出来るだけ数学を回避したLLL入門

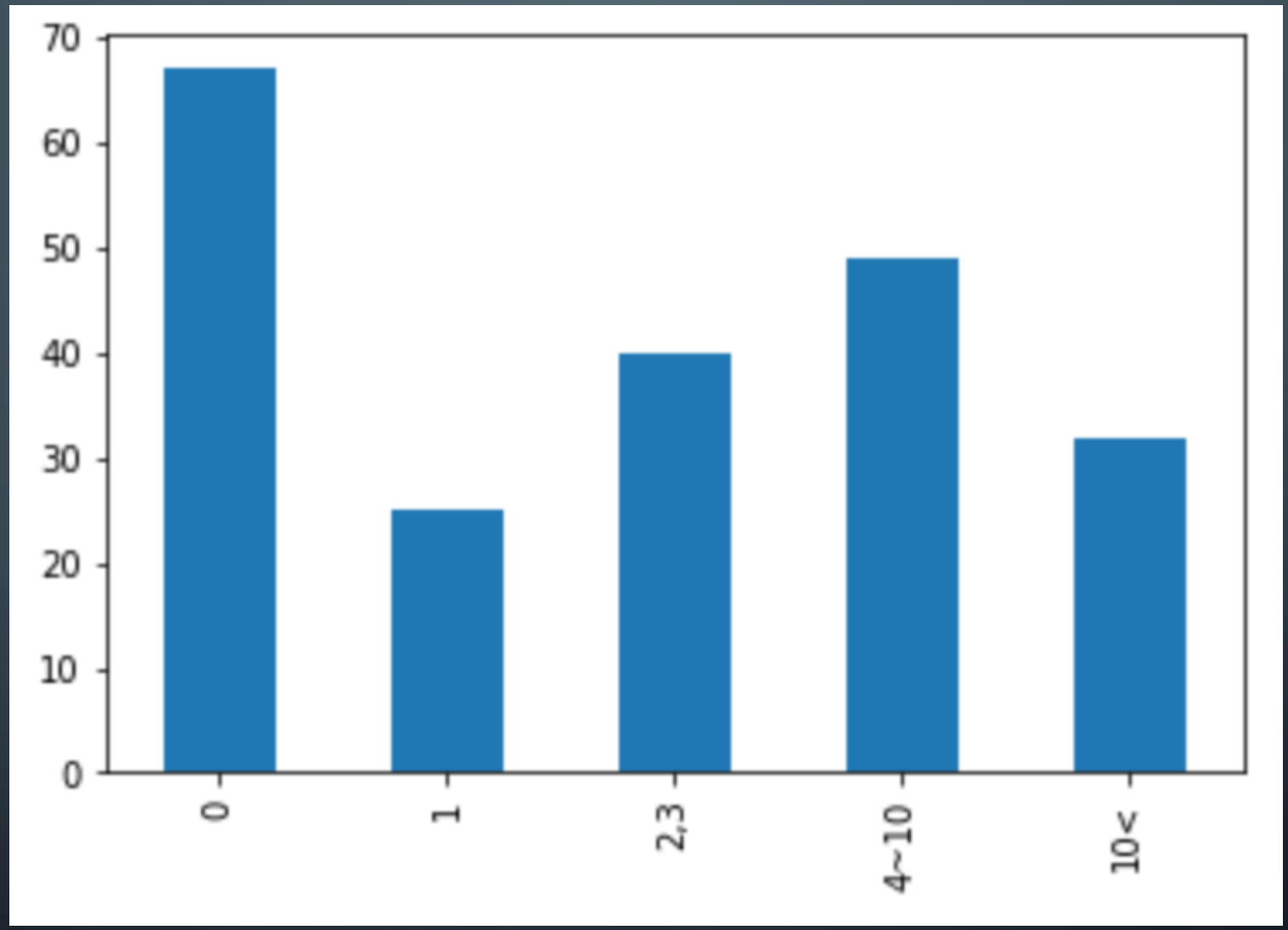
$ whoami

- 名前: Xornet (Twitter: @Xornet_Euphoria)
- CTFチーム: ./Vespiary (Founder)
- 担当: Crypto、たまにRev
- 専門: 物理(基礎実験) → 情報科学(暗号)
- CTF歴: 2年ちょっと、Cryptoは1年半ちょっと、LLLは半年ぐらい

