紅の魔術工房
Atelier kurenai

CTF 入門

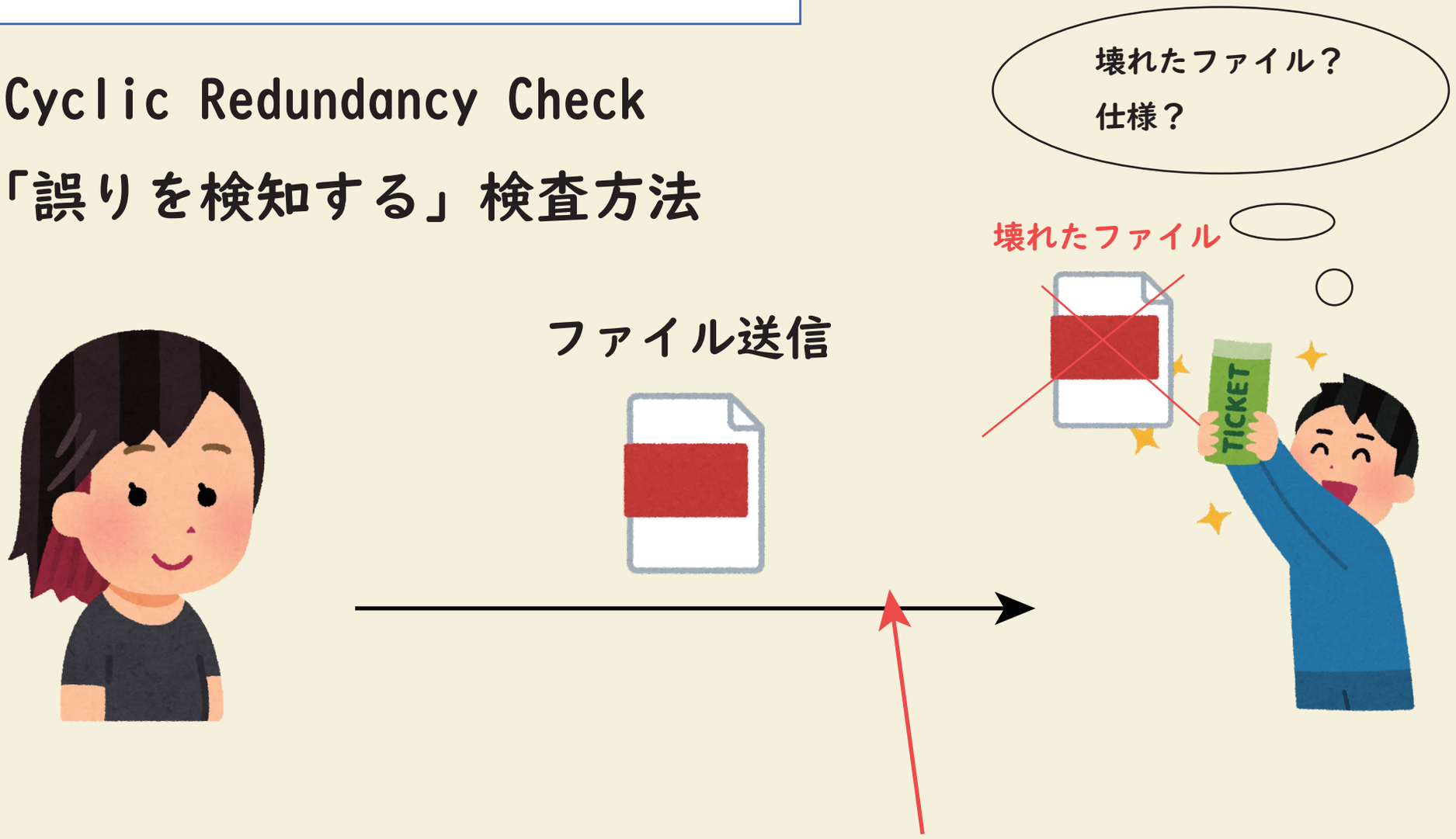
CRC32 で誤りを検知する

@kurenaif

CRC32 って？

Cyclic Redundancy Check

「誤りを検知する」検査方法



なぜ CRC32 を解説するの？

符号理論は勉強してないので、体系的に説明できない… すまない…

- 拡大体
- GF(2^n) な多項式
- 「体」であることから得られる様々な恩恵
- 「線形性」が成り立つことからの様々な遊び

暗号で広く使われるこれらを使って、比較的簡単に応用ができる分野だから

どこで CRC32 は使われているの？

png ファイルとかに内蔵されている

```
  IHDR Interlace: 0
  IHDR Compression algorithm is Deflate
  IHDR Filter method is type zero (None, Sub, Up, Average, Paeth)
  IHDR Interlacing is disabled
  Chunk CRC: -869110134
Chunk: Data Length 309 (max 2147483647), Type 1346585449 [iCCP]
  Ancillary, public, PNG 1.2 compliant, unsafe to copy
  ... Unknown chunk type
  Chunk CRC: -960355186
Chunk: Data Length 65536 (max 2147483647), Type 1413563465 [IDAT]
  Critical, public, PNG 1.2 compliant, unsafe to copy
  IDAT contains image data
  Chunk CRC: 1441794358
Chunk: Data Length 65536 (max 2147483647), Type 1413563465 [IDAT]
  Critical, public, PNG 1.2 compliant, unsafe to copy
  IDAT contains image data
  Chunk CRC: -1856956801
Chunk: Data Length 65536 (max 2147483647), Type 1413563465 [IDAT]
  Critical, public, PNG 1.2 compliant, unsafe to copy
  IDAT contains image data
  Chunk CRC: 126825411
Chunk: Data Length 19446 (max 2147483647), Type 1413563465 [IDAT]
  Critical, public, PNG 1.2 compliant, unsafe to copy
  IDAT contains image data
  Chunk CRC: -425976308
Chunk: Data Length 0 (max 2147483647), Type 1145980233 [IEND]
