Théorème de la progression arithmétique et théorème de Tchebotarev

Alexandre Bailleul

École normale supérieure de Rennes

3 février 2017

Sommaire

Plan

Un peu d'histoire

Soient $p_1, \ldots, p_r$ des nombres premiers. Les facteurs premiers de

$$N = \prod_{i=1}^{r} p_i + 1$$

ne peuvent être parmi les p_i.

Un peu d'histoire

Soient $p_1, \ldots, p_r$ des nombres premiers. Les facteurs premiers de

$$N = \prod_{i=1}^{r} p_i + 1$$

ne peuvent être parmi les p_i.

Par conséquent, il existe une infinité de nombres premiers !

Un peu d'histoire

On peut faire un peu mieux. On prend $p_1, \ldots, p_r$ des nombres premiers congrus à 5 modulo 6.

Un peu d'histoire

On peut faire un peu mieux. On prend $p_1, \ldots, p_r$ des nombres premiers congrus à 5 modulo 6.

Alors les facteurs premiers de

$$N = 6 \prod_{i=1}^{r} p_i - 1$$

ne peuvent être ni 2, ni parmi les p_i, et l'un d'eux est congru à 5 modulo 6 (sinon on aurait $N = 1[6]$).

Un peu d'histoire

On peut faire un peu mieux. On prend $p_1, \ldots, p_r$ des nombres premiers congrus à 5 modulo 6.

Alors les facteurs premiers de

$$N = 6 \prod_{i=1}^{r} p_i - 1$$

ne peuvent être ni 2, ni parmi les p_i, et l'un d'eux est congru à 5 modulo 6 (sinon on aurait $N = 1[6]$).

Donc il existe une infinité de nombres premiers $p = 5[6]$.

Un peu d'histoire

Un dernier ? Soient $p_1, \ldots, p_r$ des nombres premiers congrus à 1 modulo 4.

Un peu d'histoire

Un dernier ? Soient $p_1, \ldots, p_r$ des nombres premiers congrus à 1 modulo 4.

Alors les facteurs premiers de

$$N = 4 \prod_{i=1}^{r} p_i^2 + 1$$

ne sont ni 2, ni l'un des p_i et sont congrus à 1 modulo 4, car -1 est un carré modulo N.

Un peu d'histoire

Un dernier ? Soient $p_1, \ldots, p_r$ des nombres premiers congrus à 1 modulo 4.

Alors les facteurs premiers de

$$N = 4 \prod_{i=1}^{r} p_i^2 + 1$$

ne sont ni 2, ni l'un des p_i et sont congrus à 1 modulo 4, car -1 est un carré modulo N.

Et donc il existe une infinité de nombres premiers $p = 1[4]$.

Un peu d'histoire

En l'absence d'obstruction évidente*, il semble exister une infinité de nombres premiers dans la progression arithmétique $\{q \in \mathbb{Z}, q = a[m]\} = \{a + km, k \in \mathbb{Z}\}$.

Un peu d'histoire

En l'absence d'obstruction évidente*, il semble exister une infinité de nombres premiers dans la progression arithmétique $\{q \in \mathbb{Z}, q = a[m]\} = \{a + km, k \in \mathbb{Z}\}$.

En fait on a le

Théorème (de Dirichlet, 1838)

Soient a et m deux entiers premiers entre eux. Alors il existe une infinité de nombres premiers de la forme $a + mn$, $n \in \mathbb{N}$.

La démonstration de Dirichlet

On fixe $m \in \mathbb{N}^*$. On va commencer par montrer le résultat pour $a = 1$.

La démonstration de Dirichlet

On fixe $m \in \mathbb{N}^*$. On va commencer par montrer le résultat pour $a = 1$.

Dirichlet introduit ses fameux caractères : les morphismes de groupes $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^*$.

La démonstration de Dirichlet

On fixe $m \in \mathbb{N}^*$. On va commencer par montrer le résultat pour $a = 1$.

Dirichlet introduit ses fameux caractères : les morphismes de groupes $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^*$.

Exemples : le caractère principal χ_0 qui prend uniquement la valeur 1, ou encore le symbole de Jacobi $\left(\frac{\cdot}{m}\right)$, d'ordre 2.

