Modular Arithmetic Investigations Pre-class, Week 5

Modular arithmetic (congruences) is another equivalent way of thinking about remainders in long division. Given a natural number n > 0 (some people restrict modular arithmetic to n > 1), if n|(a − b), then we say that a is congruent to b modulo n and write a ≡ b (mod n).

1. Determine if the following congruences are true (using the definition of congruency, and prefer- ably without a calculator).

a. 430023 ≡ 23 (mod 43)

b. 23 ≡ 430023 (mod 43)

c. 7823927345612341 ≡ 7112981223576296 (mod 10)

d. 7712927345612341 ≡ 7712981223576296 (mod 5)

e. a ≡ a (mod 7) (where a is an unknown number)

f. a · k ≡ 0 (mod a) (where a is an unknown number)

If a = q1 · n + r where 0 ≤ r<n, then a ≡ r (mod n). If b = q2 · n + r, then we also have a ≡ b (mod n). So congruency is an equivalent way of reducing a number to its remainder when divided by n. The way we defined congruency makes easier to deal with negative numbers without worrying about the remainder. The definition and notation we use for congruency provides a powerful and convenient tool when dealing with many types of divisibility problems.

2. Recall the divisibility rule for 3. Using this rule, determine the remainders of 1234567771 and 1112341112 when divided by 3. Express this in mod notation.

3. If a ≡ 4 (mod 7) and b ≡ 5 (mod 7), then what can you say about (a+b), (a−b) and ab modulo 7? Justify using the definition.

4. Simplify the expression 25 · 34 + 9 · 812 (mod 7). Justify briefly.