Stockholms Universitet
Institutionen för Data och Systemvetenskap
Johan Andersson

Diskret Matematik
Vårterminen 2012
2012-02-27

Lösningsförslag Inlämningsuppgifter - Omgång 2

Talteori

1. Skriv talen 17 och 101 på binär form (med basen 2).

   Svar. Vi har att tvåpotenserna $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$. Vi får att

   (a) $17 = 16 + 1 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 10001_2$.

   (b) $101 = 64 + 37 = 64 + 32 + 5 = 64 + 32 + 4 + 1 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 1000101_2$.

   Notering: Ett alternativt sätt att lösa uppgiften ovan är att använda divisionsalgoritmen för division med 2. De binära siffrorna blir då de succesiva resterna och kommer "i andra ordningen" från ovan.

2. Skriv talen $(503)_6$ samt $(1121)_4$ på decimalform (med basen 10).

   Svar.

   (a) $(503)_6 = 5 \cdot 6^2 + 0 \cdot 6^1 + 3 \cdot 6^0 = 5 \cdot 36 + 3 = 180 + 3 = 183$.

   (b) $(1121)_4 = 1 \cdot 4^3 + 1 \cdot 4^2 + 2 \cdot 4^1 + 1 \cdot 4^0 = 1 \cdot 64 + 1 \cdot 16 + 2 \cdot 4 + 1 \cdot 1 = 64 + 16 + 8 + 1 = 89$.

3. Beräkna $\mathrm{SGD}(2^{100} \cdot 3^{20}, 2^5 \cdot 5^{10} \cdot 7^5)$.

   Svar. Eftersom talen redan är primtalsfaktoriserade så blir uppgiften enkel (vi slipper använda till exempel Euklides algoritm) och det räcker att identifiera vilka primtal som finns i båda talen. Det enda primtal som finns på båda sidor om kommatecknet är 2, och den lägsta potensen av 2 som förekommer är 2^5. Svaret blir alltså $2^5 = 32$.

4. Beräkna $\mathrm{SGD}(1422, 891)$ med hjälp av Euklides algoritm.

   Svar. Euklides algoritm ger

$$
\begin{aligned}
1422 &= 891 + 531, \\
891 &= 531 + 360, \\
531 &= 360 + 171, \\
360 &= 2 \cdot 171 + 18, \\
171 &= 7 \cdot 18 + 9, \\
18 &= 2 \cdot 9 + 0.
\end{aligned}
$$

Vi får att $\text{SGD}(1422, 891) = 9$, vilket är den sista icke-försvinnande resten.

5. (a) Vad blir sistasiffran i talet $5 \cdot 7^{40} + 3$.

   Svar. Eftersom $5 \cdot 7^{40}$ är ett udda tal som är delbart med 5 så blir sista-siffran 5. Lägger vi till 3 så blir sistasiffran alltså 8.

   (b) Vad blir den minsta ickenegativa resten av 2^{100} vid division med 13?

   Svar. Vi har att $2^{100} \equiv (2^4)^{25} = 16^{25} \equiv 3^{25} \pmod{13}$. Vi noterar att $3^3 = 27 = 2 \cdot 13 + 1 \equiv 1 \pmod{13}$. Från detta får vi att $3^{25} = 3^{3 \cdot 8 + 1} = (3^3)^8 \cdot 3 \equiv 1^8 \cdot 3 \equiv 3 \pmod{13}$, dvs vi får den minsta ickenegativa resten 3.

6. (Detta tal berör RSA-algoritmen 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.

   Svar. Uträkningen $2^7 = 128 \equiv 128 - 3 \cdot 35 = 23 \pmod{35}$ ger att $y = 23$.

   (b) Beräkna en dekrypteringsnyckel d.

