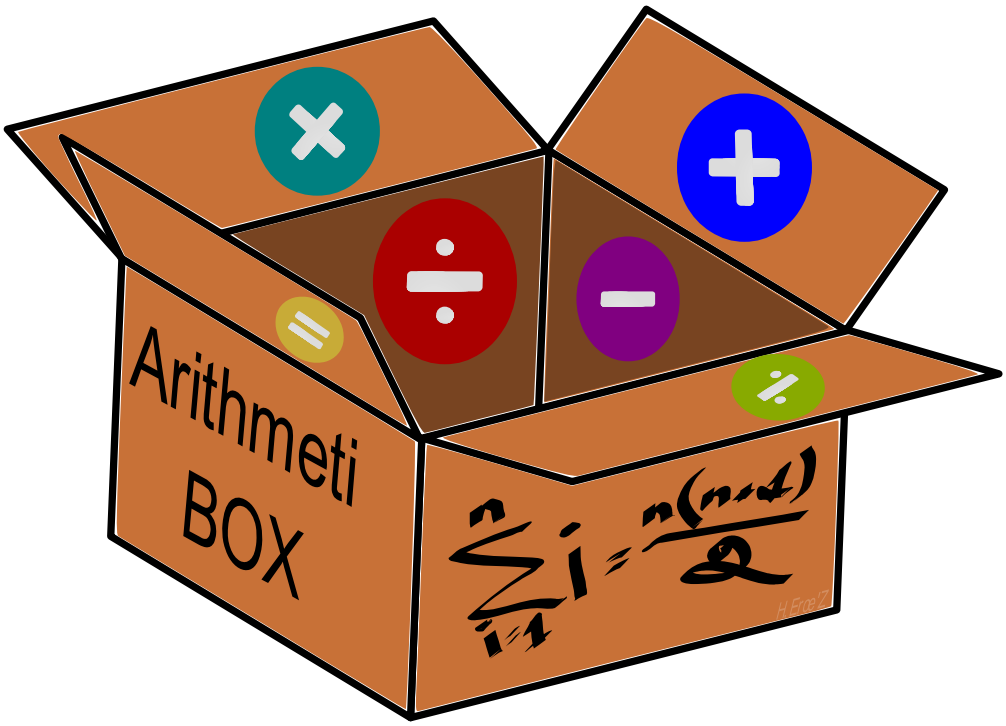
ArithmetiBox

Projet semestre 3



Team ArithmetiBox :

- *RAT Quentin*
- *WONG Jason*
- *KAING Jack*
- *DOS SANTOS Jeremy*
- *MOUGAMMADOUARIBOU Fahath*

Groupe: A1

Introduction

* La description du projet
    -résumer du projet
    -contrainte et objectifs
* Les solutions mise en œuvre
* Les problèmes rencontrés et leurs résolutions
    -risque possible rencontrer
    -principal problème rencontrés
* Gestion de projet
    - users stories
    - stories techniques
    - stories
    - estimation du temps
    - liste des Sprints
    - répartition des taches
* Les algorithmes
* Synthèse des comptes rendus des rendez vous avec l'enseignant
* La conclusion
* En annexe : un peu de code, copies d'écran, etc
* Un glossaire
* Les références bibliographique

Description du projet

Tableau d'avancement : *Mettre le lien*

Résumé du projet:
Le but du projet est de est de créer une boite à outils d'arithmétique avec les technologies du web qui sera par la suite intégrer à Ataraxy. Pour le projet nous utiliserons les langages tel que le PHP, HTML, CSS et le languages de compilation mathématique LaTeX. Ce projet sera évaluer par notre enseignant et client Mr Hébert. Il s'agit de réaliser ce projet pendant le S3 pour cela nous seront cinq pour développer le projet, Quentin Rat sera le chef de projet charger de le rendre.
La création de divers diagramme sera demander. Nous utiliserons essentiellement texMaker comme logiciel.

