+1)!}{n+2} \rfloor \rfloor$$

laquelle contient moins de symbole et plus de somme, mais requiert de lourds calculs de factoriels.

En 1995 Minac et Willans ont imaginé une formule, avec plus de 52 symboles, donnant tous les nombres premiers dans l'ordre et sans répétition :

$$\pi(m) = \sum_{j=2}^{m} \frac{\sin^2\left(\frac{\pi}{j}(j-1)!^2\right)}{\sin^2(\frac{\pi}{j})} = \sum_{j=2}^{m} \lfloor \frac{(j-1)! + 1}{j} - \lfloor \frac{(j-1)!}{j} \rfloor \rfloor$$

Preuve : Notons tout d'abord que pour $n \neq 4$ non premier, n divise $(n-1)!$: en effet si n peut s'écrire sous la forme ab avec $2 \leq a \neq b \leq n-1$, alors $ab|(n-1)!$. Sinon $n = p^2$ pour $p > 2$ premier avec donc $2p \leq p^2 - 1 = n - 1$ de sorte que n divise $2p.p$ lequel divise $(p^2-1)!$. Si j est premier alors $(j-1)! + 1 = kj$ d'après le théorème de Wilson et on a

$$\lfloor \frac{(j-1)! + 1}{j} - \lfloor \frac{(j-1)!}{j} \rfloor \rfloor = \lfloor k - \lfloor k - \frac{1}{j} \rfloor \rfloor = 1$$

alors que si j n'est pas premier, on a $(j-1)! = kj$ et

$$\lfloor \frac{(j-1)! + 1}{j} - \lfloor \frac{(j-1)!}{j} \rfloor \rfloor = \lfloor k + \frac{1}{j} - k \rfloor = 0.$$

Finalement pour $j = 4$, on a $\lfloor \frac{3!+1}{4} - \lfloor \frac{3!}{4} \rfloor \rfloor = 0$. □

En utilisant $\pi(n)$, Willans a montré que le n-ème nombre premier p_n est donné par la formule

$$p_n = 1 + \sum_{m=1}^{2^n} \lfloor \lfloor \frac{n}{1 + \pi(m)} \rfloor^{1/n} \rfloor.$$

En 2000, Ruiz a donné la formule suivante :

$$p_n = 1 + \sum_{k=1}^{2(\lfloor n \ln n \rfloor + 1)} \left(1 - \lfloor \frac{\psi(k)}{n} \rfloor\right)$$

où $\psi(k) = k - 1 + \sum_{j=2}^{k} \lfloor \frac{2}{j}\left(1 + \sum_{s=1}^{\lfloor \sqrt{j} \rfloor} \left(\lfloor \frac{j-1}{s} \rfloor - \lfloor \frac{j}{s} \rfloor\right)\right) \rfloor$.

Remarque : signalons aussi la suite de Perrin définie par

$$u_0 = 3,\ u_1 = 0,\ u_2 = 2 \qquad u_{n+1} = u_{n-1} + u_{n-2}.$$

Lucas a montré que pour p premier p divise u_p et on conjecture que la réciproque est vraie.

2. Aspects algorithmiques

2.1. Test de primalité. — La technique enseignée au lycée est le crible d'Eratosthène qui bien qu'efficace pour des nombres inférieurs à 10^{11} s'avère ensuite trop lente.

2.1.1 — Critère de Lehmer : il s'agit d'un test effectif dans le cas où la factorisation de $n-1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est connue. En effet n est premier si et seulement si pour tout $i = 1, \cdots, k$, il existe $a_i \in \mathbb{Z}$ tel que

$$a_i^{n-1} \equiv 1 \mod n \text{ et } a_i^{\frac{n-1}{p_i}} \wedge n = 1.$$

Preuve : Si n est premier et si g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ alors il suffit de poser $a_i = g$ pour tout $i = 1, \cdots, k$. Réciproquement soit p un diviseur premier de n alors pour tout $i = 1, \cdots, k$, comme $a_i^{(n-1)/p_i} \not\equiv 1 \mod p$, on en déduit que $p_i^{\alpha_i}$ divise $p-1$ et donc finalement $p - 1 \geq n - 1$ soit $n = p$. □

En particulier pour les nombres premiers de Fermat, on obtient le *critère de Pépin* : $p = F_n$ est premier si et seulement si $3^{(p-1)/2} \equiv -1 \mod p$.

2.1.2 — Critère de Lucas-Lehmer : il s'agit d'un test effectif dans le cas où la factorisation de $n + 1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est connue. Ce test utilise les suite (u_n) dites de Lucas définies par récurrence :

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Su_n - Pu_{n-1}, \ n \geq 2$$

où S et P sont des nombres entiers. Pour p un nombre premier ne divisant par DP, où $D = S^2 - 4P$ est le discriminant de $Q(X) = X^2 - SX + P$, on considère la suite $u_n \mod p$. On note r_1 et r_2 les racines Q dans $\overline{\mathbb{F}}_p$ de sorte que $u_n \equiv \frac{r_1^n - r_2^n}{r_1 - r_2} \mod p$. Si $(\frac{D}{p}) = 1$ (resp. $(\frac{D}{p}) = -1$) alors $r_1, r_2 \in \mathbb{F}_p$ et donc $r_1^{p-1} = r_2^{p-1} = 1$ (resp. $r_1^p = r_2$) et donc $u_{p-1} \equiv 0 \mod p$ (resp. $u_{p+1} \equiv 0 \mod p$. Par ailleurs si e est le plus petit entier tel que $u_e \equiv 0 \mod p$, alors $u_n \equiv 0 \mod p$ si et seulement si e divise n. En raisonnant comme précédemment, on en déduit le test de primalité suivant.

Théorème 2.1.3. — *Si on peut trouver une suite de Lucas (u_n) telle que $n \wedge DP = 1$ et telle que $u_{\frac{n+1}{p}} \wedge n = 1$ pour tout premier p divisant $n+1$ et $u_{n+1} \equiv 0 \mod n$ alors n est un nombre premier.*

Application aux nombres de Mersenne : soit v_n définie par récurrence par$v_0 = 2$, $v_1 = S$ et $v_{n+1} = Sv_n - Pv_{n-1}$ alors $u_{2n} = u_n v_n$. Si n est un nombre de Mersenne, on a donc $u_{n+1} = u_{(n+1)/2} v_{(n+1)/2}$ et on peut remplacer les deux conditions du théorème précédent par la seule condition $v_{(n+1)/2} \equiv 0 \mod n$. Pour calculer $v_{(n+1)/2}$ on peut remarquer que $v_{2n} = v_n^2 - 2P^n$. On pose alors $V_n = v_{2^n}$ et on obtient la récurrence $V_n = V_{n-1}^2 - 2P^{2^{n-1}}$. Il est donc intéressant de s'arranger pour que $P = \pm 1$, i.e. pour que le produit des racines de Q dans $\mathbb{C}$ soit égal à ± 1. Finalement on obtient le critère suivant dit *de Lucas-Lehmer* : soit $(L_i)_{i \geq 0}$ la suite de Lucas-Lehmer définie par $L_0 = 4$ et $L_{i+1} = L_i^2 - 2 \mod M_q$, alors M_q est premier si et seulement si $L_{q-2} \equiv 0 \mod M_q$.

2.1.4 — Fermat-Euler and co : un entier $n \in \mathbb{N}^*$ est dit pseudo-premier de base b si $b^{n-1} \equiv 1 \mod n$. Par exemple $n = 105 = 3.5.7$ est pseudo-premier de base 13 : en effet on a $13^{104} = (13^2)^{52} \equiv 1 \mod 3$, $13^{104} = (13^4)^{26} \equiv 1 \mod 5$ et $13^{104} = (13^6)^{17} \times 13^2 \equiv 1 \mod 7$, de sorte que d'après le lemme chinois on a $13^{104} \equiv 1 \mod 105$. En revanche on a $2^{104} = (2^6)^{17} \times 2^2 \equiv 4$

mod 7 de sorte que 105 n'est pas pseudo-premier de base 2. Le petit théorème de Fermat dit qu'un nombre premier p est pseudo-premier de base b pour tout b premier à p.

Ce test serait « bon » dans le sens où calculer a^{N-1} requiert, en utilisant l'exponentiation rapide, $O(\log N)$ multiplications ; cependant il est « mauvais » à cause des nombres de Carmichael qui vérifient le test sans être premier : le plus petit de ces nombres est $561 = 3.11.17$ et on sait que l'ensemble de ces nombres est infini. Une amélioration de ce test est donné par le test de *Solovay-Strassen* qui consiste à vérifier les congruences $a^{\frac{N-1}{2}} \equiv (\frac{a}{N}) \mod N$ dont la véracité est assurée par la proposition suivante.

Proposition 2.1.5. — *Soit* $H = \{a \in (\mathbb{Z}/N\mathbb{Z})^\times : a^{\frac{N-1}{2}} \equiv (\frac{a}{N}) \mod N\}$ *; alors* $H = (\mathbb{Z}/N\mathbb{Z})^\times$ *si et seulement si* N *est premier.*

Preuve : On a déjà vu que si N est premier alors $H = (\mathbb{Z}/N\mathbb{Z})^\times$. Réciproquement si p^2 divise N, il existe alors un élément $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ d'ordre $p(p-1)$ et comme p ne divise pas $N-1$, $a^{N-1} \not\equiv 1 \mod N$. Si $N = pp_2 \cdots p_r$ sans facteurs carrés ; par le lemme chinois soit $a \equiv 1 \mod p_2 \cdots p_r$ et a non carré modulo p de sorte que $(\frac{a}{N}) = -1$ mais $a^{(N-1)/2} \equiv 1 \mod p_2 \cdots p_r$ et donc $a^{(N-1)/2} \not\equiv 1 \mod N$. □

Applications :

- *Test probabiliste* : si N est composé alors comme $[(\mathbb{Z}/N\mathbb{Z})^\times : H] \geq 2$, en prenant a aléatoirement on a au moins une chance sur deux d'avoir $a \notin H$ de sorte que si N passe successsivement k tests, on peut dire qu'il est premier avec une probabilité $\geq 1 - 2^{-k}$.
- *Test déterministe sous GRH* : l'hypothèse de Riemann généralisée implique que si N est composé, il existe $a \leq 2(\log N)^2$ qui ne passera pas le test de Solovay-Strassen
- *Test probabiliste de Rabin-Miller* : un entier $n = 1+2^k q$ impair, q impair, est dit fortement pseudo-premier de base b si l'une des conditions suivantes est vérifiée :

$$b^q \equiv 1 \mod n \qquad \exists 0 \leq j < k,\ b^{2^j q} \equiv -1 \mod n$$

Si n est premier alors il est fortement pseudo-premier de base b pour tout $1 \leq b < n$: en effet $b^{2^k q} \equiv 1 \mod n$ et soit donc $0 \leq i \leq k$ le plus petit entier tel que $b^{2^i q} \equiv 1 \mod n$. Si $i = 0$, on a $b^q \equiv 1 \mod n$ et si $i > 0$ alors $b^{2^{i-1} q} \equiv -1 \mod n$ car dans un corps $x^2 = 1$ entraine $x = \pm 1$.