La démonstration de Dirichlet

Rappelons que

$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}.$$

La démonstration de Dirichlet

Rappelons que

$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}.$$

Donc il y a $\varphi(m)$ caractères modulo m, et on a les relations d'orthogonalité

$$\sum_{g\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(g) = \begin{cases} \varphi(m) \text{ si } \chi = \chi_0 \\ 0 \text{ sinon} \end{cases}$$

et

$$\sum_{\chi} \chi(g) = \begin{cases} \varphi(m) \text{ si } g = 1 \\ 0 \text{ sinon.} \end{cases}$$

La démonstration de Dirichlet

On étend tous ces caractères à $\mathbb{Z}$, en décrétant que $\chi(n) = 0$ si $(m, n) \neq 1$. Par exemple

$$\chi_0(n) = \begin{cases} 1 \text{ si } (m,n) = 1 \\ 0 \text{ sinon.} \end{cases}$$

La démonstration de Dirichlet

On étend tous ces caractères à $\mathbb{Z}$, en décrétant que $\chi(n) = 0$ si $(m, n) \neq 1$. Par exemple

$$\chi_0(n) = \begin{cases} 1 \text{ si } (m,n) = 1 \\ 0 \text{ sinon.} \end{cases}$$

On introduit alors les fameuses séries L de Dirichlet :

$$L(\chi, s) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}.$$

La démonstration de Dirichlet

On étend tous ces caractères à $\mathbb{Z}$, en décrétant que $\chi(n) = 0$ si $(m, n) \neq 1$. Par exemple

$$\chi_0(n) = \begin{cases} 1 \text{ si } (m,n) = 1 \\ 0 \text{ sinon.} \end{cases}$$

On introduit alors les fameuses séries L de Dirichlet :

$$L(\chi, s) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}.$$

Proposition

Si $\chi \neq \chi_0$, la fonction $L(\chi, .)$ est holomorphe sur $\{s \in \mathbb{C}, Re(s) > 0\}$ et $L(\chi_0, .)$ est holomorphe sur $\{s \in \mathbb{C}, Re(s) > 1\}$.

La démonstration de Dirichlet

On étend tous ces caractères à $\mathbb{Z}$, en décrétant que $\chi(n) = 0$ si $(m, n) \neq 1$. Par exemple

$$\chi_0(n) = \begin{cases} 1 \text{ si } (m,n) = 1 \\ 0 \text{ sinon.} \end{cases}$$

On introduit alors les fameuses séries L de Dirichlet :

$$L(\chi, s) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}.$$

Proposition

Si $\chi \neq \chi_0$, la fonction $L(\chi, .)$ est holomorphe sur $\{s \in \mathbb{C}, Re(s) > 0\}$ et $L(\chi_0, .)$ est holomorphe sur $\{s \in \mathbb{C}, Re(s) > 1\}$.

Proposition (Produits eulériens)

Pour $Re(s) > 1$ et χ un caractère, on a

$$L(\chi, s) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

La démonstration de Dirichlet

Les choses se mettent en place ! Des développements en produits eulériens, on déduit que

$$L(\chi_0, s) = \prod_{p \not| m} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right)$$

d'où $L(\chi_0, .)$ se prolonge en une fonction méromorphe sur $\mathbb{C}$ avec un unique pôle (simple) en 1,

La démonstration de Dirichlet

Les choses se mettent en place ! Des développements en produits eulériens, on déduit que

$$L(\chi_0, s) = \prod_{p \not| m} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right)$$

d'où $L(\chi_0, .)$ se prolonge en une fonction méromorphe sur $\mathbb{C}$ avec un unique pôle (simple) en 1, et que

$$\log(L(\chi, s)) = \sum_p \frac{\chi(p)}{p^s} + O(1)$$

pour $\mathrm{Re}(s) > 1$ et tout caractère χ.

La démonstration de Dirichlet

En sommant, on trouve

$$\sum_{\chi} \log(L(\chi, s)) = \sum_{p} \frac{1}{p^s} \sum_{\chi} \chi(p) + O(1),$$

et la magie opère :

La démonstration de Dirichlet

En sommant, on trouve

$$\sum_{\chi} \log(L(\chi, s)) = \sum_{p} \frac{1}{p^s} \sum_{\chi} \chi(p) + O(1),$$

et la magie opère :

$$\sum_{\chi} \log(L(\chi, s)) = \varphi(m) \sum_{p=1 \bmod m} \frac{1}{p^s} + O(1).$$

La démonstration de Dirichlet

En sommant, on trouve

$$\sum_{\chi} \log(L(\chi, s)) = \sum_{p} \frac{1}{p^s} \sum_{\chi} \chi(p) + O(1),$$

et la magie opère :

$$\sum_{\chi} \log(L(\chi, s)) = \varphi(m) \sum_{p=1 \bmod m} \frac{1}{p^s} + O(1).$$

Si la quantité à gauche tend vers $+\infty$ quand $s \to 1$, celle de droite aussi, et il existe donc une infinité de nombres premiers $p = 1 \bmod m$!

La démonstration de Dirichlet

Mais comme

$$\sum_{\chi} \log(L(\chi, s)) = \log\left(\prod_{\chi} L(\chi, s)\right),$$

il suffit de montrer que les $L(\chi, .)$ pour $\chi \neq \chi_0$ ne s'annulent pas en 1 (c'est-à-dire ne compensent pas le pôle de $L(\chi_0, .)$).