Le projet vas se dérouler en 4 grande parties:

- -La première partie consiste à:
  - -Mettre en place un espace de partage Gmail Github pour pouvoir travailler a distance
  - -Prendre en main les logiciels et langages tel que Latex et Github
  - -Nous allons concevoir des diagrammes pour modéliser le projet
  - -Il faudra planifier les tâches avec GanttProject
- -La deuxième partie consiste à:
  - -Schématiser sur papier un aperçue graphique de la page web
  - -Créer un logo pour la page (en .svg)
  - -Commencer à développer en HTML et CSS le squelette de la page web
- -La troisième partie consiste à:
  - -Commencer à coder les différentes fonctionnalités en PHP (ex: PGCD...)
  - -Intégrer la fonctionnalités précédente au menu

-Faire la partie ou l'ont générer le code Latex
(c'est trois sous partis se feront petit à petit en fonction de l'avancement du cours de crypto)

-La quatrième partie consiste à:
-Corriger les erreurs
-Tester toute les fonctionnalités

Contraintes:
Temps: Notre principal contrainte sur ce projet sera le temps, il faudra impérativement respecter le délai.

Objectifs (classement coût, délai, qualité):
1ère: il faut respecter le délai et il faudra procéder a une présentation final, il y aussi des revues toute les semaines pour voir l'avancement du projet.
2ème: il faut que la page web soit bien coder c'est a dire pas de beug et de dysfonctionnement
3ème: Le coût de la page web est nulle

Les solutions mise en œuvre

La page web est un site développer dans les languages HTML, CSS, PHP et LaTeX, c'est une une boite à outils d'arithmétique qui sera par la suite intégrer à Ataraxy, les différent outils developper seront des algorithmes d'arithmétique vue en cour de S3 (ex: PGCD, codage César...). La page web sera constituer d'un menu a gauche ou il y aura plusieurs onglet répertorier chaque onglet correspondra à un algorithme vue en cour. La page devra aussi générer du code Latex a partir des détails du résultat du calcul obtenue.

Les parties prenantes du projet son les cinq développeur et le professeur et aussi client qui sera la pour noter notre travail et nous aidez.

Les Risques et Problèmes rencontrés

Les risques du projet sont :
- Tombe malade
- Surcharge de travail
- Perte de donner (ex : perte du code)
- Mauvaise planification du temps de travail
- Beug pendant une présentation
- Trop s'éloigner du sujet donner
- Être trop ambitieux

Les 2 risques ayant la plus grande probabilité de se réaliser sont:
- Surcharge de travail
- Mauvaise planification du temps de travail

Pour être sur que ces situations n'arrive pas nous allons prendre soin de bien rédiger les taches a accomplir et bien organiser son temps pour ne pas être surmener de travail.
Si un des risques cités venait à se produire il faudrait tout de suite le corriger pour ne pas mettre en péril l'avancement du projet.

Le principal problème rencontrer lors du projet et qui n'étais pas cité étais un problème avec la bibliothèque GMP pour le PHP qui gére les grand entier, nous utilisons principalement tous MAMP sur mac et la bibliothèque n'étais pas pré installer a l'installation et nous avons rencontrer des difficultés pour l'utiliser nous avons finalement installer WAMP sur un pc avec windows qui lui bénéficie de la bibliothèque GMP déjà installer.

Diagramme de cas d'utilisation

Documentation des cas d'utilisation

Digramme cas d'utilisation

Description

Notre diagramme de cas d'utilisation est constitué de 1 acteur, qui est l'utilisateur du site, il choisit un

Acteurs impliqués

- Utilisateur (acteur primaire)

Déroulement du cas d'utilisation

- Choisir une catégorie dans le menu
- Taper les informations demander (nombre...)
- Telecharger le code LaTeX

USER STORIES:

1. En tant qu'utilisateur je veut pourvoir calculer le pgcd afin de connaître le plus grand diviseur commun.

2. En tant qu'utilisateur je veut pourvoir calculer le plus grand commun diviseur (pgcd) en appliquant l'algorithme d'Euclide étendue afin de connaître le pgcd de deux nombres et d'avoir le détail du calcul sous forme d'un tableau (a, b, r, q).