Remarque : si n est fortement pseudo-premier de base b alors il est pseudo-premier de base b : en effet il existe $0 \leq i \leq k$ tel que $b^{2^i q} \equiv 1 \mod n$; or $2^i q$ divise $n-1$ de sorte que $b^{n-1} \equiv 1 \mod n$.

Exemple : $n = 561$ est pseudo-premier de base 13 mais il n'est pas fortement pseudo-premier de base 2 : en effet $n-1 = 2^4 35$ et $2^{352^3} \equiv 1 \mod 561$ mais $2^{352^2} \equiv 67 \mod 561$.

Théorème 2.1.6. — *(Rabin) Pour* n *impair soit*

$$B_n = \{x \in (\mathbb{Z}/n\mathbb{Z})^\times \ / \ n \text{ est fortement pseudo-premier de base } x\}.$$

Alors si n *est non premier alors* $\frac{|B_n|}{\phi(n)} \leq 1/4$ *sauf pour* $n = 9$.

Remarque : autrement dit si $|B_n| \geq \phi(n)/4$ alors n est premier. Ainsi si n est fortement pseudo-premier dans m bases tirées au hasard, on peut présumer, avec une probabilité d'erreur inférieure à $1/4^m$, qu'il est premier. Par exemple pour $n = 561$, on obtient $|B_{561}| = 10$ de sorte qu'outre ± 1, il ne reste plus que 8 entiers qui font croire que 561 est premier et le rapport $\frac{|B_{561}|}{\varphi(561)} = 1/32$ est relativement faible. Ce critère est particulièrement adapté à la méthode RSA.

En juillet 2002, Agrawal-Kayal-Saxena ont donné un test de primalité en temps polynomial. Cependant pour les applications pratiques telles que RSA, le test probabiliste de Rabin-Miller est suffisant.
Remarque : d'après le petit théorème de Fermat pour n premier on a la congruence

$$\sum_{i=1}^{n-1} i^{n-1} \equiv -1 \mod n.$$

En 1950 Giuga a demandé si la réciproque était vraie. Il est facile de voir, cf. l'exercice 6.2, que si p divise un tel n alors $p^2(p-1)$ divise $n-p$ et que $p-1$ divise $n-1$. Pour l'instant cette question n'a toujours pas de réponse. Dans le même genre d'idées, cf. l'exercice 6.3 pour n premier on a la congruence

$$\binom{2n-1}{n-1} \equiv 1 \mod n^3;$$

la réciproque n'a pour l'instant pas de réponse.

2.2. Factorisation. — La factorisation naive via le crible d'Erathostene est rapidement inefficace car trop longue à mettre en oeuvre : sa complexité est $O(\sqrt{N})$. Nous allons dans ce paragraphe présenter quelques autres algorithmes plus rapides, même si on le rappelle, jusqu'à présent, le problème de la factorisation n'a pas trouvé d'algorithme en temps polynomial. En pratique en 2006 on sait factoriser en quelques heures un nombre entiers de 100 chiffres, en quelques mois avec plusieurs ordinateurs un nombre de 150 chiffres et l'on ne sait toujours pas factoriser en 100 ans, un nombre RSA de 300 chiffres. Dans la suite pour évaluer la complexité des algorithmes considérés, on introduit la notation suivante

$$L(b,N) = \exp\Big(C(\log N)^b(\log\log N)^{1-b}\Big)$$

où C est une constante ; le cas $b=0$ correspond aux algorithmes polynomiaux, le cas $b=1$ aux algorithmes exponentiels et le cas $0<b<1$ aux algorithmes sous-exponentiels.

2.2.1 — L'algorithme de Fermat : bien que l'algorithme que nous allons présenter n'est pas implémenté de nos jours, sauf si le nombre n à factoriser possède deux facteurs relativement proche de $\sqrt{n}$, son principe est au coeur de la plupart des algorithmes modernes. L'idée est la suivante : si n peut s'écrire comme la différence de deux carrés, $n = x^2 - y^2$ alors $n = (x-y)(x+y)$ est une factorisation non triviale de n.
Remarque : tout nombre n impair non premier peut s'écrire sous la forme $x^2 - y^2$: en effet si $n = ab$ alors on peut prendre $x = (a+b)/2$ et $y = (a-b)/2$.

L'algorithme est alors le suivant : on prend $x = \lceil\sqrt{n}\rceil$ et en partant de $y = 0$ et en incrémentant de 1 à chaque fois que $x^2 - y^2 > n$, on teste si $n = x^2 - y^2$. Si un des tests est positif, c'est gagné sinon on incrémente x de 1 et on recommence. Il est possible d'améliorer cet algorithme en implémentant un test probabiliste pour savoir si $x^2 - n$ est un carré, malgré tout cet algorithme est encore trop lent.

2.2.2 — L'amélioration de Kraitchik : le principe est que n n'est pas premier si et seulement si l'équation $x^2 \equiv 1 \mod n$ a au moins 4 solutions. Ainsi si on disposait d'un bon algorithme $\mathcal{A}$ « racine carrée », on factoriserait N comme suit : on prend a au hasard, puis on calcule a^2 dont on prend la racine carrée par l'algorithme $\mathcal{A}$: il y a alors au moins une chance sur deux pour que le résultat b soit différent de a de sorte que $n \wedge (a \pm b)$ fournit un diviseur non trivial de n. Evidemment on ne dispose pas de tel algorithme et il est raisonnable de penser qu'il n'en existe pas.

L'idée est alors de considérer des paires « aléatoires » d'entiers (x, y) telles que $x^2 \equiv y^2 \mod n$ de sorte que n divise $(x-y)(x+y)$ de sorte que « moralement » il y a une chance sur 2 pour que les facteurs premiers de n se répartissent sur les deux facteurs $(x-y)$ et $(x+y)$. Ainsi le pgcd $(x-y) \wedge (x+y)$ a de bonnes chances de donner un diviseur non trivial de n.

Peu après, en 1931, D. H. Lehmer et R. E. Powers ont montré comment construire de telles paires systématiquement en utilisant les fractions continues. L'idée est la suivante : si t est petit avec $x^2 \equiv t \mod n$, alors $x = t + kd^2n$ et donc $(x/d)^2 - kn = t/d^2$ est petit, autrement dit x/d est une bonne approximation de $\sqrt{kn}$. Or on sait que les fractions continues sont de bonnes approximations rationnelles : ainsi on calcule via les fractions continues de bonnes approximations P/Q de $\sqrt{kn}$ pour divers k et on essaie de factoriser $t = P^2 - Q^2kn$ via la base de petits nombres premiers que l'on considère.

Remarque : avec l'arrivée d'ordinateurs puissants, des algorithmes particulièrement performants ont alors été utilisés dès les années 70. Récemment avec l'arrivée de la mémoire à bon marché, des algorithmes plus rapides sont utilisés comme celui du crible quadratique que nous présentons plus loin.

2.2.3 — L'algorithme de Dixon : on choisit a proche de $\sqrt{N}$ au hasard et on réduit a^2 modulo N en prenant le représentation dans $[-N/2, N/2]$ et on regarde si on peut le factoriser avec des petits facteurs premiers. Une fois que l'on a obtenu quelques a_i, b_j on essaie de construire une égalité du type

$$a^2 = \prod_i a_i^2 \equiv \prod_j b_j = b^2 \mod N$$

En remarquant que si N n'est pas premier, il y a dans $(\mathbb{Z}/N\mathbb{Z})^\times$ au moins 4 racines carrés de 1, on en déduit qu'il y a au moins une chance sur deux pour que $\pm b$ soit distinct de a. On a alors une chance sur deux en étudiant $(a-b \wedge N)$ et $(a+b \wedge N)$ d'obtenir une factorisation non triviale de N. Cet algorithme a en fait une complexité $L(1/2, N) = \exp(C(\log N)^{1/2}(\log\log N)^{1/2})$ ce qui est déjà remarquable même si insuffisant pour factoriser de très grands nombres.

Dans la pratique par petits diviseurs de a on entend plus petit que 10^4. On répète le processus de sorte à trouver un nombre de telles factorisation plus grand que le nombre de premier plus petit que 10^4, i.e. ici 1229. On représente alors une telle factorisation $p_1^{r_1} \cdots p_{1229}^{r_{1229}}$ par le vecteur $v(a) = (r_1, \cdots, r_{1229})$. Si toutes les coordonnées de $v(a)$ sont paires alors $a^2 - n$ est un carré ce qui donne une factorisation de n. Dans le cas contraire comme on a plus de vecteurs que de coordonnées, on en déduit qu'il existe une somme de $v(a)$ dont toutes les coordonnées sont paires : pour obtenir cette somme, on pose $w(a) = (s_1, \cdots, s_{1229})$ avec $s_i = 0$ si r_i est paire et $s_i = 1$ sinon. L'algorithme de Gauss sur les vecteurs $w(a)$ de $(\mathbb{Z}/2\mathbb{Z})^{1229}$, très rapide dans cette situation, fournit alors la somme à considérer.