  Critical, public, PNG 1.2 compliant, unsafe to copy
  IEND contains no data
  Chunk CRC: -1371381630
```

今日の講義では
png ファイルからバイナリデータを
抽出して、
この CRC を求めるところまでを
目標にしています！

紅の魔術工房
Atelier kurenaif

CRC32 の理論を説明する道のり

- 体とは？
- 有限体とは？
- 拡大体とは？
- 多項式で体を作ろう！
- 多項式の体をコンピューターで扱ってみよう
- CRC32 への応用

「体」とは？

直感的には、「足し算」、「引き算」、「掛け算」、「割り算」ができるもの。

ただし、いくつかの制約がある。

「引き算」と「割り算」は使わない。

「体」では、「足し算」と「掛け算」のみ行う。

「引き算」と「割り算」は、「逆元」を使って表現する

2と足して0になる数

$$1-2=1+(-2)$$

$$4\div 2=4\times\frac{1}{2}$$

2とかけて1になる数

使える数（集合）の制限。

「体」では、まず使う数を制限する。

- 整数
- 有理数
- 複素数
- ベクトル
- 行列

etc...

使う範囲は自分で決めていい。

僕は「複素数のベクトル」にする！

私は「整数」だけ！

使って良い数たち全部のことを

「集合」という

制限したら、計算前も、計算後もとにかくその数以外は使用不可。

具体例は次のページで

使える数（集合）の制限。

整数だけの範囲で考えてみる。

$$1+2=3$$

$$1\times 2=2$$

$$1-2=1+(-2)=-1$$

$$4\div 2=4\times\frac{1}{2}=2$$

分数は整数ではない！

アウト！

使える数（集合）の制限。

3次元ベクトルだけの範囲で考えてみる。

$$(1,2,3)+(2,3,4)=(3,5,7)$$
$$(1,2,3)-(2,3,4)=(-1,-1,-1)$$
$$(1,2,3)\cdot(2,3,4)=20$$

掛け算を内積と割り当てると、20は3次元ベクトルじゃないのでアウト！

（それぞれの要素の掛け算やわり算であれば、分数を認めればOKですね）

使える数（集合）の制限。

0 を含む正の有理数だけの範囲で考えてみる。

$$1+2=3$$

$$5-2=5+(-2)=3$$

負の数は正の数ではない！

アウト！

$$1\times 2=2$$

$$4\div 2=4\times\frac{1}{2}=2$$

使える数（集合）の制限。

有理数だけの範囲で考えてみる。

$$1+2=3$$

$$5-2=5+(-2)=3$$

$$1\times 2=2$$

$$4\div 2=4\times\frac{1}{2}=2$$

すべて有理数で表されているので ◎

0 で割るみたいな異常なものを除いて、

選んだ範囲すべてでこのようにならなければならない。

体とは

1. まず使える数の範囲を決める（「集合」を決める）
2. 足し算と掛け算を何にするか考える（ベクトルの内積はNG）
3. 引き算と割り算は、足し算と掛け算に直す。
4. どんなときでも、使えるのは集合の中の数だけ。

