MATH 314 - Class Notes

9/20/2016

Scribe: Megan Wysocki

Summary: In today's class we went over Mission 3 (Homework 3), reviewed the Euclidean Algorithm, discussed congruences, residues and rings, and reviewed sage as well. The Euclidean Algorithm is used to calculate the GCD and is known as division with remainder. One of the most basic and useful notions in number theory is modular arithmetic. Modular arithmetic is used with congruences. The definition of congruences is as follows: "Let a, b, n be integers with $n! = 0$. We say that $a = b$ (mod n).

Notes: Include detailed notes from the lecture or class activities. Format your notes nicely using latex such as

- Euclidean Algorithm
  - Find x,y for $19x + 79y = 1$
    - **Step1** Euclidean Forward
      - $79 = 4(19) + 3$
      - $19 = 6(3) + 1$
      - $3 = 3(1) + 0$
      - Zero tells you whatever your last remainder was is your GCD
      - Therefore, 1 was your remainder before 0, so the $GCD(79, 19) = 1$
    - **Step 2** Work Backwards
      - $79 - 4(19) = 3$
      - $19 - 6(3) = 1$
      - $19 - 6[79 - 4(19)] = 1$
      - $19 - 6(79) + 24(19) = 1$
      - $25(19) - 6(79) = 1$
    - **Find** 19^{-1} **(mod 79)** using the equation $25(19) - 6(79) = 1$
      - $-6(79)\text{mod}79 = 0$
      - Therefore, $25(19) = 1$ mod 79
      - $19^{-1} = 25$ mod 79
      - Conclusion: To compute a^{-1} (mod n) we use Euclidean Algorithm to find x,y such that $ax + ny = 1$, then $a^{-1} = x$(mod n)
- **Residues and Rings**
  - If n is any positive integer, then the possible remainder modulo n are $(0, 1, 2, ..., n - 1)$
    - we call these **residues** modulo n
    - we can add or subtract residues mod n
    - we can also multiply any two residues modulo n

- Any collection of objects that you can add, subtract, and multiply while using the usual rules of arithmetic apply is called a **ring**.
  - Residues modulo n form a ring for any positive integer n.
  - Other examples of rings:
    - $2x2$ matrix or nxn matrix
    - Real Numbers
    - Integers
    - Rational Numbers (Any number you can write as a function)
    - All Polynomials with variable x
- **Note:** take Math 369 to learn more about rings

- **Chinese Remainder Theorem**
  - this is a useful tool for solving equations: mod n
  - If m,n are integers with $GCD(m,n) = 1$ then for any a,b there exists exactly one solution to $x = a$ (mod m) and $x = b$ (mod n) modulo mn.
  - **Example1:** Suppose $x = 17$ (mod 26)
    - $x = 17 + k(26)$
      - **Note:** we can factor 26 so that $26 = 13 * 2$
    - if $x = 17$ (mod 26), then $x = 1$ (mod2)
    - if $x = 17$ (mod 26), then $x = 4$ (mod13)
      - **Note:** You can check all other residues (mod 26), 17 is the only one that satisfies $17 = 1$ (mod 2) and $17 = 4$ (mod 13)
    - $x = 17$ (mod 26) iff ¡=¿ $x = 1$ (mod 2) and $x = 4$ (mod 13)
  - **Example2:**Find x such that $x = 3$ (mod 7) and $x = 11$ (mod 13)
    - **Note:** solution = number or residue modulo 91
      - (mod **7**, mod **13**)
      - $7 * 13 = 91$
    - Therefore,
      - $x = 3$ (mod7)
      - $x = 3 + k(7)$ needs to be congruent to $x = 11$ (mod 13)
      - $3 + k(7) = 11$ (mod 13)
      - SUBTRACT THE THREE FROM BOTH SIDES
      - $k(7) = 8(mod13)$
    - **Step 1:** use Euclidean Algorithm to solve 7^{-1} (mod 13)
      - $13 = 1(7) + 6$
      - $7 = 1(6) + 1$
      - $6 = 6(1) + 0$
    - **Step 2**
      - $1 = 7 - 1(6)$

        - $1 = 7 - 1[13 - 1(7)]$
        - $1 = 7 - 13 + 7$
        - $1 = 2(7) - 13$
        - $1 = 2(7) \pmod{13}$ $-13 \pmod{13}$
        - **Note:** $13 \pmod{13} = 0$
        - $1 = 2(7) \pmod{13}$
        - Therefore, $7^{-1} = 2 \pmod{13}$
    - **Step 3**
        - refer back to formula from Step 1:
        - $k(7) = 8(\text{mod}13)$
        - Multiply formula by $7^{-1} = 2$
        - $k = 16 \pmod{13}$
        - $k = 3 \pmod{13}$
    - **Step 4**
        - Take $k = 3$
        - $x = 3 + k(7)$
        - $= 3 + 3(7)$
        - $= 24$
        - $x = 24 \pmod{91} == x = 3(\text{mod } 7)$ and $x = 11 \pmod{13}$
        - Therefore we have solved for the congruency

- Sage Practice For Assignment 3

  Look at the handouts folder and click functions.