Prerequisite

- ベクトル、できれば基底の概念
- 紹介する例題を解いたり資料を読むのにはある程度Cryptoの知識が必要

本題に入る前に…



CTF初心者がまあまあ多いようなので…

自分の初心者時代

- 復号して出てきた数字をどうフラグにするのかわからなかった
  - pycryptodomeの`long_to_bytes`という関数で出来ます
  - → CTFは分かれば自明な事が分かるまでが長い

- 実は最初はWebから始めた
  - SQLiが好きだったが、フロントエンドがよくわからずCryptoに浮気
  - → 最初は色々触って自分に合う分野を見つけていこう

初心者時代の自分に今伝えたいTips (1)

- 過去問やリポジトリをうまく利用しよう
  - Dockerで動かせるようになってる事がある
  - 推奨: InterKosenCTF, redpwnCTF(2020)
- Writeupを積極的に読もう
  - 復習をしようとほぼ同義
  - なんなら自分で書こう

初心者時代の自分に今伝えたいTips (2)

- CTFtimeとうまく付き合おう
  - まずはfor beginnersと書かれてるCTFから
- 解けなくても萎えたり諦めたりしない
  - 最近のCTFの難化傾向は異常
- チームを組もう
  - 烏合の衆にならないように注意
  - チームを集団で引っ張る意識が高い人と、点数的に引っ張る頭の良い人が欲しい

