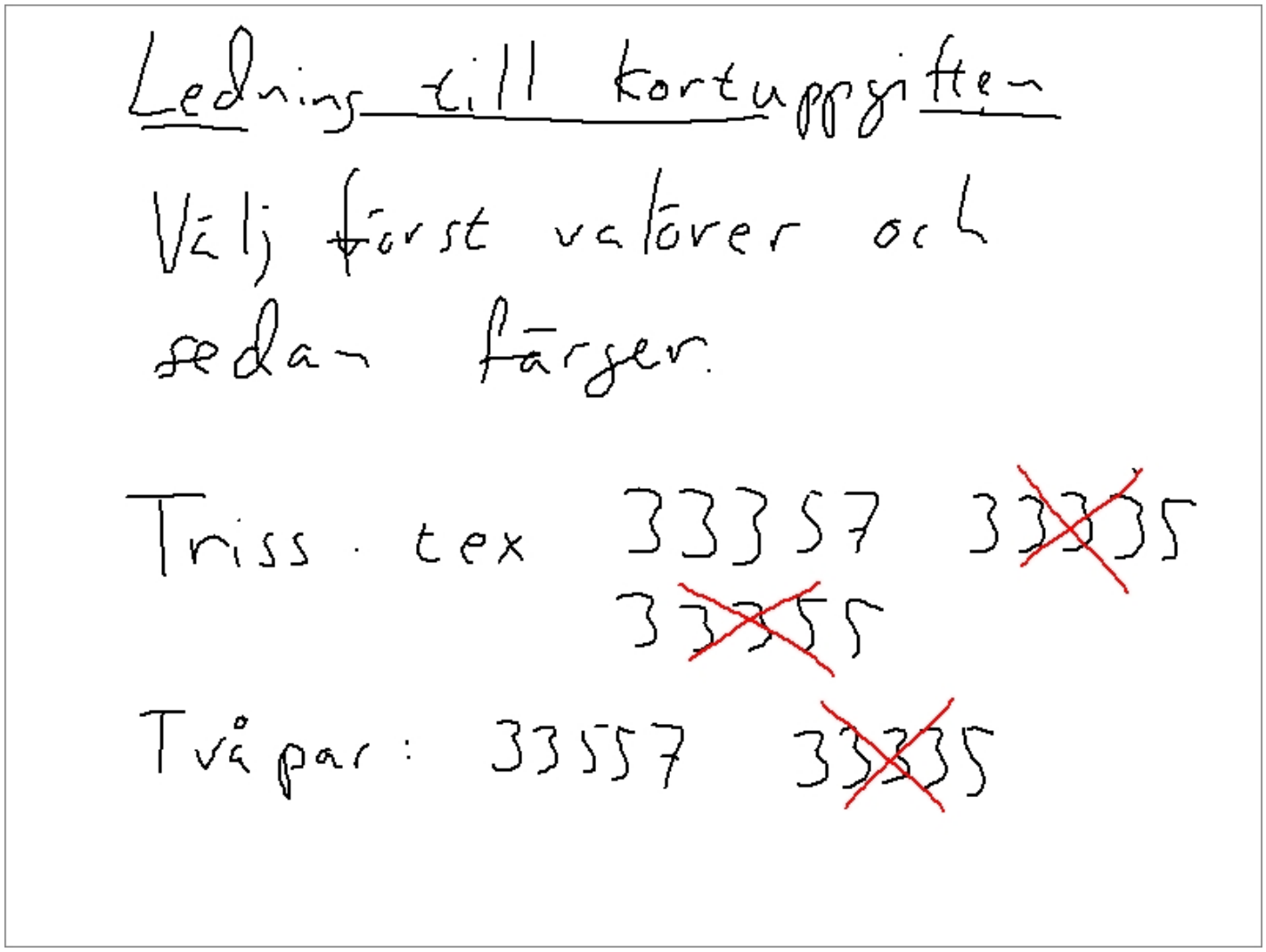
Ledning till kortuppgiften
Välj först valörer och
sedan färger.
Triss. tex 33357 33335
33355
Två par: 33557 33335

På hur många sätt kan vi få två par?

$$\binom{13}{2} \cdot 11 \cdot \binom{4}{2}\binom{4}{2} \cdot 4$$

$$\binom{13}{2}\binom{4}{2}\binom{4}{2}\,44$$

På hur många sätt kan vi få kåk?

$$13 \cdot 12 \cdot \binom{4}{3} \cdot \binom{4}{2}$$

På hur många sätt kan vi få triss?

$13 \cdot \binom{12}{2} \cdot \binom{4}{3} \cdot 4 \cdot 4$

33357

33375

På hur många sätt kan vi få fyrtal?

