Lösningsförlag till inlämningsuppgifter vecka 3

Uppgift 1 Bestäm inverserna till samtliga inverterbara element i $\mathbf{Z}_a$.

Lösning: I mitt fall är $a = 21$, så det är det inverterbara elementen i $\mathbf{Z}_{21}$ som skall inverteras. Elementen är inverterbara om de saknar gemensamma delare med $23 = 3 \cdot 7$. Alltså är de inverterbara elementen de heltal mellan 1 och 21 som inte är delbara med vare sig 3 eller 7. Vi får $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 21\}$.

Vi börjar med att invertera 2 med hjälp av Euklides algoritm.

$$21 \quad = 10 \cdot 2 + 1$$

och baklänges ger det att $1 = 21 - 10 \cdot 2$ och inversen till 2 är $-10 \equiv 11 \pmod{21}$.

Efter att ha fått fram inversen till 2 får vi inversen till potenser av 2, genom att ta potenser av inversen till 2. Vi får $4^{-1} = 11^2 \equiv 16 \pmod{21}$, $8^{-1} = (2^{-1})^3 = 11 \cdot 16 \equiv 8 \pmod{21}$, $16^{-1} = (2^{-1})^4 = 8 \cdot 11 = 4$ och $11^{-1} = 32^{-1} = 4 \cdot 11 \equiv 2 \pmod{21}$.

Ett annat sätt att få inverser från det vi redan känner till är genom att $(-a)^{-1} = -a^{-1}$. På det sättet får vi $19^{-1} = -2^{-1} = 10$, $17^{-1} = -4^{-1} = -16 \equiv 5 \pmod{21}$, $13^{-1} = -8^{-1} = -8 \equiv 13 \pmod{21}$, $5^{-1} = -16^{-1} = -4 \equiv 17 \pmod{21}$ och $10 = -11^{-1} = -2 \equiv 19 \pmod{21}$.

Till slut vet vi att $1^{-1} = 1$ och därmed också $(-1)^{-1} = -1^{-1} = -1 \equiv 20 \pmod{21}$.

Vi har nu fått alla inverser. $1^{-1} = 1$, $2^{-1} = 11$, $4^{-1} = 16$, $5^{-1} = 17$, $8^{-1} = 8$, $10^{-1} = 19$, $11^{-1} = 2$, $13^{-1} = 13$, $16^{-1} = 4$, $17^{-1} = 5$, $19^{-1} = 10$ och $20^{-1} = 20$.

Uppgift 2 Dekryptera meddelandet x i ett RSA-system med öppen nyckel n och e.

Lösning: I vårt fall är $x = 1151246$, $n = 1323037$ och $e = 1123$. För att kunna få den hemliga nyckeln d som behövs för dekryptering vill vi faktorisera n som $p \cdot q$. Eftersom n inte är mycket större än en miljon kan inte den minsta primfaktorn vara mycket större än ett tusen, som är roten ur en miljon. Vi prövar oss fram med de primtal som är högst 1200 och ser att n är delbart med 1109 och 1193. Vi har på det viset hittat både p och q och kan bestämma m som $(p-1)(q-1) = 1320736$. Vi behöver inverstera e modulo m för att finna d. Vi använder Euklides algoritm och får

$$\begin{aligned} 1320736 &= 1176 \cdot 1123 + 88 \\ 1123 &= 12 \cdot 88 + 67 \\ 88 &= 1 \cdot 67 + 21 \\ 67 &= 3 \cdot 21 + 4 \\ 21 &= 5 \cdot 4 + 1 \end{aligned}$$

och räknar vi baklänges får vi

$$\begin{aligned} 1 &= 21 - 5 \cdot 4 == 21 - 5 \cdot (67 - 3 \cdot 21) = 16 \cdot 21 - 5 \cdot 67 \\ &= 16 \cdot (88 - 1 \cdot 67) - 5 \cdot 67 = 16 \cdot 88 - 21 \cdot 67 \\ &= 26 \cdot 88 - 21 \cdot (1123 - 12 \cdot 88) = 268 \cdot 88 - 21 \cdot 1123 \\ &= 268 \cdot (1320736 - 1176 \cdot 1123) - 21 \cdot 1123 \\ &= 268 \cdot (1320736 - 1176 \cdot 1123) - 315189 \cdot 1123 \end{aligned}$$

Alltså är $d = -315189 \equiv 1005547 \pmod{1320736}$.

Vi behöver nu använda metoden med successiv kvadrering för att beräkna $D(x) = x^d$ i $\mathbf{Z}_n$. Först skriver vi d i binär form, vilket vi kan göra genom att successivt dela med 2. Sedan beräknar vi successiva kvadrater. Till slut multiplicerar vi ihop de potenser som svarar mot ettorna i binärframställningen av d. Allt detta kan göras i en enda slinga, som exempelvis i följande Javakod.

```
public class RSA{

  public static void main (String argv[]){
    int n= 1323037;
    int d= 1005547;
    int x= 1151246;
    long resultat=1;
    long potens=x;
    for (int i=d;i>0;i=i/2){
      if (i%2==1)
        resultat = (resultat*potens)%n;
      potens=(potens*potens)%n;
    }
    System.out.println("D(x) = "+resultat);
  }
}
```

som ger utskriften

```
D(x) = 1193001
```

Alltså är det dekrypterade meddelandet 1193001.

