



長崎県立波佐見高等学校

OSP事業に参加したねらい

- Linux で動作するアプリケーションを利用した授業実践
- Knoppix を効果的に活用するためのサーバの研究

今年度の成果

- Gnuplot → 物理実験データ処理
- bc → OpenSSL, RSA 暗号実習
- FedraCore6 でサーバ設定
- FSWiki でコンテンツ整理

●実施教科・単元

物理 I : 高等学校物理 I (数研) 波動

●実施環境

物理教室 : EPSON(1.8GHz, 256MB)

●活用するアプリケーション

Gnuplot (グラフ), FireFox (CMS) KWrite (データ入力)

●目的

【実践1】 Gnuplot を使って、波のグラフを作りながら、波動を数式で表す方法を学ぶ。

【実践2】 Gnuplot を使って実験データのフィッティングを行い、物理量の測定を行う。

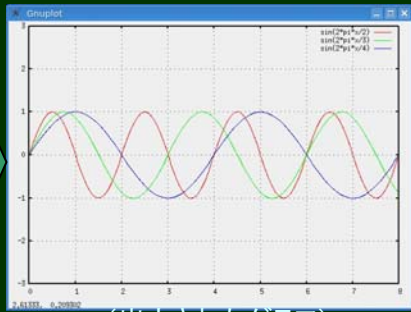
実践1: Gnuplotで波形作図実習

実践1: 波形グラフ作成実習

- ① グラフ作図練習 (→二次関数)
- ② 弧度法と三角関数
- ③ 波形のグラフ作図
- ④ 時間とともに移動する波形の作図

```
Terminal type set to 'x11'
gnuplot> set xrange[0:8]
gnuplot> set yrange[-3:3]
gnuplot> set grid
gnuplot> plot sin(2*pi*x/2),sin(2*pi*x/3),sin(2*pi*x/4)
gnuplot>
```

(波形出力のコマンド)



(出力されたグラフ)

感想および展望

OSP事業に参加し授業の幅が広がりました。本事業で得たノウハウを県内で広めていきたいと思っております。



(物理教室での実習)

実践2: Gnuplotでフィッティング実習

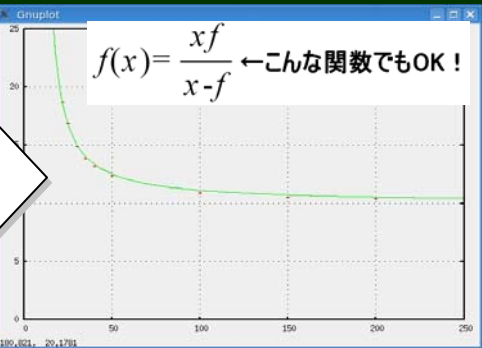
実践2: データ処理

- ① 凸レンズが作る像の実験
- ② KWrite で、データファイルを作成
- ③ データのプロット
- ④ データのフィッティングとその結果のリプロット
- ⑤ FireFox を使って、実験結果を Wiki にアップロード

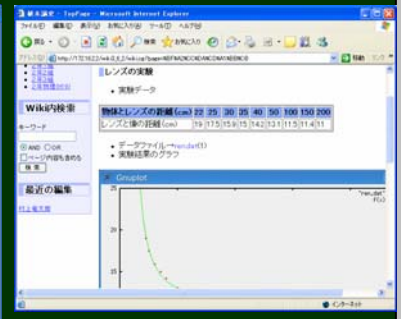
*弦の振動実験についても同様

```
ren.dat - KWrite
>set grid
>plot [0:250] [0:25] "ren.dat"
>f(x)=x*f/(x-f)
>fit f(x) "ren.dat"
...フィッティング結果の表示...
>f 表示された結果
>replot f(x)
```

(KWrite で作ったデータファイル)



(レンズの実験結果・フィッティング結果)



(FireFox を使って Wiki に保存)