3. En tant qu'utilisateur je veut pourvoir calculer non seulement leur plus grand commun diviseur (PGCD), mais aussi un de leurs couples de coefficients de Bézout afin de connaître le pgcd et d'avoir le détail du calcul sous forme d'un tableau (a, b, r, q, u, v).

4. En tant qu'utilisateur je veut pourvoir calculer l'inverse modulaire d'un nombre afin de savoir si l'inverse de se nombre modulo n, existe ou non.

5. En tant qu'utilisateur je veut pourvoir calculer les puissance modulaires communément appelé exponentiation modulaire rapide afin de connaître les puissances entières d'un nombre.

6. En tant qu'utilisateur je veut pourvoir calculer les diviseurs d'un nombre grâce à l'algorithme de factorisation afin de connaître tout les diviseurs de se nombre et ensuite d'avoir la décomposition en produits de nombres premiers de se nombre.

7. En tant qu'utilisateur je veut pourvoir calculer l'inverse d'une matrice modulaire afin de connaître l'inverse d'une matrice cette fonction sera aussi utile pour décrypter un code crypter avec le chiffrement de Hill.

8. En tant qu'utilisateur je veut pourvoir afficher la liste des nombres premier jusqu'à n afin de savoir si un nombre est premier ou pas.

9. En tant qu'utilisateur je veut pourvoir calculer la valuation p-adique afin de connaître de connaître la valuation p-adique de ce nombre.

10. En tant qu'utilisateur je veut pourvoir calculer la congruence afin de résoudre par exemple des équation diophantiennes.

11. En tant qu'utilisateur je veut pourvoir crypter et décrypter un message chiffré avec un chiffrement de Hill afin pour pourvoir lire clairement se message ou pour le cacher.

12. En tant qu'utilisateur je veut que le résultat de mes calculs soit afficher avec du LateX afin d'avoir un affichage plus esthétique.

13. En tant qu'utilisateur je veut pouvoir saisir des nombre très grand afin de de pourvoir faire différents calcul (pgcd, congruence...) avec ces grand nombres.

14. En tant qu'utilisateur je veut pourvoir faire une attaque par force brut par dictionnaire afin de décrypter les messages.

15. En tant qu'utilisateur je veut pouvoir naviguer sur la page web simplement afin de ne pas perdre de temps.

16. En tant qu'utilisateur je veut pourvoir crypter et décrypter un message chiffré en césar afin de pourvoir lire clairement se message ou le crypter.

17. En tant qu'utilisateur je veut pourvoir crypter et décrypter un message avec la méthode affine afin de pourvoir lire clairement se message ou le crypter.

21. En tant qu'utilisateur je veut pourvoir crypter et décrypter un message avec la méthode RSA afin de pourvoir lire clairement se message ou le crypter.

22. En tant qu'utilisateur je veut pourvoir crypter et décrypter un message avec la méthode de substitution afin de pourvoir lire clairement se message ou le crypter.

23. En tant qu'utilisateur je veut pourvoir crypter et décrypter un message avec la méthode Hill de dimension 3 afin de pourvoir lire clairement se message ou pour le cacher.

24. En tant qu'utilisateur je veut que quand je saisie n'importe quoi dans les zones de saisie le site m'affiche un message d'erreur afin de pourvoir limiter les erreurs de calculs ou de saisie de l'utilisateur.

25. En tant qu'utilisateur je veut pourvoir joindre un fichier avec un texte a crypter ou décrypter contenue dans ce fichier afin de ne pas avoir a copier coller le message dans la zone requise.

Stories techniques

18.
En tant que développeur, je doit installer le logiciel Wamp/Mamp afin de pourvoir exécuter du code php.

19.
En tant que développeur, je doit disposer d'un gitHub afin de pourvoir partager mon code avec le reste de l'équipe.

20.
En tant que développeur, je veut pourvoir disposer d'un groupe de messagerie afin de pouvoir discuter avec le reste de l'équipe projet sur par exemple un problème rencontré.

