Aalto-universitetet

MS-A0409 Grundkurs i diskret matematik — Gripenberg
Övning 4
Vecka 40, 2–8.10.2013
Teori för dessa uppgifter finns också i Biggs: 8, 13

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 $[18]_{31}^{-1} = [19]_{31}$.

Lösning: Talet $1411x9510$ kan skrivas som $141109510 + x \cdot 10000$ så att vi får ekvationen

$$[23]_{31} = [141109510 + x \cdot 10000]_{31} = [141109510]_{31} + [x]_{31} \cdot [10000]_{31}.$$

Av de uppgifter som gavs vet vi att $[141109510]_{31} = [21]_{31}$ och $[10000]_{31} = [18]_{31}$ så att ekvationen blir

$$[23]_{31} = [21]_{31} + [x]_{31} \cdot [18]_{31},$$

och vi får

$$[x]_{31} = [18]_{31}^{-1} \cdot [23 - 21]_{31} = [19]_{31} \cdot [2]_{31} = [38]_{31} = [7]_{31},$$

vilket betyder att $x = 7$. 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.

Lösning: Om $j \geq 0$ så är

$$[10^j]_{11} = [10]_{11}^j = [-1]_{11}^j = [(-1)^j]_{11}.$$

Nu är $n = x_0 \cdot 10^0 + x_1 \cdot 10 + \dots x_k \cdot 10^k$ och därför är

$$[n]_{11} = [x_0 \cdot 10^0]_{11} + \dots + [x_k \cdot 10^k]_{11} = [x_0]_{11} \cdot [10^0]_{11} + [x_1]_{11} \cdot [10^1]_{11} + \dots + [x_k]_{11} \cdot [10^k]_{11}$$
$$= [x_0]_{11} \cdot [(-1)^0]_{11} + [x_1]_{11} \cdot [(-1)^1]_{11} + \dots + [x_n]_{11} \cdot [(-1)^k]_{11} = [x_0 - x_1 + x_2 - \dots + (-1)^k x_k]_{11}.$$

Av det här resultatet följer att

$$[1\,213\,141\,516\,171\,819]_{11} = [9 - 1 + 8 - 1 + 7 - 1 + 6 - 1 + 5 - 1 + 4 - 1 + 3 - 1 + 2 - 1]_{11}$$
$$= [36]_{11} = [3]_{11} \neq [0]_{11}$$

så 11 delar inte talet.

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 $12^{19} = (((12^2)^2)^2)^2 \cdot 12^2 \cdot 12$.

Lösning: Om $\text{mod}\,(m,n)=0$ så betyder det att $n|m$ men det är klart att $35\not|12^{19}$ eftersom $5|35$ men $5\not|12$. Vi får

$$\begin{aligned}
&\text{mod}\,(12^2,35)=\text{mod}\,(144,35)=4,\\
&\text{mod}\,((12^2)^2,35)=\text{mod}\,(4^2,35)=\text{mod}\,(16,35)=16,\\
&\text{mod}\,(((12^2)^2)^2,35)=\text{mod}\,(16^2,35)=\text{mod}\,(256,35)=11,\\
&\text{mod}\,((((12^2)^2)^2)^2,35)=\text{mod}\,(11^2,35)=\text{mod}\,(121,35)=16,\\
&\text{mod}\,(12^2\cdot 12,35)=\text{mod}\,(4\cdot 12,35)=\text{mod}\,(48,35)=13,\\
&\text{mod}\,(12^{19},35)=\text{mod}\,((((12^2)^2)^2)^2\cdot 12^2\cdot 12,35)\\
&\qquad=\text{mod}\,(16\cdot 13,35)=\text{mod}\,(208,35)=33.
\end{aligned}$$

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?

Lösning: Enligt RSA-algoritmen skall vi räkna ut $\text{mod}\,(13^3,15)$ och vi får (om man nu inte räknar direkt med något hjälpmedel)

$$\begin{aligned}
&\text{mod}\,(13^2,15)=\text{mod}\,(169,15)=4,\\
&\text{mod}\,(13^3,15)=\text{mod}\,(13\cdot 4,15)=\text{mod}\,(52,15)=7,
\end{aligned}$$

så det krypterade meddelandet är 7.

Eftersom $15=3\cdot 5$ är $m=(3-1)\cdot(5-1)=8$. I $\mathbb{Z}_8$ är den enda inverterbara elementen $[1]_8$, $[3]_8$, $[5]_8$ och $[7]_8$ och eftersom $[3\cdot 3]_8=[9]_8=[1]_8$ ser vi att $[3]_8^{-1}=[3]_8$ så att den privata nyckeln är också $(15,3)$.

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

Lösning: Genom att använda Euklides algoritm får vi (när $n\geq 2$)

$$\begin{aligned}
11n+3&=1\cdot(7n+2)+(4n+1)\\
7n+2&=1\cdot(4n+1)+(3n+1)\\
4n+1&=1\cdot(3n+1)+n\\
3n+1&=3\cdot n+1\\
n&=n\cdot 1+0.
\end{aligned}$$

Om $n=1$ så stannar algoritmen på raden med $3n+1=(3n+1)\cdot n+0$ men också i detta är resultatet av algoritmen att $\gcd(11n+3,7n+2)=1$.
