

Övning 1, må 6 november 2017

1. Finn värdena för följande enkla kedjebråk:
 - a. $[1; 1, 1, 1, 1, \dots]$,
 - b. $[1; 2, 2, 2, 2, \dots]$,
 - c. $[1; 2, 1, 2, 1, 2, \dots]$.
2. Om $\alpha \in \mathbb{R}$ har kedjebråksutvecklingen $[a_0; a_1, a_2, \dots]$, kan du finna utvecklingen för α^{-1} ?
3. Finn inversen till elementet 76 i ringen $\mathbb{Z}_{221}$.
- 4a. Lös ekvationen $13x + 18 = 13$ i ringen $\mathbb{Z}_{64}$.
- b. Lös $\begin{cases} 7x + 2y = 5 \\ 10x + 7y = 3 \end{cases}$ i ringen $\mathbb{Z}_{13}$.
5. Finn alla element b i $\mathbb{Z}_{17}$ sådana att för minst ett $x \in \mathbb{Z}_{17}$:
$$x^2 + 3x + b = 0.$$
6. Finn $545^{112} \pmod{23}$ och $545^{112} \pmod{24}$ (dvs 545^{112} i $\mathbb{Z}_{23}$ resp. $\mathbb{Z}_{24}$).
7. Visa att om p är ett primtal så gäller
$$(p-1)! \equiv -1 \pmod{p}.$$
8. Visa att för alla $k \in \mathbb{Z}$ är $3k+2$ och $5k+3$ relativt prima.
9. Finn alla heltal n och m sådana att $314n + 218m = 12$ och $0 \leq n \leq 200$.
10. Visa att för alla $a, b \in \mathbb{Z}$ är heltalen $\frac{a}{\text{sgd}(a,b)}$ och $\frac{b}{\text{sgd}(a,b)}$ relativt prima.
11. 2^{29} har (i bas 10) 9 siffror, alla olika. Vilken siffra fattas?
12. Kalla en trippel heltal (a, b, c) för en **pythagoreisk trippel** om $a^2 + b^2 = c^2$, dvs om a, b, c är (mätetal för) sidorna i en rätvinklig triangel. Exempel på pythagoreiska trippler är $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$ och $(3312, 16766, 17090)$. Visa att om (a, b, c) är en pythagoreisk trippel måste
 - a. minst en av a och b vara delbar med 3,
 - b. minst en av a, b och c vara delbar med 5,
 - c. minst en av a och b vara delbar med 4.
13. Finn antalet lösningar till ekvationen $x^2 = 1$ i ringen $\mathbb{Z}_{990}$.
14. Lös ekvationen $(x+3)(x+5) = 0$ i ringen $\mathbb{Z}_{56}$.
15. Finn alla $x \in \mathbb{Z}$ sådana att $x \equiv 5 \pmod{8}$ och $x \equiv 73 \pmod{81}$.
16. För p ett primtal och $a_1, a_2, \dots, a_n, b \in \mathbb{Z}_p$, finn antalet lösningar $(x_1, x_2, \dots, x_n) \in (\mathbb{Z}_p)^n$ till ekvationen
$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b.$$
17. Givet ett RSA-kryptosystem med $n = 1333 (= 31 \cdot 43)$ och $e = 143$, kryptera meddelandena $x = 718$ och $x = 719$.
Kontrollera resultaten genom att finna ett värde för d och avkryptera.

18. Använd ett fermattest för att visa att talet 63 inte är ett primtal.

19. Matrisen $\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$ är kontrollmatris för en 1-felsrättande kod $\mathcal{C}$.

a. Finn alla element i $\mathcal{C}$.

b. Rätta ordet 011111.

c. Hur många ord kan inte rättas?

20. Tre personer får veta att de samtidigt skall få varsin hatt på huvudet, var och en med sannolikhet $\frac{1}{2}$ en röd och sannolikhet $\frac{1}{2}$ en blå hatt, de olika hattarnas färger oberoende. De kan se de två andras hattar, men inte sin egen. De ges chansen att gissa färgen på sin egen hatt, men kan avstå från att gissa om de vill. Om (och endast om) minst en gissar rätt färg på sin egen hatt och ingen gissar fel, får de (alla) ett pris. De får inte veta om eller vad de övriga gissar.

Hur stor sannolikhet att vinna kan de få, om de i förväg kan komma överens om en strategi för gissandet? Om de t.ex. bestämmer att A skall gissa "röd" och att B och C skall avstå, har de tydligen sannolikheten $\frac{1}{2}$ att vinna, men kan de öka sannolikheten?

Hur stor sannolikhet kan en bra strategi ge om de är femton personer?