2.2.4 — L'amélioration de Pomerance (1981) : le crible quadratique. Au lieu de prendre les a au hasard dans l'algorithme de Dixon, on prend $k = \lfloor \sqrt{n} \rfloor$ et on considère pour $a = k+1, k+2, \cdots \leq \sqrt{2n}$, les entiers $Q(a) = a^2 - N$. Supposons que l'on ait déjà testé que les premiers p inférieurs à 10^4 ne divisent pas n de sorte que si p divise $a^2 - n$ alors $\left(\frac{n}{p}\right) = 1$. Ainsi il ne faut tester la divisibilité de $a^2 - n$ que la moitié des premiers $p \leq 10^4$, ceux pour lesquels n est un résidu quadratique modulo p : cet ensemble de premiers est appelé *la base de facteurs*. Pour un tel premier on a $n \equiv (\pm t)^2$ et donc $a \equiv \pm t \mod p$: réciproquement si $a \equiv \pm t$ alors p divise $a^2 - n$.

Le procédé est alors le suivant : on prend dans l'ordre croissant les premiers de la base de facteur, étant donné un tel p soit $a_+(p) \geq \sqrt{n}$ le plus petit entier congru à t modulo p. On

sait alors que p divise $Q(a_+(p)) = a_+(p)^2 - n$, ainsi que tous les $Q(a_+(p) + pk)$. On considère alors une table $b(a)$ indexée par les k en l'initialisant à $\ln Q(a)$; pour un tel p on soustrait alors à chacun des entrées indexées par $a_+(p) + kp$ la valeur $\ln p$. On recommence ce procédé pour les $a_-(p) \equiv -t \mod p$ puis on passe au p suivant. Les calculs sur les ln sont arrondi à la partie entière et quand les $b(a)$ sont proches de zéro alors $a^2 - n$ se factorise avec des petits premiers.
Remarque : dans le procédé ci-dessus, il faut aussi tenir compte du fait que p peut diviser $a^2 - n$ plus d'une fois, de sorte que l'on est amené à résoudre des congruences $x^2 \equiv n \mod p^r$ avec $1 \leq r \leq 2 \ln L / \ln p$ où L est le plus grand premier dans la base de facteurs. Dans la pratique, on peut ignorer ces puissances.
Remarque : plus la majoration demandée sur les petits premiers sera grande plus la probabilité que $a^2 - n$ soit factorisable dans la base de facteurs associée sera grande, par contre la résolution du système linéaire associé par la méthode de Gauss sera plus longue.
Remarque : le but étant de trouver des a tels que $a^2 - n$ ait des petits facteurs, on peut s'intéresser au cas de 2. Les entiers à factoriser sont bien évidemment impairs ; si $n \equiv 3, 7 \mod 8$ alors $a^2 - n \equiv 2 \mod 4$ pour tout $a \equiv 1 \mod 2$, si $n \equiv 5 \mod 8$ alors $a^2 - n \equiv 4 \mod 8$ et si $n \equiv 1 \mod 8$ alors $a^2 - n \equiv 0 \mod 8$. Afin de se retrouver dans la situation favorable où $n \equiv 1 \mod 8$, on multiplie n par $3, 5, 7$ de façon à s'y ramener : l'algorithme précédent est tout aussi rapide à trouver de grands facteurs pour n que pour $3n$.
Remarque : pour p premier dans la base de facteurs, i.e. p petit et n est un résidu quadratique modulo p, il faut savoir résoudre l'équation $x^2 \equiv n \mod p$.

2.2.5 — Algorithme ρ de Pollard : cet algorithme construit en 1975 est le plus efficace pour trouver des petits facteurs par exemple d'ordre 10^7. En pratique, on commence par l'utiliser systématiquement pour tester s'il y a des diviseurs d'ordre 10^5 et dans la négative, on passe à des algorithmes plus efficaces comme le crible quadratique.

On choisit a_0 entre 1 et N et on considère la suite $a_{i+1} = f(a_i)$ avec $f(a) = a^2 + 1 \mod N$. On suppose que la suite des a_i modulo p est suffisamment aléatoire, ce qui est assez bien vérifié par l'expérience et la pratique. Ainsi la probabilité pour que r nombres pris au hasard modulo p soient tous distincts est

$$P_r = (1 - \frac{1}{p})(1 - \frac{2}{p}) \cdots (1 - \frac{r-1}{p}) \leq \exp(-\frac{r(r-1)}{2p})$$

Prenons r de l'ordre de $\sqrt{p}$ et disons $r > 2\sqrt{p}$ de sorte que $P_r \leq \exp(-r(r-1)/(2p)) \leq \exp(-2 + 1/\sqrt{p}) < 1/2$. On a ainsi une bonne chance qu'il existe $1 < i < j < r$ tels que $a_i \equiv a_j \mod p$ ce qui implique $a_{i+m} \equiv a_{j+m} \mod p$ pour tout $m \geq 0$. Ainsi pour $m = j - 2i$ et $k = j - i$ on aura $a_k \equiv a_{2k} \mod p$. En résumé on a au moins une chance sur deux qu'il existe k d'ordre $O(\sqrt{p})$ tel que $(a_{2k} - a_k) \wedge n$ soit distinct de 1, ce qui fournit un algorithme qui avec une bonne probabilité donne une factorisation de N en temps $O(\sqrt[4]{N})$.

2.2.6 — Algorithme $p - 1$ de Pollard : supposons que n possède un facteur premier p tel que les facteurs premiers de $p - 1$ soient petits, i.e. plus petit que 10^4. Supposons en fait que $p - 1$ divise 10000!. Comme l'exponentiation modulo n est très rapide, on calcule $m = 2^{10000!} \mod n$. Comme $p - 1$ divise 10000!, $m \equiv 1 \mod p$ et donc p divise $m - 1$ et comme par ailleurs il y a de bonnes chances que n ne divise pas 10000!, $g = (m - 1) \wedge n$ devrait être un facteur non trivial de n. Dans la pratique on teste $(2^{k!} - 1) \wedge n$, s'il est égal à 1 on passe à $k + 1$ et s'il est égal à n alors on peut essayer de remplacer 2 par une autre valeur c, ou alors essayer un autre algorithme.

2.2.7 — Méthode de factorisation de Lenstra : soit Y un entier ; on dit qu'un nombre est *Y-friable* (resp. *Y-puissance friable*) si tous ses diviseurs premiers sont inférieurs à Y (resp. si toute puissance d'un premier le divisant est inférieure à Y). Soit N le nombre à factoriser et p un diviseur de N ; si $p-1$ est Y-puissance friable pour Y de taille raisonnable, alors $p-1$ divise $m(Y) = ppcm(2, 3, \cdots, Y)$. Si donc $a \wedge N = 1$, alors $a^{m(Y)} \equiv 1 \mod p$ et donc

$$(a^{m(Y)} - 1) \wedge N \neq 1.$$

La méthode sera donc efficace si N possède un facteur premier Y-puissance friable pour Y pas trop grand : le problème est que les grands nombres premiers tels que $p-1$ soit Y-friable sont assez rares. L'idée clef de l'algorithme de Lenstra est que l'on est en train de raisonner dans $(\mathbb{Z}/p\mathbb{Z})^\times$ qui est cyclique de cardinal $p-1$ (cf. ci dessus l'algorithme $p-1$ de Pollard). Ainsi plus généralement soient n un entier à factoriser et G un groupe tel que :

- l'ensemble sous-jacent à G est un sous-ensemble de $(\mathbb{Z}/n\mathbb{Z})^r$ pour un certain entier r ;
- la loi de G est définie en termes d'opérations arithmétiques modulo n.

Pour $d|n$, on note $G|d$ le groupe obtenu à partir de G en réduisant les coordonnées modulo d.

Proposition 2.2.8. — *Soient n et G comme ci-dessus.*
(1) Test de primalité : s'il existe un $x \in G$ et un entier m satisfaisant les conditions suivantes, alors n est premier :

- *m est plus grand que l'ordre de $G|q$ pour tout éventuel diviseur q de n inférieur à $\sqrt{n}$;*
- *$x^m = e$ l'élément identité de G ;*
- *pour tout premier p divisant m, une coordonnée de $x^{m/p} - e$ est première à n.*

(2) Factorisation : soit p premier divisant n, si l'ordre de $G|p$ divise $k!$ et si n ne divise pas la i-ème coordonnées de $x^{k!} - e$ alors le pgcd de celle-ci avec n fournit un diviseur non trivial de n.

Preuve : (1) Si n n'est pas premier soit alors q un diviseur plus petit que $\sqrt{n}$. Soit alors x et m vérifiant les deux dernières propriétés de l'énoncé. On en déduit alors que l'image de x dans $G|q$ est égale à m ce qui contredit la première hypothèse.

(2) Le résultat découle du fait que p divise toutes les coordonnées de $x^{k!} - e$. □

Remarque : l'algorithme $p-1$ de Pollard correspond à l'application de cette proposition pour le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Ainsi pour trouver un diviseur q de n, il faut que $q-1$ divise $k!$ pour un entier $k \ll$ petit $\gg$. Pour appliquer pleinement la proposition précédente, il faut disposer de nombreux exemples de groupes G comme ci-dessus. Les courbes elliptiques $E(a,b) : \{[x,y,z] \in \mathbb{P}^2(\mathbb{C}) : zy^2 = x^3 + axz^2 + bz^3\}$ que l'on regarde modulo n fournissent de tels exemples. Citons sans démonstration les résultats suivants.

Théorème 2.2.9. —

- *(Hasse) L'ordre de $E(a,b)|p$ appartient à l'intervalle $I(p) =]p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}[$.*
- *(Waterhouse) Étant donné un premier $p \geq 3$ et $n \in I(p)$, il existe a et b tels que le cardinal de $E(a,b)|p = n$.*
- *(conjecture de Sato-Tate prouvée en 2006 par M. Harris et R. Taylor) On écrit*

$$-\frac{1}{2\sqrt{p}}(|E(a,b)|p - p - 1) = \cos(\theta_{a,b}),$$

alors la mesure de probabilité de θ est $\frac{2}{\pi}\sin\theta^2 d\theta$.

