

## Homework 7

Lecturer: Sasha Boldyreva

Due: April 16, 2009

Do the assigned reading!

**Assignment 7.01** Do the assigned reading.

**Assignment 7.02** Indicate how much time did you spend on this homework.

In all problems do not just give an answer, but show your reasoning/work.

**Problem 7.1, 5 points.** In the proof of the Birthday paradox we used the following very useful fact known as the union bound:

$$\Pr(E_1 \cup E_2 \dots E_n) \leq \Pr(E_1) + \Pr(E_2) + \dots \Pr(E_n) ,$$

where  $E_1, E_2, \dots E_n$  are events associated with the same sample space. Prove it by induction and use the base case  $n = 2$ .

**Problem 7.2, 5 points.** Suppose that all you know about high tide is that its expected height is 1 meter, and the height is always non-negative. What can we say about the probability that you see high tide more than 2 meters?

**Problem 7.3, 5 points.** Problem 16 from Section 6.4 of Rosen's textbook.

**Problem 7.4, 5 points.** Problem 26 from Section 6.4 of Rosen's textbook.

**Problem 7.5, 5 points.** Run the Extended GCD algorithm by hand on input (1529,14039) and show the intermediate and final results.

**Problem 7.6, 5 points.** Prove that for any integers  $a, b, c$ , if  $c|(ab)$ , and  $\gcd(a, c) = 1$ , then  $c|b$ .

**Problem 7.7, 5 points.** Explain why adding two numbers  $a$  and  $b$  modulo  $n$  takes linear time (in  $|n|$ ), if  $0 \leq a, b < n$ .

**Problem 7.8, 5 points.** Prove that if  $n$  is an integer that is not a multiple of 3, then  $n^2 \equiv 1 \pmod{3}$ .