$13 \cdot \binom{4}{4} \cdot 12 \cdot 4$

33335

Givet nyckeln $n=22$ och $e=7$, dekryptera meddelandet 15.

Lösn: $n = 2 \cdot 11$. $m = (2-1)(11-1) = 10$

Vi vill hitta d så att $de \equiv 1 \pmod{10}$

$10 = 7 + 3$ $\quad 1 = 7 - 2(10-7)$

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

$\Rightarrow 1 = 3 \cdot 7 - 2 \cdot 10 \Rightarrow d = 3$

$15^3 \equiv 15 \cdot 15^2 \equiv 15 \cdot 225 \equiv 15 \cdot 5 \equiv 75 \equiv 9 \pmod{22}$

SVAR: 9

$n = 33$, $e = 7$, dekryptera meddelandet 12.

$n = 3 \cdot 11$, $m = (3-1)(11-1) = 20$

$20 = 2 \cdot 7 + 6$ $\quad 1 = 7 - (20 - 2 \cdot 7) = 3 \cdot 7 - 20$

$7 = 6 + 1$ $\quad 1 = 7 - 6$

så ifen $d = 3$.

$12^3 \equiv 12 \cdot 144 \equiv 12 \cdot 12 \equiv 144 \equiv 12 \pmod{33}$

$n=35$, $e=11$, dekryptera meddelandet 2.

$n=35=5\cdot 7$, $m=4\cdot 6=24$.

$24=2\cdot 11+2$ $\quad 1=11-5(24-2\cdot 11)$

$11=5\cdot 2+1$ $\quad 1=11-5\cdot 2$

$d=11 \Longleftarrow 1=11\cdot 11-5\cdot 24$

$2^{11}\equiv 2\cdot(2^5)^2\equiv 2\cdot 32^2\equiv 2\cdot(-3)^2\equiv 2\cdot 3^2\equiv$

$\equiv 2\cdot 9\equiv 18$ SVAR: 18.

$$(a+b)^p \equiv \binom{p}{0}a^p + \binom{p}{p}b^p \pmod p$$

$$\sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k \qquad \binom{p}{k} \equiv 0 \pmod p \quad 1 \le k \le p-1$$

$p \ge 2$ $\quad \binom{p}{2} = \frac{p\cdot(p-1)}{2} \qquad \frac{3\cdot 2}{2} = 3$

2 kan inte dela p för p primtal.

$$\binom{p}{k} = \frac{p\cdot(p-1)\cdot\ldots\cdot(p-k+1)}{k!}$$

$\Rightarrow$ ingen faktor kan dela p

$(\overset{a}{2}+\overset{b}{1})^5 \equiv 2^5+1^5 \pmod 5$

$\equiv 32+1 \equiv \underline{\underline{3}} \pmod 5$

$3^5 \equiv 3\cdot(3^2)^2 \equiv 3\cdot 9^2 \equiv 3\cdot(-1)^2 \equiv \underline{\underline{3}}$

$9 \equiv 4+5 \equiv 4 \equiv (-1)+5 \equiv -1$

Lös ekvationen $x^2+2x+2 \equiv 0 \pmod 5$

x	x^2+2x+2
0	$0+2\cdot 0+2=2$
1	$1+2+2=0$
2	$4+4+2=0$
3	$4+1+2=2$
4	$1+3+2=1$

$(x+1)^2+2-1=$

$=(x+1)^2+1$

$(x+1)^2 \equiv -1 \pmod 5$

$\equiv 4$

$(x+1)^2 \equiv 4 \pmod 5$

$x+1 \equiv \pm 2 \pmod 5$ [5 printed]

$x+1 \equiv 2 \Rightarrow x \equiv 1$

$x+1 \equiv -2 \Rightarrow x \equiv -3 = 2$

$x^2+3x+2 \equiv 0 \pmod 5$

Vi vill rikta: $\left(x+\frac{3}{2}\right)^2 + 2 - \frac{9}{4}$ $\quad 3 = 2^{-1}$ $\quad 2 \cdot 3 \equiv 1$

$4^2 \equiv 1 \Rightarrow 4^{-1} \equiv 4$

$\left(x+2^{-1}3\right)^2 + 2 - 4^{-1}9 \equiv$

$\equiv (x+4)^2 + 2 - 4 \cdot 4 \equiv (x+4)^2 + 2 - 1$

$\equiv (x+4)^2 + 1. \Rightarrow x+4 \equiv \pm 2$

x	x^2+3x+2
0	$0+0+2 \equiv 2$
1	$1+3+2 \equiv 1$
2	$4+1+2 \equiv 2$
3	$4+4+2 \equiv 0$
4	$1+2+2 \equiv 0$

$x+4 \equiv \pm 2$

$x \equiv 2-4 \equiv 3$

$x \equiv -2-4 \equiv 4$