Ainsi pour factoriser n, il suffit de trouver un entier un entier dans un intervalle $I(p)$ qui divise $k!$ ce qui est bien plus souple que la méthode $p-1$ de Pollard. Cependant il n'est

pas simple de calculer l'ordre de $E(a,b)|p$, ni étant donné $n \in I(p)$ de trouver a et b tels que $E(a,b)|p$ soit de cardinal n. Le procédé consiste alors, d'après Sato-Tate, à prendre des courbes elliptiques « au hasard ».
Remarque : on peut montrer que la complexité de cet algorithme est $\exp\sqrt{2\log p \log\log p}$ où p est le plus petit facteur premier divisant N. Par ailleurs cet algorithme est peu gourmand en mémoire puisque l'on doit stocker un nombre de données polynomial en $\log N$.
Remarque : il existe un autre algorithme moins élémentaire appelé *le crible algébrique* dont la complexité est de l'ordre de $L(1/3)$ qui est donc plus efficace que celui de Lenstra pour les N ne possédant pas de facteurs premiers de taille moyenne, ce qui est typiquement le cas pour RSA. Enfin en 1997, Shor a montré que le problème de la factorisation pouvait être résolu en temps polynomial à l'aide d'un ordinateur quantique dont un premier exemplaire vient juste d'être construit.

3. Aspects analytiques

3.1. Répartition des nombres premiers. — Commençons par une citation du grand Euler : « Les mathématiciens ont tâché jusqu'ici en vain de découvrir quelque ordre dans la progression des nombres premiers, et l'on a lieu de croire que c'est un mystère auquel l'esprit humain ne saura jamais pénétrer. Pour s'en convaincre, on n'a qu'à jeter les yeux sur les tables des nombres premiers que quelques-uns se sont donné la peine de continuer au-delà de cent mille et l'on s'apercevra d'abord qu'il n'y règne aucun ordre ni règle. »Ne nous décourageons pas pour autant et essayons de voir ce que l'on peut actuellement dire sur le sujet.

3.1.1 — Théorème de Dirichlet : nous avons déjà vu que l'ensemble $\mathcal{P}$ des nombres premiers était infini. Dirichlet améliore ce résultat, en affirmant que pour tout $a \wedge b = 1$, il existe une infinité de nombres premiers $p \equiv a \mod b$. En utilisant la loi de réciprocité quadratique, on peut montrer quelques cas simples.

Proposition 3.1.2. — *Il existe une infinité de nombres premiers p tels que*
(a) $p \equiv 3 \mod 4$ *;* *(b)* $p \equiv 1 \mod 4$ *;*
(c) $p \equiv 1 \mod 2^m$ *;* *(d)* $p \equiv 5 \mod 6$ *;*
(e) $p \equiv 5 \mod 8$ *;* *(f)* $p \equiv 1 \mod 6$ *;*
(g) $p \equiv -1 \mod 12$ *;* *(h)* $p \equiv -1 \mod 10$.

Preuve : Le schéma de démonstration sera toujours le même : on raisonne par l'absurde en supposant la finitude de l'ensemble considéré et on construit un entier N qui permet d'aboutir à une contradiction. On note n le plus grand élément de l'ensemble supposé fini. Toute la difficulté revient donc à construire N en fonction de n et de l'ensemble considéré :

(a) $N = n! - 1$; si p divise N alors $p > n$ et donc $p \equiv 1 \mod 4$ de sorte que $N \equiv 1 \mod 4$ ce qui n'est pas.

(b) $N = (n!)^2 + 1$; si p premier divise N alors -1 est un carré modulo p soit $p \equiv 1 \mod 4$ et donc par hypothèse $p \leq n$ soit p divise $n!$ et donc $p|N - (n!)^2 = 1$ d'où la contradiction .

(c) si p divise $a^{2^{m-1}} + b^{2^{m-1}}$ avec p premier avec a, alors $\frac{a}{b}$ est d'ordre divisant 2^m et d'ordre distinct de 2^{m-1} ; il est donc d'ordre 2^m. Or l'ordre de tout élément divise le cardinal du groupe soit $p \equiv 1 \mod 2^m$. Soit alors $N = (n!)^{2^{m-1}} + 1$; tout diviseur p premier de N est congru à $1 \mod 2^n$ et supérieur à n d'où la contradiction.

(d) $p \equiv 5 \mod 6$ est équivalent à $p \equiv 1 \mod 2$ et $p \equiv 2 \mod 3$ soit $p > 2$ et $p \equiv 2 \mod 3$. Soit $N = n! - 1$; pour p premier divisant N, on a $p > n$ et donc $p \equiv 1 \mod 3$ de sorte que $N \equiv 1 \mod 3$ ce qui n'est pas.

(e) $N = 3^2 5^2 7^2 11^2 \cdots n^2 + 2^2$; N est visiblement impair. Soit alors p premier divisant N, p ne divise pas 4, de sorte que $p \equiv 1 \mod 4$, soit $p \equiv 1, 5 \mod 8$. À nouveau $p \equiv 5 \mod 8$ est exclu car sinon p diviserait $4 = N - 3^2 \cdots n^2$. On en déduit donc $N \equiv 1 \mod 8$. Or si p est premier impair on a $p \equiv 1, 3, 5, 7 \mod 8$ et on vérifie aisément que p^2 est alors congru à 1 modulo 8 et donc $N \equiv 5 \mod 8$, d'où la contradiction.

(f) $p \equiv 1 \mod 6$ est équivalent à $p > 2$ et $p \equiv 1 \mod 3$. Or si p divise $a^2 + 3b^2$ et p premier avec b, alors -3 est un carré modulo p et donc $(\frac{-3}{p}) = 1 = (-1)^{(p-1)(3-1)/4}(\frac{p}{3})(\frac{-1}{p}) = (\frac{p}{3})$ et donc -3 est un carré modulo p si et seulement si $p \equiv 1 \mod 3$. Soit alors $N = 3(n!)^2 + 1$; tout diviseur premier de N est alors congru à 1 modulo 3 et supérieur à n d'où la contradiction.

(g) si p divise $a^2 - 3b^2$ et p premier avec b alors 3 est un carré modulo p. Or on a $(\frac{3}{p}) = (\frac{p}{3})(-1)^{(p-1)/2}$ et donc 3 est un carré modulo p dans les deux situations suivantes :

- $(\frac{p}{3}) = (-1)^{(p-1)/2} = 1$ soit $p \equiv 1 \mod 3$ et $p \equiv 1 \mod 4$ soit $p \equiv 1 \mod 12$;
- $(\frac{p}{3}) = (-1)^{(p-1)/2} = -1$ soit $p \equiv -1 \mod 3$ et $p \equiv -1 \mod 4$ soit $p \equiv -1 \mod 12$;

Soit alors $N = 3(n!)^2 - 1$; tout diviseur premier p de N est alors congru à ± 1 modulo 12 et supérieur à n de sorte que par hypothèse, $p \equiv 1 \mod 12$. On en déduit alors que $N \equiv 1 \mod 12$ ce qui n'est pas car $N \equiv -1 \mod 12$.

(h) pour p premier $p \equiv -1 \mod 10$ si et seulement si $p \equiv -1 \mod 5$. Or si p divise $a^2 - 5b^2$ avec p premier avec b alors $(\frac{5}{p}) = 1 = (\frac{p}{5})$ et donc $p \equiv \pm 1 \mod 5$. Soit alors $N = 5(n!)^2 - 1$; tout diviseur premier p de N est strictement supérieur à n et congru à $\pm 1 \mod 5$. Par hypothèse il est donc congru à 1 modulo 5 et donc N aussi ce qui n'est pas. □

Cas $a = 1$: soit $L = Dec_{\mathbb{F}_p}(X^n - 1)$. Le corps L est isomorphe à $\mathbb{F}_{p^r}$ pour un certain r et $\mathrm{Gal}(L/\mathbb{F}_p) \simeq \mathbb{Z}/r\mathbb{Z}$ engendré par Fr_p. En outre on a $L = \mathbb{F}_p[\chi]$ pour $\chi \in L$ une racine primitive n-ième de l'unité. Ainsi un élément $\sigma \in \mathrm{Gal}(L/\mathbb{F}_p)$ est déterminé par $\sigma(\chi)$ qui doit être une racine primitive n-ième de l'unité et donc de la forme χ^k pour $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. On obtient ainsi une application injective naturelle

$$\sigma \in \mathrm{Gal}(L/\mathbb{F}_p) \longmapsto k \in (\mathbb{Z}/n\mathbb{Z})^\times$$

l'image étant le groupe engendré par la classe de p. Ainsi r est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Soit $\bar{\Phi}_n(X) = P_1 \cdots P_s$ la décomposition en irréductibles de la réduction modulo p de Φ_n. Soit χ une racine de P_1 de sorte que $L = \mathbb{F}_p[\chi]$ et donc P_1 est le polynôme minimal de χ sur $\mathbb{F}_p$ et donc $\deg P_1 = [L : \mathbb{F}_p]$. En conclusion tous les P_i sont de même degré $[L : \mathbb{F}_p]$ et donc $s = \frac{\psi(n)}{[L:\mathbb{F}_p]}$ où l'on rappelle que $[L : \mathbb{F}_p]$ est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Ainsi $p \equiv 1 \mod n$ est équivalent à demander que $\bar{\Phi}_n$ est totalement décomposé sur $\mathbb{F}_p$ ce qui on vient de le voir, est équivalent à demander que $\bar{\Phi}_n$ a une racine dans $\mathbb{F}_p$. Soit donc p premier divisant $\Phi_n(N!) \equiv 1 \mod N!$ soit $p > N$ et $p \equiv 1 \mod n$ car $\bar{\Phi}_n$ a pour racine $\bar{N}!$. On vient donc de montrer une version faible du théorème de progression arithmétique dont l'énoncé fort est que pour tout a premier avec n, il existe une infinité de premiers congrus à a modulo n, ceux-ci se répartissant de manière uniforme en un sens que l'on ne précise pas ici, sur les $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Remarque : en 2005 Benjamin Green et Terence Tao généralise encore le théorème de Dirichlet en prouvant que pour tout entier k, il existe une infinité de suites de k nombres premiers en

progression arithmétique, i.e. il existe a et b tels que

$$a,\ a+b,\ a+2b,\ \cdots, a+(k-1)b \in \mathcal{P}$$

Par exemple pour $k=10$ le plus petit a est 199 avec $b=210$ ce qui donne

$$199,\ 409,\ 619,\ 1039,\ 1249,\ 1459,\ 1669,\ 1879,\ 2089.$$

Étant donné k on peut noter a_k et b_k les plus petits entiers tels que a_k+ib_k soient premiers pour tout $i=0,\cdots,k-1$; Green et Tao donne une majoration de la taille de $a_k+(k-1)b_k$ en fonction de k.

