1) a) i)

$n = 21$

$FL(21) = \{a \in \mathbb{Z}^*_{21} \mid a^{20} \neq 1 \pmod{21}\}$

$a^{n-1} = 1 \mod (21)$

```
for a in range(0, 21):
    Print( a^20 % 21)
```

Fermat Lügner sind: $\{1, 8, 13, 20\}$

ii) Wie gross ist die Wahrscheinlichkeit einen Lügner zu finden wenn einmal gezogen wird? $4/20 = 1/5$

Wie oft muss man mindestens ziehen, dass die Wahrscheinlichkeit nur Lügner zu ziehen $<= 0.01$ ist?

Bsp: $1/5^k <= 0.01$

solve $(1 - 0.2^k <= 0.99) = 2.86$

↳ Mindestens 3 Ziehungen

b) $a^{n-1} = 1 \pmod{n}$

$n = 221$

for a in $A = \{18, 21, 23, 38\}$
print($a^{220} \% 221$)

Für die Zahlen 18, 21 und 38

c) for a in range(1, 4)
print($a^{8050} \% 8051$)

1 → 1
2 → 2274
3 → 509
4 → 2334

2) Wenn man $n = 3828001$ in Primfaktoren zerlegt (mittels Pari/GP) erhält man $101 \cdot 151 \cdot 251$. Eine Carmichael Zahl besteht aus mindestens 3 Primfaktoren von denen keine Primzahl doppelt vorkommt.

Mit Pari GP wurde überprüft ob für alle $a \in \mathbb{Z}_n^*$ $a^{n-1} = a \pmod p$ gilt wobei p die Primfaktoren von n sind.

Code:

```
isCarmichael(n) =
{
 factors = factor(n);
 for(i = 1, #factors,
  p = factors[i, 1];
  a = Mod(2, p);
  if (gcd(a,p) == 1 && a^p != a % p,
   return(0);
  );
 );
 return(1);
}
```

```
n = 3828001

if (isCarmichael(n),
   print(n, " ist eine Carmichael-Zahl."),
   print(n, " ist keine Carmichaehl-Zahl.")
);
```

Answer: 3828001 ist eine Carmichael-Zahl.

b) $n - 1 = 2^r \cdot u$

$3828000 = 2^5 \cdot 119625$

(1) a wird zufällig gewählt

$a = 2$

$2^{119625} \% 3828001 = 2879722$ also $!= 1$

(2) $2^{2^2 \cdot 119625} \% 3828001 = 1$ also $!= -1$

3828001 ist also zusammengesetzt.

3) $p = 17 \rightarrow \mathbb{Z}_{17}^{*}$

Beispiel $a = 5 \quad g = 7 \rightarrow \log_7(5) \bmod 17$

$7^{x} \bmod 17 = 5$

$x = 15$

g \ a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\log_7(a)$	16	10	3	4	15	13	1 17	14	6	9	5	7	12	11	2	8	\
$\log_{13}(a)$	4 8 12 16	\	\	3 7 11 15	\	\	\	\	\	\	\	\	1 5 9 13 17	\	\	2 6 10 14	\

Hilfstabellen

$7^1 \; 7^2 \; 7^3 \; 7^4 \; 7^5 \; 7^6 \; 7^7 \; 7^8 \; 7^9 \; 7^{10} \; 7^{11} \; 7^{12} \; 7^{13} \; 7^{14} \; 7^{15} \; 7^{16} \; 7^{17}$

$7 \; 15 \; 3 \; 4 \; 11 \; 9 \; 12 \; 16 \; 10 \; 2 \; 14 \; 13 \; 6 \; 8 \; 5 \; 1 \; 7$

$13^1 \; 13^2 \; 13^3 \; 13^4 \; 13^5 \; 13^6 \; 13^7 \; 13^8 \; 13^9 \; 13^{10} \; 13^{11} \; 13^{12} \; 13^{13} \; 13^{14} \; 13^{15} \; 13^{16} \; 13^{17}$

$13 \; 16 \; 4 \; 1 \; 13 \; 16 \; 4 \; 1 \; 13 \; 16 \; 4 \; 1 \; 13 \; 16 \; 4 \; 1 \; 13$