サイボウズ・ラボユース中間成果発表

2015/8/25 @elliptic_shiho

自己紹介

- 緑川 志穂 (@elliptic_shiho)
- 高校1年生
- 技術系なら割と雑食
- 数学, 暗号, ...
- seccamp 2015参加
  - 低レイヤー中心
  - でも成果発表は高レイヤーだった

背景

- OS作った
- CPUの設計もした
- Webデザインもした
- 楕円曲線触るの楽しい!✌('ω'✌)三✌ ('ω')✌三(✌'ω')✌

ただ

C++が圧倒的に”””苦手”””

C++苦手!

- Cは大体脳内でコンパイルした結果で検討を付けてコードを書ける
- オブジェクト指向はJava/(SmallTalk)で理解した
- Python, Ruby, PHP, ...でスクリプト言語の書き方をやった

C++苦手!

- C++の入門書を買った
  - publicな継承????
  - 参照ってこれポインタでよくね?
  - ギャー謎のエラー出たー
    - なんだvtableって

C++苦手!

- ネイティブアプリ(というかただ単に機械語)が好きでC言語でアプリを書くことはよくある
- 勿論クラスなんかは欲しかったし、限界を感じてもいた

  → but?

C++苦手!

- publicな継承?参照の存在意義??そもそもの意味不明なコンパイル結果???
- 毎回やる気無くして数百行消してall Cで書き直したりしてた
- TMP/constexprで遊んではいた
  - そんなんだからそもそも「完成した!」といえるプログラムが殆ど無い

ラボユース

- Twitterで流れてきたラボユースという文字を調べてみる
  - 楽しそうじゃんこれ!
  - ちょうど今の状況打破出来そう?
  - 応募してみた→面接→通った

ラボユース

- 光成さんとは私が光成さんが書いていた暗号の本のレビュワーとして参加した時から
  - 暗号を実装してみたいという気持ちもあった
  - ただ、最初からそういうのを出すのもなぁ..と思い、FFTを実装してみることにした

ラボユース

- が
  - 実際にコードレビューをされてみると、意外と自分の中での「C++」とは構造がまるで違うことに気づいた
  - C++の見方が変わった
- ユニットテスト，参照の意味，C++的お作法，…
  - この時だけでどれだけの事を学んだだろうか

ラボユース

- 結局FFT作る前に複素数クラスを作るだけで前半が結構終わってしまった...
  - この後の時間でFFT難しい?
  - ついでなので、ECDHEみたいな暗号系を実装してみよう

ラボユース(後半戦)

- gmpを使った実装になった
  - ユニットテストのコード, Makefile等は複素数クラスを作った時の資産を一般化して再活用
- operatorをメンバ関数じゃない形で定義出来ることを初めて知った
- 最後の最後にはタイムテストを入れてみたり。

ラボユース(後半戦)

- 見事に実装を完成させた。
- 実装したのは楕円曲線上の点と有限体クラス
  - gmpをフル活用
- 今でも自分で変なコードを書き出す事があるので気をつけたい

まとめ

- 進捗がすごい速さで進んだ
- 新しい世界を見ることが出来た
  - C++の脳内コンパイルはまだちょっと...
- 継承関連に関してはまだできていないので、自宅でやりたい

まとめ

- 何より、ちゃんとプログラムを完成させることが出来た。
  - しかもかなり苦手だったはずの言語で!
- これから先のモチベーションにかなりつながった
  - ラボユース制度に感謝

ありがとうございました