3.1.3 — Théorème des nombres premiers : nous avons vu que $\mathcal{P}$ était infini, on ne peut donc pas le dénombrer mais on peut par contre essayer de compter ses éléments dans des compacts, typiquement $[0,x]$ et s'il n'est pas possible d'obtenir une formule, essayer de trouver un équivalent, voire un développement limité de ce nombre quand $x \to +\infty$.

Théorème 3.1.4. — *Pour $x>0$, soit $\pi(x)$ le cardinal de l'ensemble des nombres premiers inférieurs ou égaux à x ; on a alors l'équivalent suivant quand x tends vers $+\infty$:*

$$\pi(x) \sim \frac{x}{\ln x}.$$

Remarque : la démonstration classique utilise des résultats d'analyse complexe ; il existe toutefois une preuve purement algébrique, élémentaire et donc très difficile, due indépendamment à Erdös et Selberg. Un résultat du à Tchebychef qui est relativement simple à prouver est l'encadrement suivant

$$c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_2 \frac{x}{\ln x},$$

avec $c_1 = \ln\left(\frac{\sqrt{2}\sqrt[3]{3}\sqrt[5]{5}}{\sqrt[30]{30}}\right) \simeq 0,921$ et $C_2 = 6c_1/5 \simeq 1,106$. Ce dernier résultat suffit à prouver :

- *le postulat de Bertrand* à savoir que $\pi(2n)-\pi(n)>0$;
- les résultats d'Ishikawa : $p_n+p_{n+1}>p_{n+2}$ et $p_np_m>p_{n+m}$.

Une autre façon d'interpréter le théorème des nombres premiers est :

- p_n est de l'ordre de $n\ln n$; plus précisément Felgner en 1990 a montré que

$$0,91n\ln n < p_n < 1,7n\ln n;$$

- autour de n l'écart moyen entre deux nombres premiers est de l'ordre de $\ln n$.

3.1.5 — La fonction trou : la fin du paragraphe précédent suggèrent d'étudier la fonction trou sur $\mathcal{P}$ définie comme suit :

$$p_{n+1} = p_n + g(p_n) + 1.$$

- Notons déjà que $\limsup g = +\infty$; en effet l'intervalle $[n^2, n^2+n]$ ne contient aucun nombre premier, on construit ainsi des « trous » dans $\mathcal{P}$ aussi large que l'on veut.
- En ce qui concerne la limite inf, on conjecture qu'elle est égale à 1, i.e. il existe une infinité de premiers jumeaux, soit $p, p+2 \in \mathcal{P}$.
  Remarque : en 1919, Brun a montré que la somme des inverses des nombres premiers jumeaux était convergente. Notons $\pi_2(x)$ le nombre de premiers $p \leq x$ tels que $p+2 \in \mathcal{P}$, Hardy et Littlewood conjecturent que

$$\pi_2(x) \sim 2C_2 \int_2^x \frac{dt}{(\ln t)^2}, \quad C_2 = \prod_{p\geq 3} \frac{p(p-2)}{(p-1)^2} \simeq 0,66.$$

– Le théorème des nombres premiers nous dit que pour tout $\epsilon > 0$, il existe n_0 tel que pour tout $n \geq n_0$, on a $g(p_n) \leq \epsilon p_n$. En 1937 Ingham a amélioré cette majoration en montrant que pour tout $\epsilon > 0$, il existe une constante K telle que $g(p) \leq K p^{5/8+\epsilon}$ et depuis le 5/8 a été régulièrement amélioré.
– Le théorème des nombres premiers dit que la valeur moyenne de $g(p)/\ln p$ est égale à 1 et Ricci a montré que l'ensemble des valeurs d'adhérences de $\{g(p)/\ln p : \ p \in \mathcal{P}\}$ avait une mesure de Lebesgue non nulle bien qu'à l'instant seul $+\infty$ ait été exhibé, prouvé en 1931 par Westzynthius. Maier a montré que la plus petite de ces valeurs d'adhérence était $\leq 0,249$: bien évidemment on pense qu'elle est en fait égale à 0 comme le suggère la conjecture des nombres premiers jumeaux.
– Sous l'hypothèse de Riemann, Cramer a montré l'existence d'une constante K telle que $g(p) < K\sqrt{p}\ln p$. On conjecture en fait qu'il existe une constante K telle que

$$g(p) \leq K(\ln p)^2.$$

3.1.6 — Quelques autres conjectures : une étude assez simple des anneaux euclidiens $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$ et $\mathbb{Z}[i\sqrt{3}]$ permet de montrer que :

$$\begin{array}{rcl} p = x^2 + y^2 & \Leftrightarrow & p \equiv 1 \mod 4 \\ p = x^2 + 2y^2 & \Leftrightarrow & p \equiv 1, 3 \mod 8 \\ p = x^2 + 3y^2 & \Leftrightarrow & p = 3 \text{ ou } p \equiv 1 \mod 3 \end{array}$$

Plus généralement on peut montrer le résultat suivant.

Théorème 3.1.7. — *Soit $n > 0$ un entier sans facteur carré tel que $n \not\equiv 3 \mod 4$. Il existe alors un polynôme irréductible unitaire $f_n(X) \in \mathbb{Z}[X]$ de degré $h(-4n)$ tel que si p premier impair ne divisant pas n ni le discriminant de $f_n(X)$ alors*

$$p = x^2 + ny^2 \Leftrightarrow \left\{ \begin{array}{l} (\frac{-n}{p}) = 1 \text{ et } f_n(x) \equiv 0 \mod p \\ \text{a une solution entière} \end{array} \right.$$

Exemples pour $n = 14$ on obtient

$$p = x^2 + 14y^2 \Leftrightarrow \left\{ \begin{array}{l} (\frac{-14}{p}) = 1 \text{ et } (x^2+1)^2 \equiv 8 \mod p \\ \text{a une solution entière.} \end{array} \right.$$

En ce qui concerne le cas d'une seule variable, on conjecture que si a, b, c sont premiers entre eux avec $a > 0$, $a + b \equiv c \equiv 1 \mod 2$ et $b^2 - 4ac$ qui n'est pas un carré parfait, alors il existe une infinité de premiers de la forme $an^2 + bn + c$: le cas classique est $n^2 + 1$ que l'on ne sait toujours pas prouver.

Relativement à la fonction π, Hardy et Littlewood conjecturent [2] que pour tout $x, y \geq 2$:

$$\pi(x + y) \leq \pi(x) + \pi(y)$$

ce qui implique en particulier la conjecture des nombres premiers jumeaux. Enfin on conjecture que $\pi(n^2) < \pi((n+1)^2)$.

Plus généralement, soient $f_1, \cdots, f_k$ des polynômes de degré 1, irréductibles et vérifiant la propriété que pour tout nombre premier p il y ait au moins un entier n parmi $0, \cdots, p-1$ tel que p ne divise pas le produit des $f_i(n)$. On note $\omega(p)$ le complémentaire à p du nombre de tels entiers. Un tel ensemble de polynômes est dit admissible ; on cherche à connaître la proportion d'entiers en lesquels les polynômes prennent simultanément des valeurs premières.

2. La croyance des experts est que cette conjecture devrait pouvoir être infirmée.

Remarque : se limiter à des ensembles de polynômes admissibles permet d'éviter des cas triviaux comme $f_1(t) = t$, et $f_2(t) = t + 1$.

Il est alors conjecturé que le nombre d'entiers $n \leq x$ tels que les valeurs $f_1(n), \cdots, f_k(n)$ sont simultanément premières, est pour x assez grand, de l'ordre de :

$$\Big(\prod_{p\in\mathcal{P}} \frac{1-\frac{\omega(p)}{p}}{(1-\frac{1}{p})^k}\Big)\frac{x}{\ln|f_1(x)|\cdots\ln|f_k(x)|}.$$

Le théorème des nombres premiers correspond au cas $k = 1$ et $f_1 = t$, le théorème de Dirichlet à $k = 1$ et $f_1 = at + b$, et pour $k = 2$, $f_1(t) = t$ et $f_2(t) = t + 2$, on obtient une version quantitative (et donc plus générale) de la conjecture des nombres premiers jumeaux.

La conjecture de Goldbach affirme que tout entier $n > 2$ pair est la somme de deux nombres premiers. Schnizel a montré que la conjecture de Goldbach était équivalente au fait que tout entier $n > 17$ était la somme de trois premiers distincts. Ramaré a montré que tout entier n est la somme d'au plus 6 nombres premiers et en 1966 Chen a montré que tout entier suffisament grand est la somme d'un nombre premier et d'un entier possédant au plus deux facteurs premiers.

La conjecture de Polignac affirme que tout entier naturel pair peut s'écrire comme différence de deux nombres premiers consécutifs et cela d'une infinité de manières.

Soit la suite, dite *d'Euclide-Mullin*, de premier terme $u_1 = 2$ et telle que le terme u_n soit le plus petit nombre premier diviseur du produit des termes u_i, pour $i < n$, augmenté de 1. Daniel Shanks conjecture que l'on obtient ainsi tous les nombres premiers.

3.2. La fonction zêta de Riemann. — Elle est définie pour Re $(s) > 1$ par la série $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. Cette fonction et ses généralisations (fonctions zêta de Dedekind, de Hasse-Weil, et plus généralement les fonctions L de Dirichlet, des formes modulaires, représentations automorphes...) jouent un rôle central en arithmétique. En particulier leurs valeurs aux entiers contiennent une multitude de renseignements concernant l'arithmétique des objets auxquels elles sont en fait attachées.

En guise d'introduction signalons la preuve d'Euler du fait qu'il existe une infinité de nombres premiers : celle-ci repose sur ce que désormais on appelle produit eulérien. Soit $f : \mathbb{N} \longrightarrow \mathbb{C}$ une fonction fortement multiplicative, i.e. $f(nm)f(n)f(m)$ pour tout n, m ; en particulier comme $f(n)f(1) = f(n)$, en prenant n tel que $f(n) \neq 0$, on obtient $f(1) = 1$. On suppose en outre que la série $\sum_n |f(n)|n^{-s}$ est absolument convergente de sorte que la série $\sum_k f(p^k)p^{-ks}$ est égale à $(1 - f(p)p^{-s})^{-1}$ et pour tout entier N

$$u_N(s) = \prod_{p\leq N}(\sum_k f(p^k)p^{-ks})$$

est un produit fini de séries absolument convergentes que l'on peut développer en utilisant la multiplicativité de f, soit $u_N(s) = \sum_n f(n)n^{-s}$ où la somme porte sur les n dont les facteurs premiers sont inférieurs à N.