実践3: OpenSSLコマンドを使った暗号化実習

●実施教科・単元

情報 A : 新・情報 A (日文)

●実施環境

パソコン室 : 富士通 (933MHz, 128MB)

●活用するアプリケーション

Konsole (OpenSSL), bc (RSA 暗号)

FireFox (CMS)

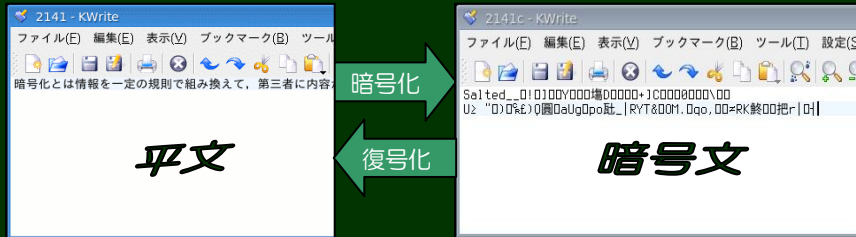
●目的

【実践3】 OpenSSL コマンドによる暗号化実習を通して、データ送信の安全性を確認する

【実践4】 RSA 暗号の方法と、そのしくみについて、bc を使ったべき乗・剰余演算を通して考える。

```
暗号化のコマンド
knoppix@knoppix:~$ cd D*
knoppix@knoppix:~/ramdisk/home/knoppix/Desktop$ openssl enc -e -des -in 2141 -out 2141c
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
knoppix@knoppix:~/ramdisk/home/knoppix/Desktop$ openssl enc -d -des -in 2141c -out 2141p
enter des-cbc decryption password:
```

(コンソール画面で暗号化のコマンドの入力)



実践3: 共通鍵暗号 (情報A)

- ① コンソールの起動と終了および練習
- ② KWrite で平文の作成・保存
- ③ コンソールを起動し、OpenSSL コマンドを用いて暗号化
- ④ 作成した暗号化ファイルを、KWrite で開きネットを流れる内容を確認
- ⑤ 暗号化ファイルを OpenSSL コマンドで復号



実践4: bcを使ったRSA暗号実習

実践4: RSA暗号 (情報A)

- ① 公開鍵暗号方式について学習
- ② bc を使ったべき乗・剰余計算
- ③ Mod 33 での冪乗剰余表の作成
- ④ RSA 暗号の暗号化・復号化のしくみ
- ⑤ 2素数 (3, 11) を使った鍵作成

	1	2	3	...	9	10	11	12	13	...	19	20	21
1	1	1	1	...	1	1	1	1	1	...	1	1	1
2	2	4	8	...	17	1	2	4	8	...	17	1	2
3	3	9	27	...	15	12	3	9	27	...	15	12	3
4	4	16	31	...	25	1	4	16	31	...	25	1	4
5	5	25	26	...	20	1	5	25	26	...	20	1	5
6	6	3	18	...	24	12	6	3	18	...	24	12	6
7	7	16	13	...	19	1	7	16	13	...	19	1	7
8	8	31	17	...	29	1	8	31	17	...	29	1	8
9	9	15	3	...	27	12	9	15	3	...	27	12	9
10	10	1	10	...	10	1	10	1	10	...	10	1	10

(Mod33のべき乗剰余表)



(bcを使ってべき乗剰余表作成)

2つの素数3, 11の積を法にとった場合、(3-1) × (11-1)+1 乗で元の数値があらわれてくることを、表を作りながら見つける。

bcは簡単なループ計算ができるので、剰余表作成に便利

```
bc
123^33
497^128598683427938449999752605643830
for(i=0;i<=32;i++) i^3%33
0
1
8
27
26
26
13
3
3
17
3
10
11
12
19
```

3乗で暗号化された数値は、7乗して剰余をとると元の数を21乗して剰余をとることと同じになるので、復号できる。

べき乗して余りをとる操作で暗号化・復号化を行う

(8を3, 33で暗号化し結果の17を7で復号)