Stories

1. créer une fonction PGCD
2. créer une fonction Euclide
3. créer une fonction Euclide étendu
4. créer une fonction Inverse modulaire
5. créer une fonction Exponentiation modulaire rapide
6. créer une fonction Algorithme de factorisation
7. créer une fonction Inverse d'une matrice modulaire
8. créer une fonction Test de primalité
9. créer une fonction Valuation p-adique
10. créer une fonction Congruence
11. créer une fonction Chiffrement Hill
12. afficher le résultat de toute les fonction en LateX
13. inclure la bibliothèque GMP au fonction pour pourvoir manipuler des grand nombre
14. faire des attaque par force brute avec dictionnaire
15. faire une page web ergonomique et simple avec un menu
16. créer une fonction chiffrement Cesar
17. créer une fonction chiffrement Affine
18. Installer logiciel requis pour le projet
19. Installer gitHub et apprendre à maitriser gitHub
20. Créer un espace de messagerie pour pouvoir échanger
21. créer une fonction pour RSA
22. créer une fonction pour Substitution
23. faire Hill en dimension 3
24. filtrer les saisies et afficher un message d'erreur lorsque la saisie n'est pas correcte
25. inclure la possibilité de joindre un fichier texte et le décrypter au lieu de le copier coller ou l'écrire dans l'espace prévue

Estimation du temps

1. 2
2. 4
3. 5
4. 2
5. 3
6. 2
7. 8
8. 3
9. 2
10. 2
11. 15
12. 15
13. 20
14. 10
15. 18
16. 15
17. 15
18. 1
19. 1
20. 1
21.15
22.15
23.5
24.4
25.3

Total= 184 points

Liste des Sprints

Sprint 1 - Date Limite : 12 octobre - Cout : 21
-Cas 18 : Installer logiciel requis pour le projet
-Cas 19 : Installer gitHub et apprendre à maitriser gitHub
-Cas 20 : Créer un espace de messagerie pour pouvoir échanger
-Cas 15 : faire une page web ergonomique et simple avec un menu
-Schématiser sur papier un aperçue de la page web
-Créer un logo
-Créer le squelette de la page

Sprint 2 - Date Limite : 2 novembre - Cout: 91
-Cas 1 : créer une fonction PGCD
-Cas 2 : créer une fonction Euclide
-Cas 3 : créer une fonction Euclide étendu
-Cas 4 : créer une fonction Inverse modulaire
-Cas 5 : créer une fonction Exponentiation modulaire rapide
-Cas 6 : créer une fonction Algorithme de factorisation
-Cas 7 : créer une fonction Inverse d'une matrice modulaire
-Cas 8 : créer une fonction Test de primalité
-Cas 9 : créer une fonction Valuation p-adique

-Cas 10 : créer une fonction Congruence
-Cas 11 : créer une fonction Chiffrement Hill
-Cas 16 : créer une fonction chiffrement Cesar
-Cas 17 : créer une fonction chiffrement Affine
-Cas 12 : afficher le résultat de toute les fonction en LateX

RENDRE UNE VERSION BETA DU PROJET LE 2 NOVEMBRE

Sprint 3 - Date Limite : 17 janvier - Cout : 72
-Cas 13 : inclure la bibliothèque GMP au fonction pour pourvoir manipuler des grand nombre
-Cas 14 : faire des attaque par force brute avec dictionnaire
-Cas 21 : créer une fonction RSA
-Cas 22 : créer une fonction Substitution
-Cas 23 : Faire Hill avec dimension 3
-Cas 24 : Filtrer les saisies des utilisateurs
-Cas 25 : inclure la possibilité de joindre des fichiers contentant le message à crypter ou décrypter

RENDUE FINAL LA SEMAINE DU JEUDI 19 JANVIER (DATE PAS ENCORE PRECISÉ)

Répartition des taches :

-Fonction PGCD =>Jeremy
-Fonction Euclide =>Jeremy
-Fonction Euclide étendu =>Quentin
-Fonction Inverse modulaire =>Jack
-Fonction Exponentiation modulaire rapide =>Jack
-Fonction Algorithme de factorisation => ?
-Fonction Inverse d'une matrice modulaire => Quentin
-Fonction Test de primalité => Jeremy
-Fonction Valuation p-adique => Quentin
-Fonction Congruence => Jack
-Fonction Chiffrement Hill =>Fahath
-Fonction chiffrement Cesar => Jason
-Fonction chiffrement Affine => Quentin
-Fonction RSA =>Jeremy
-Fonction Substitution =>Jack

