Security

Assignment 7, Monday, November 7, 2011

Handing in your answers: There are two options:

1. Put your solutions in Pim's post box (in the white cabinet, lower door, near the printer at the station-side-end of the corridor on the second floor of the Huygens building). Before handing in, make sure:
   - your names and student numbers are written on the document.
2. Send your solutions by e-mail to `pim@cs.ru.nl` with subject '*assignment 7*'. This e-mail should only contain a single PDF document as attachment. Before handing in, make sure:
   - your names and student numbers are included in the document (since it will be printed),
   - your names are part of the filename (example: PimVullers_FlavioGarcia-7.pdf), and
   - the file is a PDF document.

Deadline: Monday, November 14, 8:30 sharp!

1. **(3 points)** Prime divisors and greatest common divisor ($gcd(x, y)$).
   (a) The prime-divisor factorization of 48 is $2^4 \times 3^1$. Find the factorization of 60, then find $gcd(48, 60)$, and then factorize $gcd(48, 60)$.
   (b) Factorize 16 and 15. Find $gcd(16, 15)$, and then factorize $gcd(16, 15)$ in terms of the prime divisors 2, 3 and 5. You may use zero-degrees: 2^0, 3^0, 5^0.
   (c) Let $x = p_1^{n_1} \times \cdots \times p_k^{n_k}$ and $y = p_1^{m_1} \times \cdots \times p_k^{m_k}$ be the factorizations of x and y respectively, where some of n_i or m_j may be 0. What is the factorization of $gcd(x, y)$?
2. **(2 points)** Euler totient function ϕ.
   (a) Name the elements of the set $\{1, \ldots, 5\}$ that are relatively prime to 5. What is $\phi(5)$?
   (b) Name the elements of the set $\{1, \ldots, 6\}$ that are relatively prime to 6. What is $\phi(6)$?
3. **(2 points)** Let $a \in \mathbb{Z}_n^*$. The multiplicative inverse x of the number a is such that $ax \equiv 1 \pmod{n}$ holds.
   (a) Why can you look for x using the formula $x = \dfrac{nk+1}{a}$, for some $k = 0, 1, 2, \ldots$?
   (b) Find x such that $9x \equiv 1 \pmod{10}$ holds.
   (c) Let $a = n - 1$. Find x such that $(n-1)x \equiv 1 \pmod{n}$. Explain your answer.
4. **(3 points)** Multiplicative groups.
   (a) Look at the multiplication table for $\mathbb{Z}_{15}^*$ in Table 1. Find the order of each element.
   (b) Create the multiplication table for $\mathbb{Z}_7^*$. What are the orders of its elements? Is this group cyclic or not (and why)? If *yes*, what are the generators?

	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Table 1: Multiplication table for $\mathbb{Z}_{15}^*$