（0で割るみたいな例外を除いて、どんな計算をしても
集合の中の数字に収まらないといけない。）

（集合の中の数一個のことを「元」という）

厳密な定義は教科書とかでしっかり学んでね

有限体とは？

整数： 無限個存在する。

有理数： 無限個存在する。

複素数： 無限個存在する。

0 を含む正の整数を 5 で割った値： 5 個しか存在しない

0 を含む正の整数を N で割った値： N 個しか存在しない。

この有限個しかないやつらで、もし

「体」を作ることができれば

有限体になる。

引き算と割り算を考える。

引き算は、**足して 0 になるような数に変換**してから、

足し算をする。

$$2-3 \xrightarrow{\text{変換}} 2+(-3)=1$$

これは 3 と足すと、0 になる数。

割り算は、**かけて 1 になるような数に変換**してから、

掛け算をする。

$$2\div 3 \xrightarrow{\text{変換}} 2\times\frac{1}{3}=\frac{2}{3}$$

これは 3 とかけると、1 になる数。

正の整数 mod 5 は「体」にできるのか？

足し算と掛け算はできそう。

正の数だから負の数が存在しない。→ 引き算ができない。

整数だから分数は存在しない。→ 割り算ができない。

・引き算は、足して 0 になるような数に変換してから、
足し算をする。

・割り算は、かけて 1 になるような数に変換してから、
掛け算をする。

この方針で、引き算と割り算を考え直してみよう。

正の整数 mod 5 は「体」にできるのか？

余り 5 の世界での引き算

例えば...

変換 →

1 と足して 0 になるような数は 4

$$1 - 1 = 1 + 4 = 0 \mod 5$$

$$2 - 2 = 2 + 3 = 0 \mod 5$$

$$3 - 3 = 3 + 2 = 0 \mod 5$$

$$4 - 2 = 4 + 1 = 0 \mod 5$$

mod 5 の中のすべての数たちに対して、負の数的な数字が見つかった！

しかも全部 mod5 の中に入ってる！

紅の魔術工房
Atelier kurenaif

正の整数 mod 5 は「体」にできるのか？

余り 5 の世界での引き算

変換 →

例えば...

2 とかけて 1 になるような数は 3

$$1 \div 1 = 1 \times 1 = 1 \mod 5$$

$$2 \div 2 = 2 \times 3 = 1 \mod 5$$

$$3 \div 3 = 3 \times 2 = 1 \mod 5$$

$$4 \div 2 = 4 \times 1 = 1 \mod 5$$

mod 5 の中のすべての数たちに対して、逆数的な数字が見つかった！

しかも全部 mod5 の中に入ってる！

正の整数 mod 5 は「体」にできるのか？

使える範囲の数だけを使って、
「足し算」、「引き算」、「掛け算」、「割り算」
ができたので、**これは体！**

しかも使える数が 5 つだけの有限個なので、
有限体！

mod 素数 の世界であれば、有限体は作れる！

正の整数 mod 4 は「体」にできるのか？

2 と掛け算して、1 になる数字は存在しない。

$$2 * 1 = 2 \bmod 4$$

$$2 * 2 = 4 \bmod 4$$

$$2 * 3 = 2 \bmod 4$$

2 では割り算できないから、これは「体」ではない。

多項式と「体」

Q. 多項式って何？

A. こんなやつ↓

$$1 \times x^2 - 2 \times x + 1$$

x の n 乗と、なにか係数がひっついてるやつ

係数で使える値を束縛する

$$x^2 - 1 = 0$$

この式解けますか？

係数で使える値を束縛する

$$x^2 - 1 = 0$$

$$(x+1)(x-1) = 0$$

$$x = 1, -1$$

係数で使える値を束縛する

$$x^2 + 1 = 0$$

この式解けますか？

係数で使える値を束縛する

複素数が使えなかったら
この式変形はできない。

$$x^2 + 1 = 0$$

$$(x + i)(x - i) = 0$$

$$x = i, -i$$

複素数を使っていいテスト以外ではバツになりそう

使える係数の範囲を絞る。

明確に、複素数は使っていけませんと明記すると
答えが変わる。

多項式の「足し算」、「掛け算」、「引き算」

多項式も、整数と同じように、足し算や掛け算、引き算ができる。

多項式の足し算

$$(x^2+2x+1)+(x^3+2x^2+3)=x^3+2x^2+2x+4$$

多項式の引き算

$$(x^2+2x+1)-(x^3+2x^2+3)=-x^3-x^2-2$$

多項式の掛け算

$$(x+1)(x+2)=x^2+3x+2$$

多項式の「割り算」

（x+1）とかけて１になる多項式を
求めなければならない。

$$\frac{1}{x+1} = a + bx + cx^2 + dx^3 + \cdots$$

単項式の割り算を、なんとかしてこの形に落とし込まなければならない。
難しそう…

多項式の割り算の「あまり」

正の整数は引き算や割り算はできなかったが、
「あまり」を導入することで「有限体」にできた。

実は、多項式でも「あまり」を使うことで、「有限体」にすることができる。

多項式の割り算の「あまり」

$$
\begin{array}{r}
x+2 \\
x^2+x+1 \overline{)\ x^3+3x^2+5x+5} \\
\underline{x^3+x^2+x} \\
2x^2+4x+5 \\
\underline{2x^2+2x+2} \\
\boxed{2x+3}
\end{array}
$$

これが

x^3+3x^2+5x+5 を

x^2+x+1 で割ったあまり。

タイトル

タイトル

タイトル

タイトル

タイトル

タイトル