２０２３年１０月１３日（金）

アルゴリズム数理Ｂ　第３週　課題

理工学部　数学科　３年
1070　富山和甫

問題１．カーマイケル数

n=600000 までのカーマイケル数を計算した結果の画面をいかに示す.

```
>python carmichael.py
カーマイケル数を判定する範囲 : 600000
[561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973
, 75361, 101101, 115921, 126217, 162401, 172081, 188461, 252601, 278545, 294409, 314821, 334153,
 340561, 399001, 410041, 449065, 488881, 512461, 530881, 552721]

>
```

問題２．1024bit 素数

見つけた 1024bit の例を以下に示す.

```
---- Prime ----
1151884876032507458248104243436880861623076572370872502047161109014344421493106896861681435519785004377859855105889028082448408000800418007370721226237172243754835317309459503664782769133496495053080617950002624293847533636036062390943946649501371399124745310362112775776897245421794987062743251566509943582291
>
```

問題３．RSA 暗号

鍵長が 64bit の RSA 暗号の秘密鍵の各数値を生成した結果をいかに示す.

```
>python generate_RSA_prime.py
生成する鍵のビット数 : 64
Privete-Key: (64 bit, 2 primes)
modules: 14059173028041826547 (0xc31c37615c2fa0f3)
publicExponent: 65537 (0x10001)
privateExponent: 13254927485083768097 (0xb7f2f651effad521)
prime1: 4228986343 (0xfc1135e7)
prime2: 3324478229 (0xc6278315)
exponent1: 1080525143 (0x40678157)
exponent1: 108808853 (0x67c4a95)
coefficient: 576591821 (0x225e17cd)

>
```