Aalto-universitetet

MS-A0409 Grundkurs i diskret matematik — Gripenberg
Övning 4
Vecka 40, 2–5.10.2013
Teori för dessa uppgifter finns också i Biggs: 8, 13

Returnera lösningarna till I-uppgifterna senast 8.10.2013 kl. 16.30
Kom ihåg att skriva ditt namn och studentnummer!

I1. En person skrev ner sitt personnummer som 1411x9-510R där siffran x blev oläslig. Vad är x? Kontrolltecknet R innebär att då det tal som bildas av de nio första siffrorna divideras med 31 blir resten 23.

Man kan förstås lösa dett problem genom att kontrollera alla möjligheter men här skall du bilda en ekvation ur vilken du kan lösa x genom att tex. utnyttja att mod $(141109510, 31) = 21$, mod $(10000, 31) = 18$ och $[18]_{31}^{-1} = [19]_{31}$.

Svar: 7

I2. Visa att $[10^j]_{11} = [(-1)^j]_{11}$, $j \geq 0$ genom att använda formeln $[m^j]_n = [m]_n^j$ (två gånger). Visa att om n är decimaltalet $x_k x_{k-1} \dots x_0$ så är $[n]_{11} = [x_0 - x_1 + x_2 - \dots + (-1)^k x_k]_{11}$.

Kontrollera om 11 delar talet 1 213 141 516 171 819.

I3. Om man räknar mod $(12^{19}, 35)$ med `matlab/octave` får man som svar `0`. Av vad ser man att svaret är fel? Räkna mod $(12^{19}, 35)$ genom att använda det faktum att $19 = 2^4 + 2^1 + 2^0$ så att $12^{19} = (((12^2)^2)^2)^2 \cdot 12^2 \cdot 12$.

I4. Kryptera ”meddelandet” 13 med hjälp av RSA-algoritmen och den publika nyckeln $(15, 3)$. Eftersom 15 är ett mycket litet tal (i jämförelse med de som borde användas) är det inte speciellt svårt att räkna ut den privata nyckeln. Vad är den?

I5. Visa genom att använda Euklides algoritm att the positiva talen $11n + 3$ och $7n + 2$ har största gemensamm delare 1 för alla $n \geq 1$.

Besvara Stack-uppgifterna (`stack3.aalto.fi/course/view.php?id=15`)
senast 8.10.2013 kl. 16.30