Remarque : si on suppose seulement que f est multiplicative, i.e. $f(mn) = f(m)f(n)$ pour tout $n \wedge m = 1$, on obtient alors l'égalité

$$\sum_n f(n)n^{-s} = \prod_p (1 + f(p)p^{-s} + f(p^2)p^{-2s} + \cdots)$$

Considérons alors le cas où $f(n) = 1$ pour tout $n \geq 1$ de sorte que si la série $\sum_{p\in\mathcal{P}} \frac{1}{p}$ converge alors la série des $\log(1 - 1/p)$ converge aussi et donc le produit $\prod(1 - 1/p)^{-1}$ converge. On en

déduit alors que la série $\sum_n 1/n$ converge, ce qui est faux. Au final on obtient outre l'existence d'une infinité de nombres premiers, le fait que la série $\sum_{p\in\mathcal{P}} p^{-1}$ diverge, ce qui est plus fort.

Citons quelques résultats connus ou conjecturés sur la fonction ζ :

- **Prolongement analytique** : ζ a un prolongement méromorphe à $\mathbb{C}$ tout entier, holomorphe en dehors d'un pôle simple en $s = 1$ de résidu 1 ;
- pour $n \in \mathbb{N}$, on a $\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1} \in \mathbb{Q}$, où B_n est le n-ème nombre de Bernouilli, i.e. $\sum_{n=1}^{\infty} \frac{B_n t^n}{n!} = \frac{t}{e^t-1}$

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad \cdots, \quad B_{12} = -\frac{691}{2730}$$

- $\pi^{-2k}\zeta(2k) = \frac{2^{2k-1}(-1)^k}{(2k)!} B_{2k} \in \mathbb{Q}$.
- Kummer : si $p \geq 3$ premier ne divise pas $\zeta(-1), \zeta(-3), \cdots, \zeta(2-p)$ alors p ne divise pas le nombre de classes d'idéaux du corps $\mathbb{Q}(e^{2i\pi/p})$;
- Mazur et Wiles : ont donné une formule faisant intervenir le groupe des classes d'idéaux des $\mathbb{Q}(e^{2i\pi/p^n})$, pour calculer la puissance de p qui divise exactement le numérateur de $\zeta(-2k-1)$;
- Rivoal : il existe une infinité de $\zeta(2k+1)$ qui sont irrationnels ;
- **Hypothèse de Riemann** : hormis les zéros triviaux en les $-2n$, tous les autres sont sur la droite critique Re $(s) = 1/2$: ce que l'on sait :
  - les zéros non triviaux sont dans la bande critique $0 <$ Re $(s) < 1$ et même dans une certaine zone...
  - il y a une infinité de zéros sur la droite critique ;
  - au moins $1/3$ des zéros sont sur la droite critique.

Elle a des applications très importantes sur la répartition des nombres premiers :

$$\pi(x) = \mathrm{Li}(x) + \mathcal{O}(\sqrt{x}\log x)$$

où $\mathrm{Li}(x) := \int_2^x \frac{dt}{\ln t}$: le théorème des nombres premiers donne $\pi(x) \sim \mathrm{Li}(x)$.

4. Applications diverses

4.1. Développement décimal de $1/p$. — Partons de quelques constatations amusantes :

$$\frac{1}{7} = 0,142\ 857\ 142\ 857\ 142\ 857\cdots$$

avec $7 \times 142857 = 999999$, $142 + 857 = 999$, $14 + 28 + 57 = 99$, $1 + 4 + 2 + 8 + 5 + 7 = 3 \times 9$ et encore

$$\frac{1}{7} = 0,142857\cdots, \quad \frac{2}{7} = 0,285714\cdots, \quad \frac{3}{7} = 0,428571\cdots$$
$$\frac{4}{7} = 0,571428\cdots, \quad \frac{5}{7} = 0,714285\cdots, \quad \frac{6}{7} = 0,857142\cdots$$

Sans calculs le 53-ème chiffre de $1/53$ est 0, le 52-ème étant 3 car $3 \times 3 = 9$. Essayons désormais d'ordonner toutes ces coïncidences.

Proposition 4.1.1. — *Le développement décimal de $\frac{1}{p}$ est périodique, après la virgule, de période l'ordre de 10 dans $(\mathbb{Z}/p\mathbb{Z})^\times$.*

Preuve : L'écriture s'obtient en effectuant la division euclidienne par p, puis en multipliant le reste par 10 et en effectuant la division euclidienne par p... Ainsi en notant r_k les restes et q_k les quotients qui sont donc les chiffres du développement décimal de $\frac{1}{p}$, on a :

$$\begin{aligned} r_0 &= 1 \\ r_1 &= 10r_0 - q_1 p \\ &\vdots \\ r_k &= 10r_{k-1} - q_k p. \end{aligned}$$

On a donc $r_k \equiv 10^k \mod p$ et si on note k_0 l'indice à partir duquel le développement est périodique de période T, on a $q_{k_0+T} = q_k$ avec $r_{k_0+T} = r_k$ et donc $10^{k_0+T} \equiv 10^{k_0} \mod p$ soit $10^T \equiv 1 \mod p$. On en déduit que $r_0 = r_T$ et donc $q_1 = q_{T+1}$, i.e. le développement est périodique dès le premier chiffre après la virgule. Notons alors $d|T$ l'ordre de 10 modulo p ; comme précédemment on a $r_{k+d} = r_k$ pour tout $k > 0$ et donc $q_{k+d} = q_k$ et donc $T|d$ d'où le résultat. □

Exemples $\frac{1}{13} = 0,076923\cdots$ et 10 est d'ordre 6 dans $(\mathbb{Z}/13\mathbb{Z})^\times$.

Remarque : le même raisonnement s'applique pour les $\frac{k}{p}$ avec $1 \leq k \leq p-1$.

Corollaire 4.1.2. — *Soit T la période du développement décimal de $\frac{1}{p} = 0, a_1 a_2 \cdots, a_T\, a_1 \cdots$ et notons $n = \sum_{i=1}^{d} a_i 10^{T-i}$. On a alors*

$$np = 10^T - 1.$$

Preuve : On a l'égalité

$$\frac{1}{p} = \sum_{i=1}^{+\infty} n 10^{-iT} = \frac{10^{-T} n}{1 - 10^{-T}} = \frac{n}{10^T - 1}$$

et donc $np = 10^T - 1$. □

Remarque : pour retrouver l'entier n associé à $p = 7$, on peut partir de l'égalité $999999 = 7n$ soit classiquement par division $999999 = 7 \times 100000 + 299999$... soit au contraire en partant de droite : $999999 = 7 \times 7 + 999950$... C'est comme cela par exemple que l'on trouve aisément le $p-1$-ème chiffre du développement décimal de $1/p$.

Remarque : comme $10^{p-1} - 1$ s'écrit avec un nombre pair de 9, l'entier pn est divisible par 99 et donc pour $p \neq 3, 11$, n est divisible par 99 ainsi donc que la somme de ses paquets de 2 chiffres ($100 \equiv 1 \mod 99$). Si $3|p-1$ alors n est divisible par 999 ainsi donc que la somme de ses paquets de 3 chiffres ($1000 \equiv 1 \mod 999$). Dans le même genre d'idée, on a le résultat suivant.

Proposition 4.1.3. — *Soit $d = 2e$ un multiple de l'ordre T de 10 dans $(\mathbb{Z}/p\mathbb{Z})^\times$ tel que e n'est pas un multiple de T. Pour*

$$A = \sum_{i=1}^{e} a_i 10^{e-i}, \qquad B = \sum_{i=1}^{e} a_{e+i} 10^{e-i}.$$

on a alors $A + B = 10^e - 1$.

Preuve : On a $n = 10^e A + B$ avec $0 \leq A, B < 10^e - 1$ car $p > 1$. Ainsi on a

$$\frac{10^{2e}}{p} = 10^e A + B + \frac{1}{p} \Rightarrow \frac{10^e + 1}{p} \times (10^e - 1) = 10^e A + B$$

. Or comme $(10^e)^2 \equiv 1 \mod p$ et que $10^e \not\equiv 1 \mod p$, on en déduit que $10^e + 1 \equiv 0 \mod p$ de sorte que $A + B \equiv 0 \mod 10^e - 1$ et le résultat découle de l'encadrement $1 \leq A + B < 2(10^e - 1)$. □
Remarque : dans le cas où T est divisible par r, le raisonnement précédent donne que la somme des paquets de T/r chiffres de n est de la forme $k(10^r - 1)$ avec $1 \leq k < r$.
Exemples $\frac{1}{19} = 0,052631578947368421\cdots$ et on a

$$052+631+578+947+368+421 = 3\times 999 \quad 05+26+31+57+89+47+36+84+21 = 4\times 99.$$

Proposition 4.1.4. — *Soit p premier tel que la période de son développement décimal soit égale à* $p-1$ *; le nombre dn s'obtient alors à partir de n par permutation circulaire.*

Par exemple : pour $p = 7$, on a

$$\begin{aligned} 2 \times 142857 &= 285714 \\ 3 \times 142857 &= 428571 \\ 4 \times 142857 &= 571428 \\ 5 \times 142857 &= 714285 \\ 6 \times 142857 &= 857142 \end{aligned}$$

Preuve : On reprend les notations de la proposition 4.1.1 : comme $T = p - 1$ on en déduit que $\{r_1, \cdots, r_{p-1}\} = \{1, \cdots, p-1\}$. En notant $1 \leq i_0 \leq p-1$ l'indice tel que $r_{i_0} = k$, on en déduit du calcul même du développement décimal que le i-ème chiffre b_i du développement décimal de k/p est égal à $i + i_0$, d'où le résultat. □
Remarque : une autre façon d'énoncer le résultat précédent est de dire que le n_k du développement décimal de k/p s'obtient par permutation circulaire de n en utilisant, avec les notations de la proposition 4.1.1 le premier reste $r_i = k$. Dans le cas général où la période est égale à T un diviseur quelconque de $p-1$, les restes des divisions euclidiennes des k/p pour k décrivant $\{1, \cdots, p-1\}$ se répartissent en $(p-1)/T$ sous-ensembles de sorte que les kn pour k décrivant $\{1, \ldots, p-1\}$, à permutations circulaires près, sont en nombre $(p-1)/T$.

