Matematik, KTH **SF1679 Diskret matematik**
B.Ek **ht 2017**

Övning 1, må 6 november 2017
svar och ledningar

1a. $x = [1; 1, 1, \ldots] = 1 + \frac{1}{x}$ ger $x = \frac{1+\sqrt{5}}{2}$, gyllene snittet,
b. $x = [1; 2, 2, \ldots] = 1 + \frac{1}{y}$, där $y = [2; 2, 2, \ldots] = 2 + \frac{1}{y}$, $y = \sqrt{2} + 1$, $x = \sqrt{2}$,
c. $x = [1; 2, 1, 2, 1, \ldots] = 1 + \frac{1}{2+\frac{1}{x}} = 1 + \frac{x}{2x+1} = \frac{3x+1}{2x+1}$ och $x = \frac{1+\sqrt{3}}{2}$.

2. Om $\alpha = [a_0; a_1, a_2, \ldots]$ med $a_0 > 1$ är $\alpha^{-1} = [0; a_0, a_1, a_2, \ldots]$,
om $a_0 = 1$ med a_1 definierad är α^{-1} som ovan och $[1;]^{-1} = [1;]$,
då $a_0 = 0$ och a_1 existerar (dvs $\alpha \neq 0$) är $\alpha^{-1} = [a_1; a_2, a_3, \ldots]$.
Om $a_0 < 0$ är det svårare.

3. $76^{-1} = 32$ i $\mathbb{Z}_{221}$. (Euklides algoritm ger $1 = -11 \cdot 221 + 32 \cdot 76$).

4a. $x = 39$ ($13^{-1} = 5$ i $\mathbb{Z}_{64}$), **b.** $x = 1$, $y = 12$ (Gausselimination).

5. Möjliga är $b = 0$, 2, 6, 7, 11, 13, 14, 15, 16
($x^2 + 3x + b = (x + 10)^2 + 2 + b$ i $\mathbb{Z}_{17}$, så $15 - b$ måste vara en kvadrat i $\mathbb{Z}_{17}$).

6. $545^{112} \equiv_{23} 3$ och $545^{112} \equiv_{24} 1$
(Fermats lilla och Eulers satser eller $\mathbb{Z}_{24} \cong (\mathbb{Z}_8 \times \mathbb{Z}_3)$).

7. Ledning: för $a \in \mathbb{Z}_p \setminus \{0\}$ gäller $a = a^{-1}$ omm $a = \pm 1$.

8. $(\mathrm{sgd}(5k + 3, 3k + 2) = \mathrm{sgd}(3k + 2, (5k + 3) - (3k + 2)) = \mathrm{sgd}(3k + 2, 2k + 1) \ldots)$

9. De sökta lösningarna är $(41, -59)$, $(150, -216)$
(Euklides algoritm (alla lösningar är $n = 41 + 109k$, $m = -59 - 157k$)).

10. ($\mathrm{sgd}(a, b) = ma + nb$ ger $1 = m\frac{a}{\mathrm{sgd}(a,b)} + n\frac{b}{\mathrm{sgd}(a,b)}$, så ± 1 enda gemensam delare.)

11. Den felande siffran är 4
($\theta(2^{29}) \equiv_9 2^{29} \equiv_9 2^5 \equiv_9 5$ (ty $\mathrm{sgd}(2, 9) = 1$ och $\phi(9) = 6$) och $0 + 1 + \ldots + 9 \equiv_9 0$).

12. Ledningar: a. betrakta problemet i $\mathbb{Z}_3$, b. betrakta det i $\mathbb{Z}_5$,
c. betrakta i $\mathbb{Z}_4$, se att inte båda udda; om båda jämna, en av $\frac{a}{2}$, $\frac{b}{2}$ jämn;
om exakt en jämn, betrakta i $\mathbb{Z}_8$, ger $\not\equiv_4 2$.

13. Antalet lösningar är 8 (de är $x = \pm 1$, ± 89, ± 109, ± 199)
($\mathbb{Z}_{990} \cong (\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_{11})$).

14. Alla lösningar är $x = 9$, 11, 23, 25, 37, 39, 51, 53 ($\mathbb{Z}_{56} \cong (\mathbb{Z}_8 \times \mathbb{Z}_7)$).

15. Alla lösningar är $x = 397 + 648u$, $u \in \mathbb{Z}$
(t.ex. $x = 73 + 81t \equiv_8 5$ omm $t = 4 + 8u$, $u \in \mathbb{Z}$).

16. Om något $a_i \neq 0$: p^{n-1} lösningar (x_j:na, $j \neq i$, godtyckliga, ger x_i),
om alla $a_i = 0$: p^n lösningar (om $b = 0$) eller inga lösningar (om $b \neq 0$).

17. $E(718) = 707$, $E(719) = 615$, $d = 467$
(eftersom $\mathrm{mgm}(30, 42) = 210$ fungerar alla $d = 47 + 210n$, $n \in \mathbb{N}$).

18. ($2^{62} \equiv_{63} (2^6)^{10} \cdot 2^2 \equiv_{63} 1^{10} \cdot 4 \not\equiv_{63} 1$.)

19a. $\mathcal{C} = \{000000, 110001, 101010, 011011, 011100, 101101, 110110, 000111\}$,
b. 011011 sändes (antagligen, det kan ha varit mer än ett fel också), c. 8 st.

20. En bra strategi är att passa om man ser två olikfärgade hattar och gissa på motsatt färg om man ser två likfärgade.
(De vinner då omm inte alla hattar har samma färg, så med sannolikhet $\frac{3}{4}$. Varje person gissar rätt och fel med samma sannolikhet, men strategin får dem att alla gissa fel vid samma färgfördelning (alla hattar likfärgade) och aldrig rätt samtidigt. (Om person i gissar rätt och fel med vardera sannolikhet p_i är sannolikheten att de lyckas $\leq \min(\sum p_i, 1 - \max p_i)$, så bättre går inte.)
7 personer kan lyckas med sannolikhet $\frac{7}{8}$, 15 med sannolikhet $\frac{15}{16}$ osv.
Hur kan deras strategier formuleras med hjälp av hammingkoder?)