Aalto-universitetet

MS-A0409 Grundkurs i diskret matematik — Gripenberg
Övning 4
Vecka 40, 29.9–3.10.2014
Teori för dessa uppgifter finns också i Biggs: 8, 13

Returnera lösningarna till I-uppgifterna senast 6.10.2014 kl. 10.30
Kom ihåg att skriva ditt namn och studentnummer!

I1. I ett universitet används studentnummer som bildas av sex siffror och en kontrollbokstav. En student skrev ner sitt nummer i formen $53x576J$ där siffran x blev oläslig. Bestäm x genom att utnyttja det faktum att kontrollbokstaven J betyder att då det tal som bildas av siffrorna före kontrollbokstaven divideras med 23 så blir resten 9 och att $[530576]_{23} = [12]_{23}$, $[1000]_{23} = [11]_{23}$ och att $[11]_{23}^{-1} = [21]_{23}$. (Använd alltså inte alternativet att prova med alla siffror $0, 1, \ldots, 9$ tills du hittar det rätta.)

Svar: 9

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 $x_k x_{k-1} \ldots x_0$ (dvs. $n = x_k \cdot 10^k + x_{k-1} \cdot 10^{k-1} + \ldots + x_0$) så är $[n]_{11} = [x_0 - x_1 + x_2 - \ldots + (-1)^k x_k]_{11}$.

Kontrollera om 11 delar talet 1 543 212 347 231 932.

I3. Kryptera ”meddelandet” 6 med hjälp av RSA-algoritmen och den publika nyckeln $(22, 3)$. Eftersom 22 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?

I4. Om vi räknar mod $(11^{19}, 7)$ och mod $(11^{20}, 7)$ med `matlab` (version R2104a) får man som resultat 1 och 3. Av vad kan man se att dethär inte är rätt och vad beror det på?

Däremot lyckas räkningen med följande funktion som räknar ut mod (a^b, n) (men som inte tex. kontrollerar om argumenten är något annat än positiva heltal):

```
function y=pmod(a,b,n)
  y=1;
  z=mod(a,n);
  while b>0
   k=mod(b,2);
   if k==1
     y=mod(z*y,n);
   end
   z=mod(z*z,n);
   b=(b-k)/2;
  end
endfunction
```

Bestäm en funktion h så att om $m = a^b$ där a och b är positiva heltal och vi beräknar mod (m, n) med kommandot `pmod(a,b,n)` så räknar funktionen $O(h(m))$ gånger ett värde av `mod`-funktionen.

I5. Använd Euklides algoritm för att bestämma en största gemensamma delare av polynomen $2x^4 - x^3 + 7x - 3$ och $2x^3 - x^2 - 2x + 6$, dvs. ett polynom $p(x)$ med så högt gradtal som möjligt så att $2x^4 - x^3 + 7x - 3 = p_1(x)p(x)$ och $2x^3 - x^2 - 2x + 6 = p_2(x)p(x)$ för några polynom $p_1(x)$ och $p_2(x)$.

Svar: $2x + 3$

Besvara Stack-uppgifterna (`stack3.aalto.fi/course/view.php?id=15`)
senast 6.10.2014 kl. 10.30