Uppgift 3 Visa att Stirlingtalet $S_{k,4}$ ges av $(4^{k-1} - 1)/6 + (2^{n-1} - 3^{n-1})/2$ för alla $k \geq 4$.

Lösning: Eftersom antalet surjektiva funktioner från en mängd med k element till en mängd med 4 element ges av $4!S_{k,4}$ kan vi beräkna Stirlingtalet genom att räkna surjektiva funktioner. Detta kan vi göra med hjälp av sållprincipen. Mängden av alla funktioner från $\{1, 2, \ldots, k\}$ till $\{1, 2, 3, 4\}$ betecknar vi M och delmängderna A_1, A_2, A_3 och A_4 definierar vi genom

$$A_i = \{f \in M \mid f(x) \neq i \text{ för } x = 1, 2, \ldots, k.\}$$

dvs de funktioner som missar talet i. De surjektiva funktionerna är komplementet till unionen av dessa fyra mängder. Vi använder sållprincipen för att beräkna antalet element i unionen. Vi får $\alpha_1 = |A_1| + |A_2| + |A_3| + |A_4| = 4 \cdot 3^k$, eftersom A_i är mängden av funktioner från $\{1, 2, \ldots, k\}$ till en mängd med 3 element. Vidare är $\alpha_2 = |A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4| + |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4| = 6 \cdot 2^k$, eftersom varje $A_i \cap A_j$ är funktioner till en mängd med två element. $\alpha_3 = |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| = 4 \cdot 1^k = 4$, eftersom varje term är antalet funktioner till en mängd med ett element. $\alpha_4 = |A_1 \cap A_2 \cap A_3 \cap A_4| = 0$, eftersom det inte finns någon funktion till en mängd med noll element.

Sammantaget får vi $|A_1 \cup A_2 \cup A_3 \cup A_4| = \alpha_1 - \alpha_2 + \alpha_3 - \alpha_4 = 4 \cdot 3^k - 6 \cdot 2^k + 4 \cdot 1 - 0$. Eftersom det totalt finns 4^k funktioner i M får vi att $4^k - (4 \cdot 3^k - 6 \cdot 2^k + 4 \cdot 1) = 4^k - 4 \cdot 3^k + 6 \cdot 2^k - 4 \cdot 1$ funktioner är surjektiva. Stirlingtalet $S_{k,4}$ får vi nu genom att dela med $4! = 24$. Alltså

$$S_{k,4} = \frac{1}{24}(4^k - 4 \cdot 3^k + 6 \cdot 2^k - 4 \cdot 1) = \frac{1}{6}(4^{k-1} - 1) + \frac{1}{2}(2^{k-1} - 3^{k-1})$$

vilket skulle visas.

Uppgift 4 Hur många permutationer p i S_m är involutioner, dvs uppfyller $p^2 = id$?

Lösning: Vi kan försöka skapa en rekursion för a_m, antalet involutioner i S_m. Om $m = 1$ finns en permutation och den är en involution och för $m = 2$ finns två permutationer som båda är involutioner. Alltså är $a_1 = 1$ och $a_2 = 2$. Om vi nu ser på involutionerna i S_m kan vi dela in dem i två delar. Den ena delen består av de involutioner p som uppfyller $p(m) = m$, dvs de som fixerar m. Då permuteras de övriga $m - 1$ elementen för sig och vi får en involution på mängden $\{1, 2, \ldots, m-1\}$. Resterande involutioner sänder m till något annat tal i, men eftersom de är involutioner måste vi ha att $p(i) = m$, eftersom $p(p(m)) = m$. Alltså permuteras övriga $m - 2$ element för sig och vi får en involution på mängden $\{1, 2, \ldots, m\} \setminus \{i, m\}$. Sammantaget har vi delat upp mängden av involutioner i S_m i två delar, där den ena delen har a_{m-1} element och den andra $(m-1)a_{m-2}$ element, eftersom det finns $m-1$ olika sätt att välja $i = p(m)$. Vår rekursion blir alltså

$$a_m = a_{m-1} + (m-1)a_{m-2}$$

för $m \geq 3$. Sätter vi in begynnelsevärdena får vi

$$\begin{aligned}
a_3 &= a_2 + 2a_1 = 2 + 2 \cdot 1 = 4 \\
a_4 &= a_3 + 3a_2 = 4 + 3 \cdot 2 = 10 \\
a_5 &= a_4 + 4a_3 = 10 + 4 \cdot 4 = 26 \\
a_6 &= a_5 + 5a_4 = 26 + 5 \cdot 10 = 76 \\
a_7 &= a_6 + 6a_5 = 76 + 6 \cdot 26 = 232 \\
a_8 &= a_7 + 7a_6 = 232 + 7 \cdot 76 = 764 \\
a_9 &= a_8 + 8a_7 = 764 + 8 \cdot 232 = 2620 \\
a_{10} &= a_9 + 9a_8 = 2620 + 9 \cdot 764 = 9496 \\
a_{11} &= a_{10} + 10a_9 = 9496 + 10 \cdot 2620 = 35696 \\
a_{12} &= a_{11} + 11a_{10} = 35696 + 11 \cdot 9496 = 140152
\end{aligned}$$