Algorithme

…

Synthèse des comptes rendus des rendez vous avec l'enseignant

Compte rendue 29 septembre

-Présentation d'un début de page web et de quelque fonctionnalité

A FAIRE POUR LE PROCHAIN RENDEZ-VOUS:
-Donner un vrai nom au variable
-Presenter Gestion projet (diagramme, CDCF…)
-Apprendre Latex

A NOTER:
-Le bouton latex sera supprimé

Compte rendue 6 octobre

A FAIRE POUR LE PROCHAIN RENDEZ-VOUS:
-Faire l'algorithme d'Euclide étendue
-Faire Euclide
-Faire inverse modulaire (trouver a-1)
-Faire matrice modulaire, pour la saisie de la matrice c'est un champ texte(1 nombre un espace...)
-Faire Algorithme de factorisation (on rentre un entier n sa renvoi l'ensemble des diviseur)
-Faire exponentiation modulaire rapide
-Faire l'inverse d'une matrice modulaire
changement de base...
-Faire test de primaliter
-Faire un onglet à propos ou l'on explique pourquoi on a fait le projet, qui sommes nous et dans quel but nous avons fait le projet ?
-Ajouter MaitreAtaraxy sur github

Compte rendue 12 octobre

A FAIRE POUR LE PROCHAIN RENDEZ-VOUS:
-Faire Hill et inverse modulaire opérationnelle et changer la saisie des matrices avec un textearea (sur plusieurs ligne)
-Faire l'algorithme de factorisation (ex: 12 = 2*2*3)
-Déterminer la valuation péadique
-Faire l'algorithme d'expo rapide
-Décryptage/Cryptage césar force brut avec dictionnaire et pareil pour affine
-en php il y a une librairie qui s'appelle GMP qui joue avec des grand nombre donc on refait tout avec une gestion des grand entier (ex: GMPadd_$y)
-preparer un fichier zipper pour le prof il sera mis sur la page

Compte rendue 2 novembre

A FAIRE POUR LE PROCHAIN RENDEZ-VOUS:
-Le test de primalité de Miller-Rabin
-Mettre un bouton à part pour Eratosthène
-proposer plusieurs resolution pour les nombres premier
-1 boutons attaque et propose le choix entre affine, Cesar et Hill
-Mettre des exemples de format de saisie
-/times pour changer le signe multiplication
-rajouter module inverse modulaire
-rajouter des titres au fonction quand on est dedans
-retirer lien vers ataraxy
-changer quand le pcgd n'est pas égal a 1 on n'affiche pas u et v
-ordonner par importance dans l'ordre:
    -PGCD
    -Euclide
    -Euclide étendue
    -Congruence
    ...
-LateX pour algo de factorisation, changer le nom en factorisation et on enlève les diviseur possible (2^2*3) et non 2*2*3 utiliser val_p
-Deux partis Math/Crypto

Compte rendue 16 novembre

A FAIRE POUR LE PROCHAIN RENDEZ-VOUS:
-Faire en sorte de filtrer la saisie et de mettre un message d'erreur lorsque la saisie n'est pas correcte
-Commencer RSA
-Commencer Substitution
-Commencer a se renseigner sur Hill en dimension 3

Compte rendue 8 décembre

FAIRE POUR LA PRESENTATION FINAL:
- Faire Hill a dimension 3
- Faire RSA
- Faire Substitution
- Faire un rapport comportant un sommaire, une introduction, le description du projet, les solutions mise en oeuvre, les problèmes rencontrés et leurs résolutions, une présentation des algorithmes, une synthèse des comptes rendus des points de rendez vous avec l'enseignant et le client, une conclusion et En annexe : un peu de code, copies d'écran, etc ... Ainsi que un glossaire et les références bibliographique
- Faire un diaporama pour la présentation (mettre peut de texte privilégier les explication à l'oral)