   Svar. Vi använder Euklides algoritm

   $$24 = 3 \cdot 7 + 3,$$
   $$7 = 2 \cdot 3 + 1.$$

   Genom att räkna baklänges så ser vi att $1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (24 - 3 \cdot 7) = (1 + (-2) \cdot (-3)) \cdot 7 - 2 \cdot 24 = 7 \cdot 7 - 2 \cdot 24$. Detta ger $d = 7$.

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

   Svar. Vi har att $z \equiv y^d \equiv 23^7 \equiv (-12)^7 = (-12)^{2 \cdot 3 + 1} = ((-12)^2)^3 \cdot (-12) = 144^3 \cdot (-12) \equiv (144 - 4 \cdot 35)^3 \cdot (-12) = 4^3 \cdot (-12) = 64 \cdot (-12) \equiv (-6) \cdot (-12) = 72 \equiv 2 \pmod{35}$. Detta bevisar att $z = 2 = x$.

7. Bevisa att talet 73 är ett primtal.

   Svar. Om 73 är sammansatt så måste 73 ha minst en primfaktor mindre än $\sqrt{73}$. Allstså räcker det att visa att 73 ej är delbart med $2, 3, 5$ eller 7.

Eftersom sistasiffran är udda så är 73 ej delbart med 2. Siffersumman i talet blir $7+3 \equiv 1 \pmod 3$. Alltså är 73 ej delbart med 3. 73 är ej heller delbart med 5 eftersom sistasiffran inte är 5 eller 0. Från $73 = 7 \cdot 10 + 3$ så ser vi att 73 ej heller är delbart med 7. Alltså är 73 ett primtal.

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

   Svar. Antag att $\sqrt{7}$ är rationellt. Då kan vi skriva $\sqrt{7} = \frac{p}{q}$ där $\text{SGD}(p, q) = 1$ eftersom varje bråktal kan skrivas på förkortad form. Kvadrering ger

   $$7 = \frac{p^2}{q^2}.$$

   Multiplikation av båda leden i likheten med q^2 ger oss att

   $$7q^2 = p^2.$$

   Eftersom 7 delar vänsterledet så följer det att 7 även delar högerledet, dvs $7|p^2$. En känd sats säger att om för ett primtal P, $P|ab$ så har vi att $P|a$ eller $P|b$. Tillämpning av den satsen med $P = 7$, $a = p$ och $b = p$ ger oss att $7|p$, dvs $p = 7k$. Insättning av detta i ekvationen ger oss att $7q^2 = (7k)^2$, dvs $7q^2 = 7^2k^2$, vilket efter förkortning med 7 ger oss att

   $$q^2 = 7k^2.$$

   Samma argument som ovan ger oss nu att $7|q$. Alltså har vi att $7|q$ samt $7|p$ vilket motsäger att $\text{SGD}(p, q) = 1$. Detta innebär att vårt första antagande måste vara felaktigt, dvs det är fel att $\sqrt{7}$ är ett rationellt tal, dvs $\sqrt{7}$ 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.

   Svar. Om n är ett heltal så tillhör n en av fem möjliga kongruensklasser modulo 5. Det räcker att testa alla de fem möjliga fallen för vilka vi får

   (a) $n \equiv 0 \pmod 5$: $n^5 \equiv 0^5 \equiv 0 \equiv n \pmod 5$. OK!

   (b) $n \equiv 1 \pmod 5$: $n^5 \equiv 1^5 \equiv 1 \equiv n \pmod 5$. OK!

   (c) $n \equiv 2 \pmod 5$: $n^5 \equiv 2^5 = 32 \equiv 2 \equiv n \pmod 5$. OK!

   (d) $n \equiv 3 \equiv -2 \pmod 5$: $n^5 \equiv (-2)^5 = -32 \equiv -2 \equiv n \pmod 5$. OK!

   (e) $n \equiv 4 \equiv -1 \pmod 5$: $n^5 \equiv (-1)^5 \equiv -1 \equiv n \pmod 5$. OK!

