

1.

$$28x + 36y = 100$$

Förkorta

$$36 = 128 + 8$$

$$28 = 38 + 4$$

$$8 = 24 + 0$$

Sgd(9,7)=1

$$7x + 9y = 25$$

$$9 = 1 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

Bezout

$$1 = 7 - 3 \cdot 2 = 7 - 3(9 - 7) = 4 \cdot 7 - 3 \cdot 9$$

Vi söker svar för "=25"

$$25 = 4 \cdot 7 \cdot 25 - 3 \cdot 9 \cdot 25 + 7 \cdot 9 \cdot n - 7 \cdot 9 \cdot n = 7(100 + 9n) + 9(-75 - 7n)$$

Sätt $n = -11$

$$7(1 + 9n) + 9(2 - 7n)$$

$$(x, y) = (1 + 9n, 2 - 7n)$$

2.

Låt x vara den summa pengar som Emilia äger.

$$\begin{cases} x \equiv 3 \pmod{29} \\ x \equiv 8 \pmod{40} \end{cases}$$

Euklides

$$40 = 129 + 11$$

$$29 = 2 \cdot 11 + 7$$

$$11 = 1 \cdot 7 + 4$$

$$7 = 1 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

Bezouts

$$1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 1 \cdot 7 = 2(11 - 7) - 1(7) = 2 \cdot 11 - 3 \cdot 7 = 2 \cdot 11 - 3(29 - 2 \cdot 11) =$$

$$8 \cdot 11 - 3 \cdot 29 = 8(40 - 29) - 3 \cdot 29 = 8 \cdot 40 - 11 \cdot 29$$

$$x_0 = 8 \cdot 3 \cdot 40 - 11 \cdot 8 \cdot 29 = -1592$$

$$x = -1592 + 29 \cdot 40 \cdot n = -1592 + 1160n$$

$$0 \leq x < 1000$$

$$n = 2 \Rightarrow 728$$

Mammas sida

$$728 - 3 = 725$$

$$725 \cdot \frac{1}{25} = 29$$

Pappas sida

$$728 - 8 = 720$$

$$720 \cdot \frac{1}{40} = 18$$

$$29 - 18 = 7$$

Svar: Det är 7 kusmer fler på mammas sida.

3.

Visa sann för $n=1$

$$V_L = 3 \cdot 0^2 + 3 \cdot 0 + 1 = 1$$

$$H_L = 1^3 = 1$$

Antag sann för n

$$\sum_{k=0}^{n-1} 3k^2 + 3k + 1 = n^3$$

Visa sann för $n+1$

$$\sum_{k=0}^n 3k^2 + 3k + 1 = \sum_{k=0}^{n-1} (3k^2 + 3k + 1) + 3n^2 + 3n + 1 = n^3 + 3n^2 + 3n + 1 = (n+1)^3 \quad \text{QED}$$

4.

- a) KAFFEKOPP : $\frac{9!}{(2!)^4}$
 b) LINUX : $5!$
 c) LUFTMADRASS : $\frac{11!}{(2!)^4}$

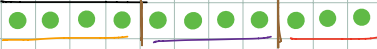
5.

- a) 3 siffror ska fördelas på 3 positioner: 3^3
 b) Det finns $\binom{7}{2}$ sätt att placera ut två eller 1 kombination med att det finns 2^5 sätt att fylla de övriga positionerna har vi $\binom{7}{2} \cdot 2^5$ sätt totalt
 c) 2 siffror fördelas på 7 platser: 2^7
 d) Vi söker 4, eller 5, eller 6, eller 7 1:or. $\sum_{k=4}^7 \binom{7}{k} 2^{(7-k)} = 379$

6.

Emil Emilia Gösta

Alternativ



- a) Pondera att vi använder 2 st avgränsare för att kunna dela upp de 11 karamellerna. Vi får då 13 objekt att placera och de två avgränsarna kan placeras på $\binom{13}{2}$ sätt.
 b) Vi kan nu bara lägga avgränsare mellan kulor. Dessa får inte läggas i samma mellanrum. $\binom{10}{2} = 45$.

7.

- a) $\binom{52}{5}$ - av 52 kort väljer vi 5.
 b) $\binom{13}{1} \binom{48}{1}$ - välj en av valörerna, välj sedan det återstående kortet
 c) $\binom{13}{1} \binom{12}{1} \binom{4}{1} \binom{4}{1}$ - välj, valör 1, valör 2, tag 3 av färg 1, 2 av färg 2.
 d) $\binom{13}{2} \cdot \binom{4}{2} \binom{4}{2} \cdot \binom{44}{1}$ - välj 2 valörer av 13, välj två från vardera färg, tag ett av 44 återstående kort.

8.

Vi söker den delen av den privata nyckeln som inte finns angiven, nämligen: inversen till $s \bmod \Phi(pq) \Leftrightarrow$ inversen till $23 \bmod (p-1)(q-1) = 40$.

Denna invers ges av $t=7$ ty $7 \cdot 23 = 161 \equiv 1 \bmod 40$. Det riktiga meddelandet ges nu av $3^7 = 42 \bmod 55$, det riktiga talet är alltså 42.