

CS 235: Algebraic Algorithms

Assignment 1

Due: January 29, 2008

Handins are due in class and should be typed or neatly handwritten (be kind to your grader!) Check the course webpage at <http://cs-people.bu.edu/charlton/cs235/> for any updates or corrections.

1 Modular Multiplication

In Lecture 1 we proved:

$$a + b = (a \bmod n) + (b \bmod n) \pmod{n} \quad (1)$$

Prove the related claim, asserted but not proven in class:

$$a \cdot b = (a \bmod n) \cdot (b \bmod n) \pmod{n} \quad (2)$$

You will prove this claim in two different ways.

1.1 Proof by induction (10 points)

For arbitrary (fixed) n and a , prove Equation 2 by induction on b , and argue the inductive step by applying Equation 1. Make sure you allow for b to be negative.

1.2 Proof by cancellation (10 points)

Without relying on Equation 1, prove Equation 2 directly by canceling multiples of n , as we did in class to prove the additive case.

2 Modular Exponentiation

2.1 Proof by induction (10 points)

Prove the following claim, which extends the preceding cancellation laws to cover exponents:

$$a^m = (a \bmod n)^m \pmod{n} \quad \forall m \geq 0 \quad (3)$$

This claim follows inductively from Equation 2 above. We even used this implicitly in Lecture 1 when we said that $10^k = 1^k = 1 \pmod{3}$. Here you should give an explicit justification for that simplification, using induction on m .

2.2 Cancelling the exponent (10 points)

From all these rules, it is tempting to make the following similar claim:

$$a^m = a^{(m \bmod n)} \pmod{n} \quad (4)$$

Is this true? Prove your answer.

3 Divisibility by 7

In Lecture 1 we showed “tricks” to check divisibility by 2, 3, 4, 5, 6, 8, and 9 in the base-10 number system, but we showed that similar tricks for divisibility by 7 don’t work very well. Here we will investigate tricks that work in other number systems. Remember that for $n > 0$, the base- n number system describes integers using digits d_i in the range 0 to $(n - 1)$ as follows:

$$m = d_k d_{k-1} \dots d_1 d_0 = \sum_{i=0}^k d_i \cdot n^i \quad (5)$$

3.1 Last digit (15 points)

For which integers n does the base- n number system allow us to check divisibility by 7 by looking at only the last digit? Prove your answer.

3.2 Summing of digits (15 points)

Recall the trick to check divisibility by 3 (or 9) in the base-10 system: sum up all the individual digits, then check divisibility of that total. For which integers n does the base- n number system allow us to check divisibility by 7 using that same trick? Prove your answer.