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 $a = c$.
      Svar. Vi undersöker relationen map reflexivitet, symmetri samt transitivitet.

         A. Reflexivitet: $(a, b)R(a, b)$ är sant eftersom $a = a$. OK!

         B. Symmetri: Om $(a, b)R(c, d)$ så är $a = c$ och alltså även $c = a$ varför även $(c, d)R(a, b)$. OK!

         C. Transitivitet: Om $(a, b)R(c, d)$ och $(c, d)R(e, f)$ så är $a = c$ och $c = e$ vilket från transitiviteten för vanliga likhetsrelationen medför att $a = e$ och $(a, b)R(e, f)$. OK!

      Relationen är en ekvivalensrelation.

      ii. $(a, b)R(c, d)$ om och endast om $a = c$ eller $b = d$.
      Svar. Relationen är ej transitiv, vilket kan ses av följande exempel $(1, 2)R(1, 3)$ samt $(1, 3)R(2, 3)$ men vi har inte att $(1, 2)R(2, 3)$. Detta ger att R ej är en ekvivalensrelation.

      iii. $(a, b)R(c, d)$ om och endast om $a = c$ och $b = d$.
      Svar. Relationen blir precis den vanliga likhetsrelationen "=" på mängden $\mathbb{Z} \times \mathbb{Z}$. Likhetsrelationen är en välkänd ekvivalensrelation.

   (b) Låt A vara mängden av svenska medborgare.

      i. aRb om och endast om a och b har samma födelsedag.
      Svar. Vi undersöker relationen map reflexivitet, symmetri samt transitivitet.

         A. Reflexivitet: Vi har att aRa eftersom en person a har samma födelsedag som sig själv. OK!

         B. Symmetri: Om aRb dvs a har samma födelsedag som b så har b givetvis samma födelsedag som a dvs bRa. OK!

         C. Transitivitet: Om a har samma födelsedag som b och b har samma födelsedag som c så har a samma födelsedag som c. OK!

      Relationen är en ekvivalensrelation.

      ii. aRb om och endast om de känner varandra.
      Svar. Relationen är inte transitiv eftersom att om a känner b och b känner c så behöver a inte känna c. Därför är relationen inte en ekvivalensrelation.

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

   (a) Reflexivitet: Vi har inte att $2R2$, därför är relationen inte reflexiv.

   (b) Symmetri: $1R1 \implies 1R1$ OK!, $2R1 \implies 1R2$ OK!, $1R2 \implies 2R1$ OK!, $3R3 \implies 3R3$ OK!. Relationen är symmetrisk.

   (c) Transitivitet: Relationen är ej transitiv eftersom $2R1$ och $1R2$ men inte $2R2$

3. Vilka av följande relationer R på mängden $A = \{1,2,3,4\}$ 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) $\{(3,1),(2,2),(4,2),(4,4)\}$.

   Svar. *a*) och *d*) är funktioner, eftersom varje element i A ger ett unikt element element i A. *b*) är inte en funktion eftersom $2R2$ och $2R3$ skulle ge både att $f(2) = 2$ samt $f(2) = 3$ vilket är omöjligt. *c*) är inte en funktion eftersom $3R2$ och $3R3$ skulle ge både att $f(3) = 2$ samt $f(3) = 3$ vilket är omöjligt. *e*) är inte en funktion eftersom $4R2$ och $4R4$ skulle ge både att $f(4) = 2$ samt $f(4) = 4$ vilket är omöjligt.

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?

   Svar. Från reflexivitet nRn fås att $f(n) = n$. Eftersom en funktion måste anta ett unikt funktionsvärde bestämmer detta funktionen fullständigt. Relationen R blir då likhetsrelationen "=" på mängden $\mathbb{Z}$. Detta är en välkänd ekvivalensrelation och ekvivalensklasserna blir mängder med ett element, dvs $\{n\}$ för $n \in \mathbb{Z}$.