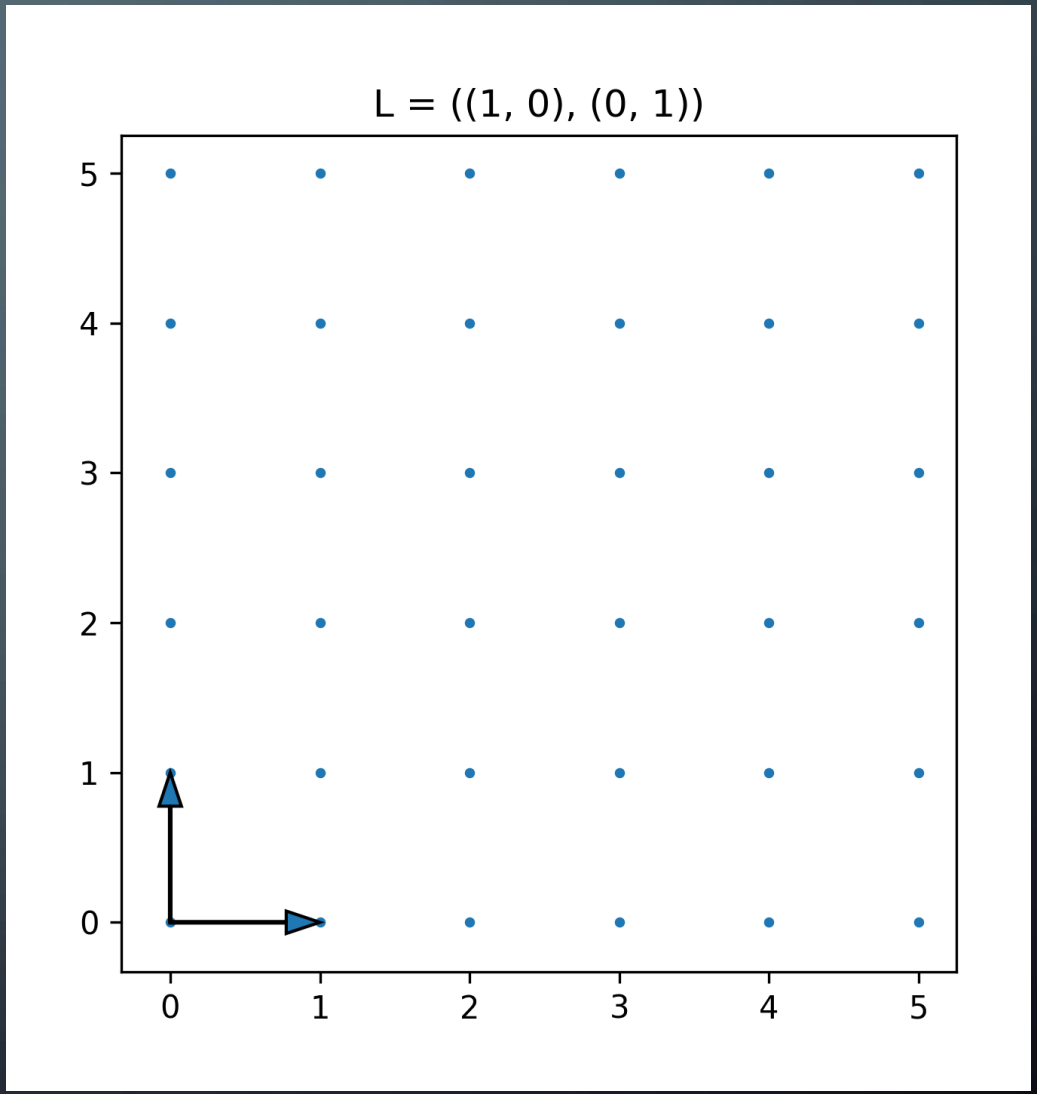
本題に入ります

お断り

- LLLの学習障壁を下げる為に「出来るだけ数学を回避した」説明をします
- より詳細な議論等は後述する資料等を参照してください

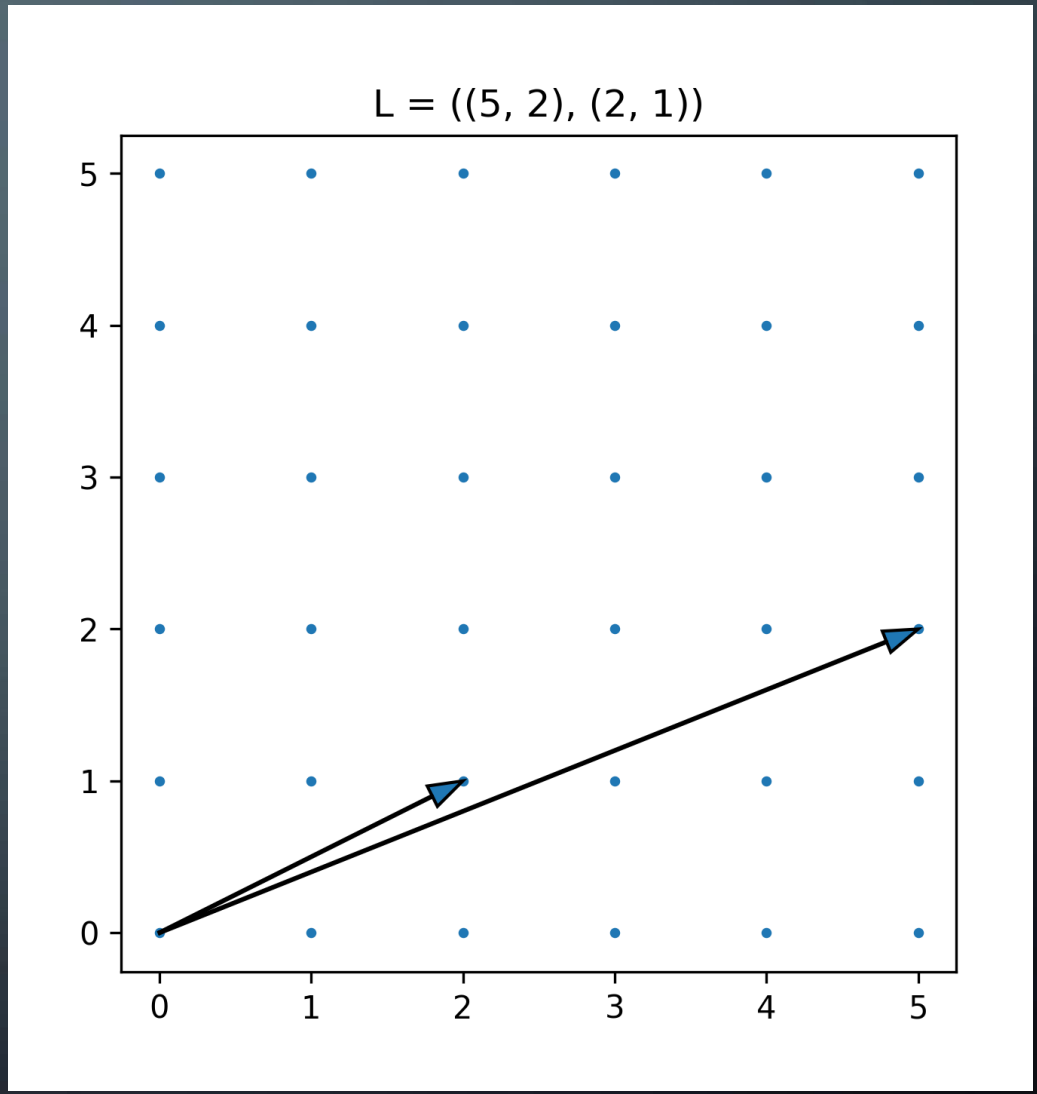
格子って何?

