

CLAUDE FONDATIONS · COURS

Fonctionnalités, limites et bonnes pratiques

Module 03

5 leçons

LEÇON 01

Les gammes de modèle et la performance

Haiku, Sonnet, Opus : trois gammes pensées pour trois compromis différents entre vitesse, coût et puissance. Choisir la bonne, c'est déjà bien travailler.

Une famille, trois profils

Anthropic décline Claude en trois gammes. **Haiku** est le modèle le plus rapide et le plus économique, idéal pour les tâches simples et à fort volume. **Sonnet** est le modèle équilibré, polyvalent, qui couvre la grande majorité des usages professionnels. **Opus** est le plus capable, taillé pour les problèmes complexes, le raisonnement poussé et le code difficile. Ces gammes évoluent de version en version, mais la logique reste stable.

Le triangle vitesse / coût / performance

Il n'existe pas de « meilleur » modèle dans l'absolu : il y a un modèle adapté à chaque tâche. Un modèle plus puissant répond mieux aux problèmes durs, mais il est plus lent et plus coûteux. Utiliser Opus pour reformuler un e-mail, c'est du gâchis ; utiliser Haiku pour une analyse juridique fine, c'est risqué. L'art consiste à faire correspondre l'exigence de la tâche à la gamme.

Comment décider

Quelques repères : privilégiez une gamme légère pour la reformulation, la classification, les résumés courts, les réponses factuelles ; passez à la gamme équilibrée pour la rédaction soignée, l'analyse de documents, le code courant ; réservez la gamme haute pour le raisonnement complexe, les tâches à plusieurs étapes et les enjeux élevés. En cas de doute, on peut commencer léger et monter en gamme si la qualité ne suffit pas.

À RETENIR

Haiku (rapide/économique), Sonnet (équilibré), Opus (le plus puissant). Le bon réflexe : ajuster la gamme à la difficulté réelle de la tâche, pas prendre systématiquement la plus grosse.

LEÇON 02

Les limites des LLM

Un LLM est un outil remarquable mais faillible. Connaître ses limites n'est pas du pessimisme : c'est la condition d'un usage professionnel et responsable.

Les hallucinations

Parce qu'il génère du plausible, un modèle peut produire des informations **fausses avec assurance** : une citation inventée, une référence inexistante, un chiffre erroné. On appelle cela une *hallucination*. Le risque est d'autant plus grand que le sujet est précis, récent ou peu représenté dans les données. La parade : vérifier les faits importants, demander des sources, et utiliser la recherche web quand l'actualité compte.

La date de coupure des connaissances

Le savoir du modèle s'arrête à une certaine date. Il ne « sait » rien des événements postérieurs et peut l'ignorer lui-même. Pour toute information susceptible d'avoir changé (prix, dirigeants, actualités, versions logicielles), il faut lui faire chercher la donnée à jour plutôt que se fier à sa mémoire.

Les autres limites

Un LLM peut se tromper en calcul mental, mal compter des éléments, perdre le fil sur des consignes très longues, ou refléter des **biais** présents dans ses données. Il n'a pas d'accès direct au monde ni à vos systèmes sans outils dédiés. Et il reste **non déterministe** : deux réponses à la même question peuvent différer.

La bonne posture

Traitez Claude comme un collaborateur brillant mais à qui l'on relit le travail sur les points critiques. Il accélère, propose, rédige, analyse — mais la **responsabilité de la vérification** reste humaine, surtout pour les décisions importantes.

À RETENIR

Hallucinations, coupure des connaissances, erreurs de calcul, biais, non-déterminisme : un LLM se vérifie. Faire chercher les faits d'actualité et relire les points sensibles est un réflexe, pas une option.

LEÇON 03

Bonnes pratiques générales d'utilisation d'un LLM

La qualité d'une réponse dépend surtout de la qualité de la demande. Quelques principes simples améliorent considérablement les résultats.

Être clair et précis

Dites ce que vous voulez, pour qui, dans quel format et avec quelles contraintes. « Rédige un e-mail » donne un résultat vague ; « Rédige un e-mail court et cordial pour reporter une réunion à jeudi, en français, ton professionnel » donne un résultat utilisable. Le contexte que vous fournissez fait la différence.

