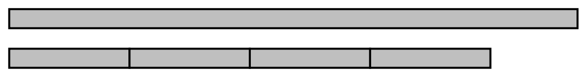
Group 1
Daniel King
Lane Murphy
Jack Gilbert

Lecture Notes for 9/10/18

- Given ax + by = c where a, b, & c are integers and the solutions are to be integers
    - Example: 2x = 3
        - Form is ax = c, and b = 0
        - Solution is x = c/a where a must divide c (notation a|c)
        - Euclid's terminology is that "a measures c"
            - Or a certain distance a can be measured by an amount of smaller distances c:
              a:
              c:
              
              with potentially some leftover amount less than c: 
    - If d measures a & b, then it must measure c
    - Problem restated: what is the greatest common measure, or greatest common denominator (gcd) of a & b?
    - Example: given x = 43 and y = 31
        - To start, if you have a & b given where a < b, divide b by a
        - Either you will have a leftover that is less than a or no leftover, i.e. a measures b
        - In this case, 31 goes into 43 once with 12 leftover
        - Repeating this process:
            - 12 goes into 31 twice with 7 leftover
            - 7 goes into 12 once with 5 leftover
            - 5 goes into 7 once with 2 leftover
            - 2 goes into 5 twice with 1 leftover
            - 1 is a special entity, as 1 measures all numbers
        - Can be rewritten as:

43	
31	1
12	2
7	1
5	1
2	2
1	-

        - Euclid's method leads us to show that there is no common measure because the lowest left hand value is 1
            - In modern terminology, 43 & 31 are coprime
    - If there is a common measure between two numbers that is greater than 1, it is obtained as the last step of the process above with 0 remainder in the right hand column
    - In general terms, ax + by = c to be all integers is possible only if there is a gcd that divides (or measures) c
    - Called Euclid's Division Algorithm

        - States that there is a solution, but not how to solve this type of problem
- How to solve?
    - Given a & b with gcd(a,b) = d, we can write d = ax - by for some x & y
    - Called the Extended Euclidian Algorithm
        - Not truly Euclidian because Euclid did not have the language to describe the subtraction required
    - Appears in Aryabhata in 476 AD
        - Arybhata describes process called "kuttka," or "pounding down" as a process of reducing numbers systematically
    - Example: a third column can be added as shown below to the left of the given numbers, with a 0 & 1 on the bottom of this newly added row

	43	
	31	1
	12	2
	7	1
	5	1
1	2	2
0	1	-

    - The numbers above the 0 & 1 can be filled in by multiplying the topmost left hand value by the value in the far right column across it and then adding the number below it
        - For the above, this would be the number 1 (next to 5), and this would yield $1 \times 2 + 0 = 2$
        - Repeating for the remaining missing values yields:

18	43	
13	31	1
5	12	2
3	7	1
2	5	1
1	2	2
0	1	-

    - Then the four values in the two left columns of the top rows can be set into the original equation using the bottom center value of 1 for d yields
        - ax - by = d → (18)(31) - (13)(43) = 1
    - To find all possible solutions, the coefficients 18 & 13 can have any multiple of their opposite term's coefficient added to them
        - (18 + (t43))31 - (13 + (t31))43) = 1 for any integer t
    - Substituting the t terms yields:
        - (p + 18)31 - (q + 13)43 = -1
    - Subtracting the original equation yields:
        - (p + 18)31 - (q + 13)43 = -1
          -      (18)31 -   (13)43 = -1
          ___
                p(31) -   q(43) = 0
    - So p must be divided by 43, or (t × 43) = p, and q must be divided by 31, or (t × 31) = q

    - Using negative numbers, or (-18)(31) - (-13)43 = 1
        - Given known answer of (43)(31) - (31)(43) = 0 and subtracting this from the above yields:
            - (43-18)31 - (31-13)43 = 1, or
            - (25)31 - (18)43 = 1
- The Chinese Remainder Theorem is a specific problem cited from around 250 AD: find n such that n divided by 12 leaves a remainder of 2 and the same n divided by 7 leaves a remainder 5
    - So n = 12x + 2 = 7y + 5 → 12x - 7y = 3 (in the form as above examples)
    - Using division algorithm:

5	12	
3	7	1
2	5	1
1	2	2
0	1	-

    - Arranging the diagonal product of the top and left values so that a positive number results: (3)12 - (5)7 = 1
    - Original formula required that it be equal to 3, so multiplying right hand side and coefficients in parenthesis on left hand side by 3 yields: (9)12 - (15)7 = 3
    - Subtracting the opposite coefficients from the parenthetical coefficients yields the final answers for x and y:

  (9)12 - (15)7 = 3
- (7)   (-12)
____

  (2)12 - (3)7 = 3

    - Answer: n = 12(2) + 2 = 7(3) + 5 = 26