- 基底ベクトルの整数係数線形結合
- 右の図は(1, 0)と(0, 1)からなる格子



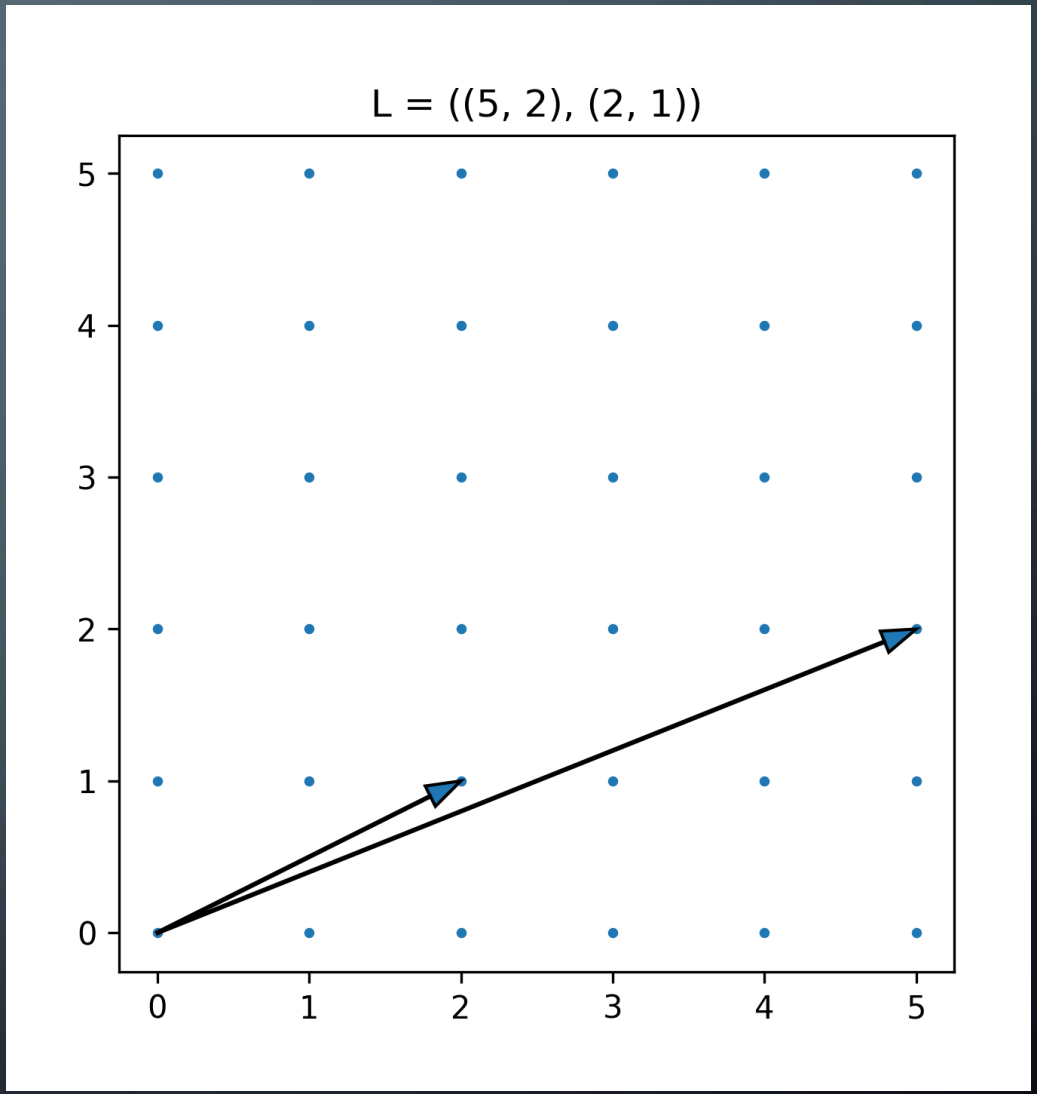
格子によって基底は一意?