La démonstration de Dirichlet

Mais comme

$$\sum_{\chi} \log(L(\chi, s)) = \log\left(\prod_{\chi} L(\chi, s)\right),$$

il suffit de montrer que les $L(\chi, .)$ pour $\chi \neq \chi_0$ ne s'annulent pas en 1 (c'est-à-dire ne compensent pas le pôle de $L(\chi_0, .)$).

C'est de loin l'étape la plus dure...

La démonstration de Dirichlet

Mais comme

$$\sum_{\chi} \log(L(\chi, s)) = \log\left(\prod_{\chi} L(\chi, s)\right),$$

il suffit de montrer que les $L(\chi, .)$ pour $\chi \neq \chi_0$ ne s'annulent pas en 1 (c'est-à-dire ne compensent pas le pôle de $L(\chi_0, .)$).

C'est de loin l'étape la plus dure...

Au final on obtient le théorème de Dirichlet pour $a = 1$, et le cas général se démontre de manière similaire en considérant

$$\sum_{\chi} \overline{\chi(a)} \log(L(\chi, s)) = \varphi(m) \sum_{p = a \bmod m} \frac{1}{p^s} + O(1).$$

Plan

Un peu de théorie algébrique des nombres

Un corps de nombres K est une extension finie (donc algébrique) de $\mathbb{Q}$.

Un peu de théorie algébrique des nombres

Un corps de nombres K est une extension finie (donc algébrique) de $\mathbb{Q}$.

L'anneau des entiers de K est $\mathcal{O}_K = \{x \in K, x \text{ est entier sur } \mathbb{Z}\}$. C'est un anneau de Dedekind :

Un peu de théorie algébrique des nombres

Un corps de nombres K est une extension finie (donc algébrique) de $\mathbb{Q}$.

L'anneau des entiers de K est $\mathcal{O}_K = \{x \in K, x \text{ est entier sur } \mathbb{Z}\}$. C'est un anneau de Dedekind :

Théorème ("Théorème fondamental de l'arithmétique pour les idéaux")

Tout idéal non nul $I \subset \mathcal{O}_K$ se décompose de manière unique (à l'ordre près) sous la forme

$$I = \prod_{i=1}^{r} \mathcal{P}_i^{e_i}$$

où les $\mathcal{P}_i$ sont des idéaux premiers.

Un peu de théorie algébrique des nombres

On suppose maintenant $K/\mathbb{Q}$ galoisienne, et $I = p\mathcal{O}_K$ avec p un nombre premier.

Un peu de théorie algébrique des nombres

On suppose maintenant $K/\mathbb{Q}$ galoisienne, et $I = p\mathcal{O}_K$ avec p un nombre premier. Alors $Gal(K/\mathbb{Q})$ agit transitivement sur les idéaux $\mathcal{P}_i$ au-dessus de I et les exposants e_i sont tous les mêmes.

Un peu de théorie algébrique des nombres

On suppose maintenant $K/\mathbb{Q}$ galoisienne, et $I = p\mathcal{O}_K$ avec p un nombre premier. Alors $Gal(K/\mathbb{Q})$ agit transitivement sur les idéaux $\mathcal{P}_i$ au-dessus de I et les exposants e_i sont tous les mêmes.

Exemples : $(2) = (2+\sqrt{6})^2$ dans $\mathcal{O}_{\mathbb{Q}(\sqrt{6})} = \mathbb{Z}[\sqrt{6}]$.

Un peu de théorie algébrique des nombres

On suppose maintenant $K/\mathbb{Q}$ galoisienne, et $I = p\mathcal{O}_K$ avec p un nombre premier. Alors $Gal(K/\mathbb{Q})$ agit transitivement sur les idéaux $\mathcal{P}_i$ au-dessus de I et les exposants e_i sont tous les mêmes.

Exemples : $(2) = (2+\sqrt{6})^2$ dans $\mathcal{O}_{\mathbb{Q}(\sqrt{6})} = \mathbb{Z}[\sqrt{6}]$.
$(p) = (1-\zeta_p)^{p-1}$ dans $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$. ($p$ nombre premier, ζ_p racine p-ième de l'unité)

Un peu de théorie algébrique des nombres

Si de plus p est non ramifié* dans K, alors chaque $\mathcal{P} \mid p$ induit un élément de $Gal(K/\mathbb{Q})$, noté $Frob_{\mathcal{P}}$, tel que

$$Frob_{\mathcal{P}}(x) = x^p \bmod \mathcal{P}.$$

Un peu de théorie algébrique des nombres

Si de plus p est non ramifié* dans K, alors chaque $\mathcal{P} \mid p$ induit un élément de $Gal(K/\mathbb{Q})$, noté $Frob_{\mathcal{P}}$, tel que

$$Frob_{\mathcal{P}}(x) = x^p \bmod \mathcal{P}.$$

Ces morphismes sont tous conjugués dans $Gal(K/\mathbb{Q})$. On appelle $Frob_p$ la classe de conjugaison associée (ou encore $(p, K/\mathbb{Q})$, symbole d'Artin).

