Stockholms Universitet
Institutionen för Data och Systemvetenskap
Johan Andersson

Diskret Matematik
Vårterminen 2012
2012-02-06

Inlämningsuppgifter - Omgång 2

Inlämningsuppgifterna skall lösas *individuellt* samt lämnas senast i samband med föreläsningen Onsdagen den 15:e Februari, alternativt om ni vill skriva på datorn eller scanna in era lösningar, mejlas in till `jander@dsv.su.se`, senast midnatt natten mot Torsdagen. Fullständiga lösningar skall lämnas in. Ni skall vara beredda att presentera era lösningar på en muntlig gruppexamination Fredagen den 17:e Februari eller Måndagen den 20:e Februari. Exakt Gruppindelning kommer att meddelas senare.

Talteori

1. Skriv talen 17 och 101 på binär form (med basen 2).
2. Skriv talen $(503)_6$ samt $(1121)_4$ på decimalform (med basen 10).
3. Beräkna SGD$(2^{100} \cdot 3^{20}, 2^5 \cdot 5^{10} \cdot 7^5)$.
4. Beräkna SGD(1422,891) med hjälp av Euklides algoritm.
5. (a) Bestäm sistasiffran i talet $5 \cdot 7^{40} + 3$.
   (b) Bestäm den minsta ickenegativa resten av 2^{100} vid division med 13?
6. (Detta tal berör RSA-algoritmen för kryptering i ett förenklat exempel. I ett riktigt exempel så skulle Ada välja betydligt större primtal än $p = 5$ samt $q = 7$)

   Ada finner primtalen $p = 5$ samt $q = 7$ vilket ger $N = pq = 5 \cdot 7 = 35$. Hon bestämmer sig att hon vill använda krypteringsnyckeln $e = 7$. En dekrypteringsnyckel d kan beräknas genom att lösa den Diofantiska ekvationen

   $$7d - 24q = 1,$$

   där 7 kommer från $e = 7$ samt talet 24 kommer ifrån att $24 = (p-1)(q-1) = 4 \cdot 6$. Bernt krypterar meddelandet $x = 2$ genom att beräkna $y \equiv x^e \equiv 2^7 \pmod{35}$ där $0 \leq y < 35$.

   (a) Bestäm y.
   (b) Beräkna en dekrypteringsnyckel d.
   (c) Ada dekrypterar Bernts meddelande genom att beräkna $z \equiv y^d \pmod{35}$ där $0 \leq z < 35$. Visa att $z = x = 2$.

7. Bevisa att talet 73 är ett primtal.

8. Bevisa att $\sqrt{7}$ är ett irrationellt tal.

9. Bevisa Fermats lilla sats för primtalet $p = 5$, dvs att $n^5 \equiv n \pmod 5$ för alla heltal n.

Relationer

1. Låt R vara en relation på A. Avgör om följande relationer är ekvivalensrelationer

   (a) Låt $A = \mathbb{Z} \times \mathbb{Z}$.

      i. $(a, b)R(c, d)$ om och endast om $a = c$.

      ii. $(a, b)R(c, d)$ om och endast om $a = c$ eller $b = d$.

      iii. $(a, b)R(c, d)$ om och endast om $a = c$ och $b = d$.

   (b) Låt A vara mängden av svenska medborgare.

      i. aRb om och endast om a och b har samma födelsedag.

      ii. aRb om och endast om de känner varandra.

2. Avgör om relationen $R = \{(1, 1), (2, 1), (1, 2), (3, 3)\}$ på mängden $A = \{1, 2, 3\}$ är reflexiv, symmetrisk, respektive transitiv.

3. Avgör vilka av följande relationer R på mängden $A = \{1, 2, 3, 4\}$ som bestämmer en funktion:

   (a) $\{(1, 2), (2, 2), (3, 2), (4, 2)\}$,

   (b) $\{(2, 1), (2, 2), (2, 3), (2, 4)\}$,

   (c) $\{(1, 2), (2, 2), (3, 2), (3, 3), (4, 2)\}$,

   (d) $\{(3, 1), (2, 2), (4, 2), (1, 3)\}$,

   (e) $\{(3, 1), (2, 2), (4, 2), (4, 4)\}$.

4. Låt för en funktion $f : \mathbb{Z} \to \mathbb{Z}$, relationen R vara funktionens graf, dvs $R = \{(x, f(x)) : x \in \mathbb{Z}\}$. Bestäm alla funktioner f så att R är en ekvivalensrelation. Vilka blir ekvivalensklasserna?