Théorème 4.1.5. — *Soit* $p > 11$ *premier alors* $a_{(p+1)/2} = 0$ *si et seulement si* $(\frac{10}{p}) = 1$ *et sinon elle est égale à* 9.

Preuve : On écrit $A = \sum_{i=1}^{(p-1)/2} a_i 10^{(p-1)/2-i}$ et $B = \sum_{i=1}^{(p-1)/2} a_{(p-1)/2+i} 10^{(p-1)/2-i}$ de sorte que d'après 4.1.3 soit $A = B$ soit $A + B = 9\cdots 9$. Dans le premier cas comme $a_1 = 0$, on en déduit que $a_{(p+1)/2} = 0$ et dans le deuxième on obtient 9. Il faut alors décider si $(p-1)/2$ est un multiple d'une période, i.e. si $10^{(p-1)/2} \equiv 1 \mod 2$ ce qui est équivalent à $(\frac{10}{p}) = 1$ d'où le résultat. □
Remarque : d'après la loi de réciprocité quadratique, le résultat ne dépend que de la congruence de p modulo 40. Dans le même ordre d'idée, on peut facilement déterminer le $(p-1)/2$-chiffres du développement décimal de $1/p$: en effet si $(p-1)/2$ est le multiple d'une période alors ce chiffre est le même que le $p-1$-ème que l'on détermine facilement comme expliqué ci-avant. Dans le cas où $(p-1)/2$ n'est pas une période comme avec les notations ci-dessus, $A + B = 9\cdots 9$, on en déduit que le chiffre cherché est égal à 9 moins le $(p-1)$-ème chiffre.

Notons alors $\mathcal{P}(10)$ l'ensemble des premiers p tels que leur développement décimal est de période $p-1$: cet ensemble est-il infini et si oui quel est sa densité

$$d_{10}(x) = \frac{\sharp\{p \in \mathcal{P}(10),\ p \leq x\}}{\sharp\{p \in \mathcal{P},\ p \leq x\}}, \qquad \lim_{x\to+\infty} d_{10}(x).$$

On conjecture que cette limite est égale à

$$C_{Artin} = \prod_{p\in\mathcal{P}}\Big(1 - \frac{1}{p(p-1)}\Big) \simeq 0,3739558136\cdots$$

Le choix de la base 10 ne semble pas intervenir dans le résultat, on conjecture que le résultat doit être vrai pour tout choix d'entier a en lieu et place de 10.

4.2. en cryptographie. — Il s'agit d'un système dit à clef publique, i.e. tout le monde connaît le procédé de cryptage mais seul une personne (le receveur) connaît la clef qui permet de déchiffrer. Concrètement on choisit deux nombres premiers p et q distincts impairs très grands (plus quelques autres contraintes) et on pose $n = pq$; on fixe aussi $0 \leq c < n$ un entier premier avec $\varphi(n)$. Sont publiques les entiers n et c ainsi que le procédé suivant. Si A veut envoyer un message à R, il le coupe d'abord en bouts et les transforme en des nombre m_i plus petit que n ; ensuite il envoie les m_i^c modulo n.

Le problème pour R ou pour B indiscret est de retrouver m connaissant n et c et sachant que $n = pq$ avec p, q premiers connus seulement de R. Pour R la méthode est assez simple, il lui suffit de connaître l'inverse e de c dans $(\mathbb{Z}/n\mathbb{Z})^\times$; en effet on a alors $(m^c)^e \equiv m \mod n$. Pour calculer e, R utilise le théorème chinois et calcule donc les inverses e_p et e_q de c dans respectivement $(\mathbb{Z}/p\mathbb{Z})^\times$ et $(\mathbb{Z}/q\mathbb{Z})^\times$ qui est d'après le petit théorème de Fermat égal à c^{p-2} et c^{q-2}. On construit alors facilement e en utilisant la version constructive du théorème chinois. Pour B, la situation est plus critique ; pour l'instant sa stratégie est de casser n, i.e. de trouver p ce qui est très long pourvu que R ait choisi p et q très grand convenablement. A ce propos signalons les précautions élémentaires à prendre :

- p et q doivent être pris tous deux grands, sinon l'algorithme ρ de Pollard pourrait très facilement trouver le petit facteur ;
- il faut que $|p - q|$ soit grand sinon pour $q = p + \delta$ avec δ beaucoup plus petit que p, on aurait pour $N = pq$,$\sqrt{N} = p\sqrt{1+\delta} \sim p + \delta/2$ et on pourra trouver p par un algorithme naïf en $O(\delta)$ étapes ;
- il faut que $p - 1$ et $q - 1$ ne soit pas trop friable au sens précédent, sinon l'algorithme $p - 1$ de Pollard permettrait de le trouver rapidement ;
- il faut que l'exposant secret e ne soit pas trop petit ; trivialement si $e = O(\log N)$ alors en faisant $O(\log N)$ essais on trouvera e. En fait on peut montrer qu'il faut éviter $e << N^{1/4}$.

Il existe sûrement d'autres contraintes connues ou pas sur les choix de p, q, e. Signalons tout de même que la construction de grands nombres premiers ne posent pas de problèmes pratiques : pour cela on part d'un entier impair k grand, on test en temps polynomial s'il est premier et sinon on teste $k + 2$ et ainsi de suite. Le théorème des nombres premiers nous dit qu'en moyenne on devrait tomber sur un nombre premier au bout de $\ln k$ étapes. Si la conjecture sur la fonction trou, comme quoi $g(p_n) \leq K(\ln p_n)^2$ est vrai, on est assuré de trouver ainsi un nombre premier en temps polynomial.

4.3. en algèbre. — Il s'agit de développer quelques thèmes en algèbre dans lesquels l'utilisation des nombres premiers intervient.

4.3.1 — Théorie des corps : soit K un corps, l'application $n \in \mathbb{Z} \mapsto n.1_K \in K$ a pour noyau $p\mathbb{Z}$ avec soit $p = 0$ soit p premier. Cet entier est appelé la caractéristique de K. Si K est fini, il est alors commutatif de cardinal une puissance de p. Dans ce cas, le groupe de Galois de $K/\mathbb{F}_p$ est engendré par le morphisme dit de Frobenius : $x \mapsto x^p$. On rappelle que le symbole de Legendre $(\frac{n}{p})$ est 0 si $p|n$ et 1 (resp. -1) si $p \wedge n = 1$ et si n est un carré modulo p (resp.

sinon). On vérifie alors que pour $n \wedge p = 1$, on a $(\frac{n}{p}) \equiv n^{(p-1)/2} \mod p$. Par ailleurs le symbole de Legendre qui est clairement multiplicatif peut se calculer aisément en utilisant la loi de réciprocité quadratique.

Théorème 4.3.2. — *Pour tout p, q premiers distincts, on a*

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

et $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Preuve : L'idée est d'utiliser la relation

$$\mathrm{Res}(P, Q) = (-1)^{\deg P . \deg Q} \mathrm{Res}(Q, P)$$

et de choisir des polynômes P et Q de degré respectifs $\frac{p-1}{2}$ et $\frac{q-1}{2}$, où p et q sont des premiers impairs distincts, de sorte que

$$\mathrm{Res}(P, Q) = (\frac{p}{q}) \text{ et } \mathrm{Res}(Q, P) = (\frac{q}{p}).$$

Lemme 4.3.3. — *Pour tout p premier impair, il existe un polynôme $Q_p \in \mathbb{Z}[X]$ tel que*

$$X^{p-1} + X^{p-2} + \cdots + X + 1 = X^{(p-1)/2} Q_p(X + \frac{1}{X}).$$

Preuve : En posant $Y = X^{-1}$, le membre de gauche est égal à $X^{(p-1)/2} + \cdots + X + 1 + Y + \cdots + Y^{(p-1)/2}$, de sorte que d'après le théorème sur les polynômes symétriques, il existe $R \in \mathbb{Z}[X, Y]$ tel que le terme précédent est égal à $R(X + Y, XY)$, d'où le résultat en notant que $XY = 1$. □

Lemme 4.3.4. — *Pour $p \neq q$ des nombres premiers impairs, le résultant de Q_p et Q_q est égal à ± 1.*

Preuve : Raisonnons par l'absurde et considérons l premier divisant $\mathrm{Res}(Q_p, Q_q)$ de sorte que modulo l, $\bar{Q}_p$ et $\bar{Q}_q$ ont une racine commune $\beta \in \mathbb{F}_{l^n}$ pour $2n \leq \min\{p-1, q-1\}$. Soit alors $x \in \bar{\mathbb{F}}_l$ tel que $x^2 - \beta x + 1 = 0$ de sorte que

$$x^{p-1} + \cdots + x + 1 = x^{(p-1)/2} \bar{Q}_p(\beta) = 0.$$

En multipliant cette égalité par $x - 1$, on en déduit que $x^p = 1$ dans $\bar{\mathbb{F}}_l$. De la même façon on a aussi $x^q = 1$ et comme $p \wedge q = 1$, on en déduit $x = 1$ et donc $p \equiv q \equiv 0 \mod l$ ce qui n'est pas car $p \wedge q = 1$. □

Proposition 4.3.5. — *Pour $p \neq q$ des nombres premiers distincts, on a*

$$\mathrm{Res}(Q_p, Q_q) = (\frac{q}{p}).$$

Preuve : On raisonne modulo p de sorte que d'après le lemme précédent, il suffit de prouver que ce résultant est $\equiv q^{(p-1)/2} \mod p$:

$$X^{p-1} + \cdots + X + 1 \equiv (X-1)^{p-1} \equiv (X^2 - 2X + 1)^{(p-1)/2} \equiv X^{(p-1)/2} (X + \frac{1}{X} - 2)^{(p-1)/2} \mod p,$$

de sorte que $Q_p(X + \frac{1}{X}) \equiv (X + \frac{1}{X} - 2)^{(p-1)/2} \mod p$ et donc

$$Q_p(X) \equiv (X - 2)^{(p-1)/2} \mod p.$$

Ainsi on en déduit que $\mathrm{Res}(Q_p, Q_q) \equiv Q_p(2)^{(p-1)/2} \equiv Q_q(1+\frac{1}{1})^{(p-1)/2} \equiv q^{(p-1)/2} \mod p$, d'où le résultat. □

□

4.3.6 — Théorie des groupes : étant donné un groupe fini G de cardinal n, on peut se demander si la décomposition en facteurs premiers de n permet de le décomposer. Si G est abélien alors G est le produit direct de se parties primaires, i.e. $G \simeq \prod_p G_p$ où G_p est un p-groupe ; par ailleurs G_p peut s'écrire de manière unique comme un produit de groupe cyclique. Dans le cas non commutatif, le théorème de Sylow donne l'existence d'un p-groupe de Sylow mais en général G n'est pas le produit direct de ses groupes de Sylow sauf si pour tout p, il existe un unique groupe de p-Sylow.