Le théorème de Tchebotarev

Théorème (Tchebotarev, 1922)

Soit $K/\mathbb{Q}$ corps de nombres galoisien et C une classe de conjugaison de $G = Gal(K/\mathbb{Q})$. Alors

$$\frac{\left|\{p \leq x, p \text{ non ramifié}, Frob_p = C\}\right|}{|\{p \leq x\}|} \underset{x \to +\infty}{\longrightarrow} \frac{|C|}{|G|}.$$

Le théorème de Tchebotarev

Avec le théorème de Tchebotarev, on peut montrer, entre autres, les résultats suivants :

Le théorème de Tchebotarev

Avec le théorème de Tchebotarev, on peut montrer, entre autres, les résultats suivants :

Théorème (Frobenius, 1880)

Soit f un polynôme unitaire à coefficients dans $\mathbb{Z}$ de degré $n \geq 1$. On identifie son groupe de Galois à $G \subset \mathfrak{S}_n$. La densité des nombres premiers p tels que f mod p soit de type $(n_1, \ldots, n_r)$ est égal à $\frac{|T|}{|G|}$ où T est l'ensemble des permutations de type $(n_1, \ldots, n_r)$ dans G.

Le théorème de Tchebotarev

Un autre exemple :

Théorème

Soit f un polynôme unitaire à coefficients dans $\mathbb{Z}$ de degré $n \geq 1$. La densité des nombres premiers tels que f mod p n'admette pas de racine dans $\mathbb{F}_p$ est supérieure à $\frac{1}{n}$.

Le théorème de Tchebotarev

Un autre exemple :

Théorème

Soit f un polynôme unitaire à coefficients dans $\mathbb{Z}$ de degré $n \geq 1$. La densité des nombres premiers tels que f mod p n'admette pas de racine dans $\mathbb{F}_p$ est supérieure à $\frac{1}{n}$.

On peut également s'en servir pour étudier le groupe de Galois de polynômes, ou encore les valeurs premières de formes quadratiques. Mais on peut aussi retrouver le théorème de Dirichlet, de manière plus précise !

Le théorème de Dirichlet revisité

On fixe $m \in \mathbb{N}^*$ et on prend $K = \mathbb{Q}(\zeta_m)$. $K/\mathbb{Q}$ est galoisienne de degré $\varphi(m)$ et de groupe de Galois $G \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ (abélien !).

Le théorème de Dirichlet revisité

On fixe $m \in \mathbb{N}^*$ et on prend $K = \mathbb{Q}(\zeta_m)$. $K/\mathbb{Q}$ est galoisienne de degré $\varphi(m)$ et de groupe de Galois $G \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ (abélien !).

Soit p un nombre premier qui ne divise pas m (équivalent à non ramifié ici). On vérifie facilement qu'en fait
$Frob_p = \sigma_a \in Gal(\mathbb{Q}(\zeta_m), \mathbb{Q})$, où $\sigma_a(\zeta_m) = \zeta_m^p = \zeta_m^a$ avec $p = a \bmod m$.

Le théorème de Dirichlet revisité

On fixe $m \in \mathbb{N}^*$ et on prend $K = \mathbb{Q}(\zeta_m)$. $K/\mathbb{Q}$ est galoisienne de degré $\varphi(m)$ et de groupe de Galois $G \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ (abélien !).

Soit p un nombre premier qui ne divise pas m (équivalent à non ramifié ici). On vérifie facilement qu'en fait
$Frob_p = \sigma_a \in Gal(\mathbb{Q}(\zeta_m), \mathbb{Q})$, où $\sigma_a(\zeta_m) = \zeta_m^p = \zeta_m^a$ avec $p = a \bmod m$.

Il y a donc une correspondance

$$p = a \bmod m \longleftrightarrow Frob_p = \sigma_a \in Gal(\mathbb{Q}(\zeta_m), \mathbb{Q}).$$

Le théorème de Dirichlet revisité

Notons $\pi(x,a,m) = \left|\{p \leq x, p = a[m]\}\right|$ et $\pi(x) = |\{p \leq x\}|$. Le théorème de Tchebotarev nous donne donc le

Théorème (Théorème de la progression arithmétique, version quantitative)

On a

$$\frac{\pi(x,a,m)}{\pi(x)} \underset{x\to+\infty}{\to} \frac{1}{\varphi(m)},$$

et donc l'équivalent

$$\pi(x,a,m) \sim \frac{Li(x)}{\varphi(m)}$$

quand x tend vers $+\infty$.

Merci de votre attention.

Et vive les maths!