Aalto University

MS-A0401 Foundations of discrete mathematics
Exercise 4
28.9–2.10.2015, week 40

Gripenberg, Potka, Pöllänen, Tuhkanen, Ääri

Return your solutions to the P-questions and answer the S-questions not later than 5.10.2015 at 16.
Remember to write your name, student number and group!

P1. When a person wrote his social security number the result was $2x1189-321W$ where the digit x was illegible. What is x? The control letter W implies that when one forms a number out of the digits preceding it and divides that number by 31, then the remainder is 28.

One can, of course, solve this problem by testing all possibilities but here you should find an equation, from which you can (easily?) solve x and you can use the knowledge that $\mathrm{mod}\,(201\,189\,321, 31) = 3$, $\mathrm{mod}\,(10\,000\,000, 31) = 20$ and $[20]_{31}^{-1} = [14]_{31}$ and it is a good idea to write the number $2x1\,189\,321$ in the form $201\,189\,321 + x \cdot 10\,000\,000$.

P2. Show, using the Euclidean algorithm, that the positive integers $11n+3$ and $7n+2$ are relatively prime for all $n \in \mathbb{Z}_+$.
Note! *In the case where $n=1$ the algorithm works in a slightly different way than in the cases where $n \geq 2$.*

P3. A wants to send a message to B and asks her to send her public RSA-algrithm key to A. However, C intercepts this message containing the key, which is $(21, 5)$ and sends instead his own public key, which is $(34, 11)$ to A. Next A sends a message, which encrypted is 15 to C although she believes she is sending it to B. Then C decrypts this message, reads it and sends it to B, encrypted with B:s public key.

What was the original message and what message does C send to B?
Note! *This is an example of a "Man-in-the-middle"-attack by B who only reads the message but does not change it.*

Answer: 9 ja 18

P4. If you calculate mod $(13^{21}, 9)$ and mod $(13^{22}, 9)$ with Matlab (version R2015a) then the results are 7 and 4. How can you see that this is not correct and what is the reason for that?

This calculation works with the following function that calculates mod (a^b, n) (but does not check whether the arguments are something else than positive integers):

```
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
```

Determine a function h so that if $m = a^b$ where a and b are positive integers and mod (m, n) is calculated with the command `pmod(a,b,n)` then the program calculates $O(h(m))$ times the value of the `mod`-function (and h does not grow "unreasonably fast").

Hint: What would mod $(13^{22}, 9)$ *be if* mod $(13^{21}, 9) = 7$?

P5. If you have to solve the equation $[a]_n \cdot [x]_n = [b]_n$ and gcd $(a, n) = 1$ there is an inverse $[a]_n^{-1}$ and the solution is $[x]_n = [a]_n^{-1}[b]_n$ (and this solution is unique as a congruence class). Determine the possible solutions in the case where gcd $(a, n) = d > 1$ in the following way.

(a) Show that if there is a solution, then $d \mid b$ and hence we assume below that this is the case.
(b) Let $c = a/d$ and $m = n/d$ (both of which are integers) and show that gcd $(c, m) = 1$.
(c) Let $e = b/d$ (which by assumption is an integer). Since gcd $(c, m) = 1$ by part (b) there is a number y so that $[y]_m = [c]_m^{-1}$, i.e., $c \cdot y = 1 + k \cdot m$. Show that $x = y \cdot e$ is a solution to the original equation (by showing that $a \cdot x = b + r \cdot n$).
(d) Show that $y \cdot e + j \cdot m$ is a solution as well for every $j \in \mathbb{Z}$, (but you don't have to show that in this way one gets exactly d different congruence classes $[x]_n$).