En ce qui concerne l'ordre des éléments, bien évidemment si G n'est pas cyclique il n'existe pas d'éléments d'ordre n. Par contre pour tout p premier divisant n, le théorème de Cauchy montre qu'il existe un élément d'ordre p ; le résultat ne tient toujours pas pour p^r : considérer par exemple $(\mathbb{Z}/2\mathbb{Z})^2$.

4.3.7 — Polynômes : le critère d'Eisenstein est un moyen simple de construire un polynôme irréductible de degré n donné. Pour cela on prend $a_0 \equiv a_1 \equiv \cdots \equiv a_{n-1} \equiv 0 \mod p$ et a_n, a_0/p non divisible par p de sorte que $P(X) = a_n X^n + \cdots + a_0$ est irréductible sur $\mathbb{Z}$: c'est un cas particulier du théorème de Lucas.

Remarque : une façon de le démontrer est de considérer la réduction modulo p de $P(X)$. Plus généralement si la réduction modulo p d'un polynôme $Q(X)$ est irréductible alors $Q(X)$ l'est aussi sur $\mathbb{Z}$: malheureusement cette technique n'est pas très efficace. En effet si n est tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique, alors la réduction modulo p du polynôme irréductible Φ_n dit cyclotomique, n'est pas irréductible car le degré d'un quelconque de ses facteurs irréductibles est égal à l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$ qui ne peut donc jamais égaler $\psi(n)$.

5. Développements

- pot pourri autour de l'infinité de l'ensemble des nombres premiers ;
- nombres de Fermat et Mersenne : tests de primalité effectifs ;
- formules donnant les nombres premiers : L, $t(n)$, $f(n)$ via le théorème de Wilson
- Cas particuliers du théorème de Dirichlet ;
- théorème de Tchebychef et application au postulat de Bertrand ;
- développement décimal de $1/p$;

6. Questions

Exercice 6.1. — *Soit $n \geq 2$; montrez que si $k^2 + k + n$ est premier pour tout entier $0 \leq k \leq \sqrt{n/3}$ alors c'est encore vrai pour tout entier $0 \leq k \leq n-2$.*

Remarque : on peut montrer que les seules valeurs n telles que la condition de l'énoncé est vérifiée sont $2, 3, 5, 16$ et 41 ; on peut montrer que cette condition est équivalent à demander que $\mathbb{Z}[\sqrt{1-4n}]$ est factoriel, résultat prouvé par Heegner en 1952 alors qu'il était professeur de lycée à Berlin. Par ailleurs le lecteur notera que si on numérote les entiers en spirale autour de n, les nombres $k^2 + k + n$ sont sur la diagonale $y = x$: spirales d'Ulam.

Exercice 6.2. — *Soit $n > 1$ un entier ; on pose $A = 1 + \sum_{k=1}^{n-1} k^{n-1}$.*

(i) Soit $n = pt$ avec p premier, montrez que $A \equiv 1 + tS \mod p$, où $S = \sum_{k=1}^{p-1} k^{t-1}$.

(ii) En déduire que $A \equiv 0 \mod p$ *si et seulement si* $p-1|t-1$ *et* $p|t-1$.
(iii) Montrez que si $n>1$ *est tel que* $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \mod n$ *alors pour tout* p *premier divisant* n, *on a* $p^2(p-1)$ *divise* $n-p$.
(iv) Sous les hypothèses de (iii) montrez que $p-1$ *divise* $n-1$.

Exercice 6.3. — *Soit* $p>3$ *un nombre premier.*
(i) Montrez que dans $\mathbb{Z}/p\mathbb{Z}$ *on a* $\sum_{i=1}^{p-1} \frac{1}{i} = 0$.
(ii) Pour $1 \leq k < p$, *on note* k' *l'inverse de l'image de* k *dans* $\mathbb{Z}/p^2\mathbb{Z}$. *Montrez que* $\sum_{k=1}^{p-1} k' = 0 \in \mathbb{Z}/p^2\mathbb{Z}$ *est équivalent au fait que le numérateur de la fraction* $\sum_{k=1}^{p-1} \frac{1}{k}$ *est divisible par* p^2.
(iii) En utilisant le polynôme $\prod_{k=1}^{p-1}(X-k)$ *montrez que* p^2 *divise l'entier* $(p-1)!\sum_{k=1}^{p-1} \frac{1}{k}$.
(iv) En déduire le théorème de Wolstenholme à savoir p^2 *divise le numérateur de la fraction* $\sum_{k=1}^{p-1} \frac{1}{k}$.
(v) Montrez que le numérateur de la fraction $C_p = \sum_{k=1}^{p-1} \frac{1}{k^2}$ *est divisible par* p.

Exercice 6.4. — *En utilisant le théorème des nombres premiers* $\pi(x) \sim \frac{x}{\ln x}$, *donnez des équivalents quand* N *et* x *tendent vers l'infini de :*

$$p_N, \quad \sum_{n=1}^{N} p_n, \quad \sum_{p\leq x} p, \quad \sum_{p\leq x} \ln p, \quad \sum_{p\leq x} p^{-1}, \quad \sum_{p\leq x} \frac{\ln p}{p}$$

où p_n *désigne le* n*-ième nombre premier. On désigne par* d_n *le ppcm des entiers* $1, 2, 3, \cdots, n$ *: vérifiez que* $\ln d_n \sim n$ *pour* $n \to \infty$.

Exercice 6.5. — *Soient* $a_1, a_2, \cdots, a_m$ *et* $b_1, \cdots, b_n$ *des chiffres (*$0 \leq a_i, b_j \leq 9$*) tels que* $b_n = 1, 3, 7, 9$. *Montrez qu'il existe une infinité de nombres premiers* p *tels que leur écriture en base* 10 *commence par les* a_i *et finisse par les* b_j.

7. Solutions

6.1 Raisonnons par l'absurde et supposons qu'il existe $\sqrt{n/3} \leq l \leq n-2$ tel que l^2+l+n ne soit pas premier ; on prend l minimal. Soit alors q le plus petit diviseur premier de l^2+l+n ; on a $q \leq 2l$ car sinon on aurait $(2l+1)^2 \leq q^2 \leq l^2+l+n$ et donc $l \leq \sqrt{n/3}$. On écrit alors q sous la forme $l-k$ ou $l+k+1$ avec $0 \leq k \leq l-1$; de la factorisation

$$(l^2+l+n) - (k^2+k+n) = (l-k)(l+k+1)$$

on en déduit que q divise k^2+k+n lequel par minimalité de l est premier soit $q = k^2+k+n$. La relation $q^2 \leq l^2+l+n$ implique

$$(k^2+k+n)^2 \leq (n-2)^2 + (n-2) + n < n^2$$

ce qui est absurde.

6.2 (i) On écrit $pt-1 = (p-1)t + (t-1)$ de sorte que d'après le petit théorème de Fermat $k^{pt-1} \equiv k^{t-1} \mod p$ et $k^{t-1} \equiv (k+\lambda p)^{t-1} \mod p$ ce qui donne le résultat.

(ii) D'après (i) on a $A \equiv 1 \mod p$ si $p-1$ ne divise pas $t-1$ et sinon $A \equiv 1-t \mod p$.

(iii) Le résultat découle directement de (ii) en utilisant que pour $n = pt$ avec p premier, la condition $p^2(p-1)$ divise $pt-p$ est équivalente aux deux conditions $p|t-1$ et $p-1|t-1$.

(iv) De (iii), on en déduit que $n \equiv p \equiv 1 \mod p-1$ ce qui donne le résultat.

6.3 (i) On remarque que $i(\frac{1}{i}+\frac{1}{p-i}) = 1-1 = 0 \in \mathbb{Z}/p\mathbb{Z}$ et donc $\frac{1}{i}+\frac{1}{p-i} = 0$ de sorte qu'en regroupant les termes deux par deux on obtient le résultat.

(ii) On a $k(p-1)! = kk'\frac{(p-1)!}{k'} = \frac{(p-1)!}{k'}$ de sorte que

$$(p-1)!(1+2+\cdots+p-1) \equiv (p-1)!\sum_{k=1}^{p-1} k' \in \mathbb{Z}/p^2\mathbb{Z},$$

ce qui donne le résultat en remarquant que $(p-1)!$ est inversible modulo p^2.

(iii) On a $\prod_{k=1}^{p-1}(X-k) = X^{p-1} - \sigma_1 X^{p-2} + \cdots - \sigma_{p-2}X + \sigma_1$ ce qui pour $X = p$ donne $(p-1)! = p^{p-1} - \sigma_1 p^{p-2} + \cdots - \sigma_{p-2}p + (p-1)!$ et donc

$$p^{p-2} - \sigma_1 p^{p-3} + \cdots - \sigma_{p-2} = 0.$$

En particulier on en déduit que $p|\sigma_k$ pour tout $k = 1, \cdots, p-2$ et donc $p^2|\sigma_{p-2}$ avec $\sigma_{p-2} = (p-1)!\sum_{k=1}^{p-1}\frac{1}{k}$, d'où le résultat.

(iv) Cela découle directement de (ii) et (iii).

(v) Le résultat découle directement de ce qui précède en remarquant que le numérateur de C_p est égal à $\sigma_{p-2}^2 - 2\sigma_{p-1}\sigma_{p-3}$.

6.4

6.5