

Problem 1

$$\begin{aligned} \text{b) } -99 \% 1001 &= -99 + 1001 \% 1001 \\ &= 902 \% 1001 = 902 \end{aligned}$$

$$\begin{aligned} \text{c) } 232 + 22 \cdot 77 - 18^3 \% 8 \\ &= 232 + 22 \cdot 77 - 2^3 \% 8 \\ &= 232 + 22 \cdot 77 - 0 = 232 + 1694 \\ &= 1926 \end{aligned}$$

$$\begin{aligned} \text{d) } 55 &\equiv 77 (\% 12) \Leftrightarrow 12 \mid (55 - 77) \\ &= 12 \mid -22 \quad -22 = (-1) \cdot (1 \cdot 12 + 10) \rightarrow 12 \nmid -22 \Rightarrow \\ &55 \not\equiv 77 (\% 12) \end{aligned}$$

Problem 2 $ab \equiv 1 \pmod{n} \Leftrightarrow n \mid ab - 1$

b) We can see in the multiplication table which numbers have another number that yields 1 when multiplied and mod 12. These pairs are: $(1, 1), (5, 5), (7, 7), (11, 11)$

c) Mult inverse pairs are:
 $(1, 1), (2, 6), (3, 4), (4, 3), (5, 9)$
 $(6, 2), (7, 8), (8, 7), (9, 5), (10, 10)$

e) a has a multiplicative inverse mod n iff $\gcd(a, n) = 1$

Problem 3

$$\begin{aligned} b) e_R(\text{alice}) &= e_R(a)e_R(L)e_R(i)e_R(c)e_R(e) \\ &= 11:18:9:17:23 = \text{LSJRX} \end{aligned}$$

$$c) d_R(y) = a^{(-1)}(y - b) \% 26$$

Found $a^{-1} = 9$ programmatically.

$$d_R(y) = 9(y - 11) \% 26$$

$$\begin{aligned} d) d_R(RBK K \times RQ) \\ &= d_R(R)d_R(B)d_R(K)d_R(K)d_R(\times)d_R(R)d_R(Q) \\ &= 11:14:17:17:4:2:19 \\ &= \text{correct} \end{aligned}$$

e) An affine cipher is considered more secure than a rotation cipher since there are more keys to choose from, making it less susceptible to brute force COAs. For KPAs, this also holds, but since both use the same key for all letters, the search is so small that they're practically equally susceptible. Both are equally susceptible to frequency analysis.

f) b can be any number in $[1, 25]$, a can be any odd number in $[1, 25]$. Even numbers cannot be used since the function will not be injective. $\#k = 25 \cdot 13 = 300$

Problem 4

Teeksten en:

rekening aangeven zodat alles gaat

Nettel dekrypt: $(7, 4)$

Nettel encrypt: $(15, 4)$