INLÄMNINGSUPPGIFT, DISKRET MATEMATIK HT 12

Namn: _____

Personnummer: _____

Följande uppgift ska lösas. Uppgiften betygssätts med 0-12 poäng, eventuellt fördelade på flera deluppgifter.För godkänt resultat krävs 6 av 12 poäng.

För denna inlämningsuppgift är den huvudsakliga redovisningen lösningsgången, inte svaret. Hur korrekt, hur fullständig och vilken kvalitet lösningen och dess presentation har är mycket mer avgörande för poängsättningen än själva svaret. Svaret ska dock naturligtvis vara med i lösningen. Lösningarna ska vara renskrivna och väl motiverade. Jag kommer att lägga ännu större vikt på detta vid bedömningen av inl.uppgiftlösningar än vid bedömningen av duggalösningar.

Talteori, Matriser

1. I den här uppgiften ska vi genomföra lite RSA-kryptering. (6p)

   Välj som p och q i algoritmen de två största primtalen mindre än eller lika med årtalssiffrorna i ditt personnummer. Välj som talet e i algoritmen det största heltal mindre än eller lika med månadstalet i ditt personnummer som uppfyller villkoren i RSA-algoritmen.

   Med dessa parametrar för RSA-algoritmen bestämda, kryptera meddelandet som består av dina initialer så att meddelandet har två bokstäver. (har du mer än ett förnamn/efternam väljer du initialerna för första förnamnet och första efternamnet). Omvandlingen av meddelandet till en siffra görs genom den klassiska kodningen A$\leftrightarrow$ 1, B$\leftrightarrow$ 2 … Z$\leftrightarrow$ 26, Å$\leftrightarrow$ 27, Ä$\leftrightarrow$ 28, Ö$\leftrightarrow$ 29.

   När du erhållit det krypterade meddelandet, dekryptera detta med dekrypteringsmetoden som hör till RSA-kryptot. Svaret är redan känt, så det är stegen i dekrypteringen som är det intressanta, men genomför det helt till det dekrypterade meddelandet.

2. Betrakta mängden av alla positiva heltal som bara består av ettor (de 4 första talen av denna typ är 1,11,111 och 1111). Vilka av alla dessa tal är delbara med 9? Fullständig motivering krävs. (4p)

3. Beräkna den boolska matrispotensen $A^{[100]}$ där (2p)

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Lycka till! från Jan-Olav och Mikael

ENGLISH VERSION

The following problem are to be be solved. The problem is graded with 0-12 points, which might be distributed among several subproblems. To pass this moment you must have at least 6 out of 12 points.

For this home exercise the most important thing to present is the solution, not the answer. How correct and complete the solution is and what quality the solution and its presentation has is much more significant for the final scoring than the answer itself. But of cause the answer is to be part of the solution.
The solutions must be well written and well motivated. I will put even more emphasis on this for the home exercise than for the duggas.

Numbeer theory, Matrices

1. In this part we are going to work a little with the RSA-cryptation. (6p)

   Chose p and q in the algorithm to be the two largest primes less than or equal to the number representing the year of birth in your swedish personal number/id number. Choose the number e in the algorithm as the largest integer less than or equal to the number representing the month of birth in your swedish personal number/id number that satisfies the conditions in the RSA-algorithm.

   With these parameters for the RSA-algoritmen decided, encrypt the message consisting of your initials so that the message has two letters (if you have more than one first or family name you chose the initials for the first first name and the first family name). The transformation of the message to a number is done with the classical coding A$\leftrightarrow$ 1, B$\leftrightarrow$ 2... Z$\leftrightarrow$ 26, Å$\leftrightarrow$ 27, Ä$\leftrightarrow$ 28, Ö$\leftrightarrow$ 29.

   When you recieve the encrypted message, decrypt it with the decryption method corresponding to the RSA-kryptot. The answer is of cause already known, so it is the steps in the decryption procedure that are intersting, but go through the whole process and include the resulting message in the answer.

2. Consider the set of all positive integers whose digits are only ones (the 4 first of these integers are 1,11,111 and 1111). Which of all these integer has 9 as a factor? A complete motivation is required. (4p)

3. Calculate the boolean matrix power $A^{[100]}$ where (2p)

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Good Luck! Jan-Olav and Mikael