- いいえ、異なる基底でも同じ格子を張る事がある
- 右の図は(5, 2), (2, 1)からなる格子だが前ページと同じ格子を張る



SVPって何?

- 格子に含まれるベクトルで最も短い非零なものを探す問題
- 前スライドの例だと(0,1)と(1,0)
- 格子の次元が高いと難しい



LLLって何?

- ある格子の基底から同じ格子を張り、ある程度短くて直交した別の基底を求めるアルゴリズム

- 得られた基底から最も短いものを持ってくればSVPを近似的に解決出来る

LLLを使うと(CTF的に)何が嬉しい?

- Merkle-Hellmanナップサック暗号の解読
- 合同方程式への応用
- Hidden Number Problemの解法
  - ECDSAのBiased Nonce Attack等に使える
- Learning with Errors (誤差付き合同方程式)
- 出力の一部しかわからないLCGの解読
- Coppersmith's Attack (小さい解を持つ合同方程式の解法)

LLLの資料(日本語サイト)

- katagaitai workshop #7 crypto ナップサック暗号と低密度攻撃
- LLLで殴る【yoshi-camp 2020 Spring備忘録】
- LLLでCrypto問題を解く - Project Euphoria

LLLの資料(英語サイト)

- [English] How to use lattice in CTF? - SECCON 2020 sharsable writeup by Kurenaif
- jhs7jhs/LLL - GitHub
- rkm0959/Inequality_Solving_with_CVP - GitHub

LLLの資料(書籍)

- 格子暗号解読のための数学的基礎
- 耐量子計算機暗号
- 現代暗号への招待(15章)

LLLを使う問題例 (1)

- CryptoHack (常設CTF)
  - そもそもLatticeというサブカテゴリーがあります
- ナップサック暗号問題全般
  - この土日に開催されたctf4bにも出てたらしいですね
- sharsable - SECCON 2020
  - SVPで解く良いWriteupがあります
- not so hard rsa - HITCON 2019

LLLを使う問題例 (2)

- Wilhelmina Says - Harekaze mini CTF
  - Hidden Number Problem
- Leak - pbctf
  - Biased Nonce Attack
- Easy pseudo random - zer0pts CTF 2021
  - 多変数Coppersmith's Attackが想定解ですがSVPでも解けます

最後に

- 後ほど資料や問題集のページにリンクを載せてスライドを公開します
  - 指摘事項や追加資料、問題情報があれば反映しますので何かあればTwitterまで
- 私もまだ勉強中の身ですが、この発表を期にCryptoや格子理論に興味を持っていただけたら幸いです

ありがとうございました