Donner des exemples et un rôle

Montrer un ou deux exemples de ce que vous attendez (le style, la structure) oriente puissamment le modèle. Préciser un rôle (« tu es un correcteur exigeant ») cadre le ton et le niveau. Ces techniques, simples, sont parmi les plus efficaces.

Procéder par itérations

N'attendez pas la perfection au premier essai. Demandez, puis affinez : « plus court », « ajoute un exemple », « change le ton ». Le dialogue est le mode naturel de travail avec Claude. Découper une tâche complexe en étapes donne aussi de meilleurs résultats qu'une consigne monolithique.

Demander la vérification

Pour les sujets à enjeu, demandez explicitement des sources, une relecture critique, ou une double vérification des calculs. Vous pouvez aussi inviter le modèle à raisonner étape par étape. Enfin, encadrez le format attendu (liste, tableau, JSON...) pour obtenir un résultat directement exploitable.

À RETENIR

Clarté, contexte, exemples, itérations et vérification : cinq réflexes qui transforment la qualité des réponses. Une bonne demande vaut mieux qu'un gros modèle mal briefé.

LEÇON 04

Qu'est-ce qu'un outil (tool) ?

Seul, un LLM ne fait que produire du texte. Les outils lui donnent des « mains » : la capacité d'agir sur le monde extérieur.

Définition

Un **outil** (*tool*) est une fonction que le modèle peut décider d'appeler pour accomplir quelque chose qu'il ne sait pas faire par lui-même : rechercher sur le web, exécuter du code, lire un fichier, interroger une API, envoyer une requête à un service. Le modèle ne « fait » pas l'action lui-même ; il produit une demande d'appel, l'outil s'exécute, et le résultat lui est renvoyé dans le contexte.

Comment ça marche

Concrètement, le modèle reçoit la description des outils disponibles. Face à une tâche, il choisit s'il en a besoin, avec quels paramètres. L'outil renvoie un résultat (par exemple les pages trouvées, la sortie d'un calcul), que Claude intègre pour formuler sa réponse. C'est ce va-et-vient qui rend l'assistant capable de dépasser sa simple culture générale figée.

Pourquoi c'est essentiel

Les outils compensent directement les limites vues précédemment : la recherche web contourne la date de coupure ; l'exécution de code fiabilise les calculs ; l'accès aux fichiers et aux applications ancre les réponses dans vos données. Les **connecteurs** que nous verrons plus loin ne sont, au fond, que des outils reliés à des services externes (Gmail, Drive, Slack...).

À RETENIR

Un outil permet au modèle d'agir au-delà du texte : chercher, calculer, lire, écrire, interroger un service. C'est la brique qui transforme un générateur de texte en assistant opérationnel.

LEÇON 05

Qu'est-ce qu'un agent ?

Quand un modèle enchaîne outils et décisions pour atteindre un objectif de façon autonome, on parle d'agent. C'est un changement de nature dans la manière de travailler.

De l'assistant à l'agent

Un assistant répond à une demande. Un **agent** poursuit un **objectif** : il planifie, appelle des outils, observe les résultats, ajuste, recommence, jusqu'à atteindre le but. Au lieu de « réponds à cette question », on lui confie « organise ceci », « traite ces fichiers », « prépare ce livrable » — et il enchaîne les étapes nécessaires.

La boucle agentique

Le fonctionnement typique est une boucle : *réfléchir* → *agir (via un outil)* → *observer le résultat* → *décider de la suite*. Cette boucle se répète tant que la tâche n'est pas terminée. C'est précisément ce qui permet à un agent de mener des travaux à plusieurs étapes sans qu'on le guide à chaque instant.

Exemples et cadre

Claude Code (assistant de développement) et Cowork (délégation de tâches sur vos fichiers) sont des exemples d'usages agentiques. Cette autonomie s'accompagne de **garde-fous** : validation humaine pour les actions sensibles (envoyer un message, supprimer, payer), permissions explicites, et transparence sur les étapes. Nous y reviendrons dans les modules Cowork et sécurité.

À RETENIR

Un agent poursuit un objectif en bouclant « réfléchir → agir → observer → ajuster » à l'aide d'outils. Plus d'autonomie, donc plus de valeur — mais aussi la nécessité de garde-fous sur les actions irréversibles.