

EXAM MODULAR ARITHMETIC
(PART OF THE COURSE INTRODUCTION TO MATHEMATICS)
SEPTEMBER 17TH, 2013
9:00 – 10:45

The maximal score for this exam is 20 points. 2 points you receive for writing your name on every sheet of paper you intend to hand in; the remaining 18 points can be obtained by formulating complete arguments and calculations to each of the following problems.

(1) [3+3 points] Prove the following statement dealing with two integers n, m :
 $\gcd(n, m) = m \Leftrightarrow m$ is positive and $m|n$.

(2) [3 points] Calculate two integers a, b satisfying $42a + 1001b = 7$.

(3) [3 points] Suppose that the integers n, m satisfy
 $42n + 1001m = 7$.

Prove that $\gcd(n, m) = 1$.

(4) Take $n = 17^9 + 1 = 118587876498$.

(a) [2 points] Explain why $17^{18} \equiv 1 \pmod{n}$.

(b) [4 points] Determine the inverse of $17^{2013} \pmod{n}$.