Sveučilište u Dubrovniku
Prof. dr. sc. Hrvoje Kraljević
Dr. sc. Daniel Kressner

2005/2006

Logika, skupovi i diskretna matematika

Exercise 4

The assignments are due to 05.12.2005.

Tutorial 4.1

1. Compute $\gcd(a, b)$ and find integers m, n such that $\gcd(a, b) = ma + nb$ for $a = 190, b = 34$.
2. Find a solution in integers to the equation $325x + 26y = 91$.

Tutorial 4.2

1. Show that if p and p' are primes, and $p \mid p'$, then $p = p'$.
2. Provide an example which shows that Lemma 3.14 of the lecture notes is not true if p is just known to be a positive integer (and not necessarily a prime).
3. Find the prime factorizations of 201, 1001 and 2010000.
4. Using the Sieve of Eratosthenes, find all the primes from 1 to 50.

Tutorial 4.3

1. Compute the remainder of 5^{10} under division by 21 using Theorem 3.19 from the lecture notes.
2. Compute the remainder of 572^{29} under division by 713.
3. Encrypt 333 using the public key 713, 29 from Example 3.18.
4. Decrypt 411 using $s = 569$ as in Example 3.18.
5. Assume that we choose primes $p = 17, q = 23$, and $n = 31$.
   (a) Compute the values of z, ϕ, s as described in Section 3.6.
   (b) Encrypt 101 using the key z, n.
   (c) Decrypt 250.

Tutorial 4.4

1. Draw the digraph of the relation $R = \{(1, 2), (2, 1), (3, 3), (1, 1), (2, 2)\}$ on $X = \{1, 2, 3\}$.
2. For each of the following relations defined on the set of natural numbers, determine whether it is reflexive, symmetric, antisymmetric, transitive, and/or a partial order:
   (a) $(x, y) \in R$ if $x = y^2$,
   (b) $(x, y) \in R$ if $x = y$,
   (c) $(x, y) \in R$ if 3 divides $x - y$.
3. For each of the following relations defined on the collection of all nonempty subsets of real numbers, determine whether it is reflexive, symmetric, antisymmetric, transitive, and/or a partial order:
   (a) $(A, B) \in R$ if for every $\epsilon > 0$, there exists $a \in A$ and $b \in B$ with $|a - b| < \epsilon$,
   (b) $(A, B) \in R$ if for every $a \in A$ and $\epsilon > 0$, there exists $b \in B$ with $|a - b| < \epsilon$.

Homework assignment 4.1 **5 points**

1. Compute $\gcd(a, b)$ and find integers m, n such that $\gcd(a, b) = ma + nb$ for $a = 2406, b = 654$.
2. You are given an unlimited supply of water, a large container, and two jugs whose capacities are 7 litres and 9 litres. How would you put one litre of water in the container? Can you do the same with two jugs whose capacities are 6 litres and 9 litres?
3. Find integers x and y satisfying $966x + 686y = 70$.

Homework assignment 4.2 **5 points**

1. Show that 123456789 is not a prime.
2. Find the prime factorizations of 111, 1111, 1234, and 123456786.

BONUS Homework assignment **up to 5 additional points**

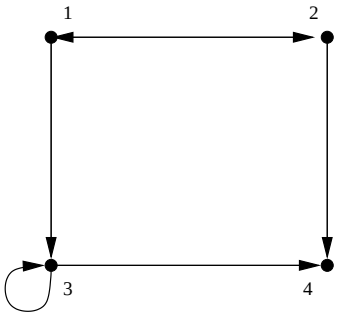
Write a C program which prints all primes from 1 to 1000 using the Sieve of Eratosthenes. Print the C program along with the produced output (please use a compact output format).

Homework assignment 4.3 **8 points**

1. Compute the remainder of 143^{10} under division by 230 using Theorem 3.19 from the lecture notes.
2. Encrypt 444 using the public key 713, 29 from Example 3.18.
3. Decrypt 511 using $s = 569$ as in Example 3.18.
4. Assume that we choose primes $p = 59, q = 101$, and $n = 41$.
   (a) Compute the values of z, ϕ, s as described in Section 3.6.
   (b) Encrypt 584 using the key z, n.
   (c) Decrypt 250.

Homework assignment 4.4 **6 points**

1. Give an example of relation, which is both symmetric and antisymmetric.
2. Draw the digraph of the relation $\{(1,2),(2,3),(3,4),(4,1)\}$ on $X = \{1,2,3,4\}$.
3. Write the relation as a set of ordered pairs for the following digraph:



4. For each of the following relations defined on the set of natural numbers, determine whether it is reflexive, symmetric, antisymmetric, transitive, and/or a partial order:
   (a) $(x,y) \in R$ if $x > y$,
   (b) $(x,y) \in R$ if $x \geq y$,
   (c) $(x,y) \in R$ if 3 divides $x + 2y$.
5. What is wrong with the following argument, which supposedly shows that any relation R on X that is symmetric and transitive is reflexive?

   Let $x \in X$. Using symmetry, we have (x,y) and (y,x) both in R. Since $(x,y),(y,x) \in R$, by transitivity we have $(x,x) \in R$. Therefore, R is reflexive.