Discrete Math: Homework #3

Due on November 9, 2022 at 3:10pm

Professor J Section A

V **U**

Problem 1

Use the Euclidean algorithm to calculate gcd(102,70). Use the extended Euclidean algorithm to write gcd(663,234) as an integer linear combination of 663 and 234.

Solution. Euclidean algorithm can be described as followed:

$$\gcd(a,b) := \begin{cases} a & \text{if } b = 0 \\ \gcd(b, a \mod b) & \text{otherwise} \end{cases} \tag{1}$$

Thus

$$\begin{aligned} \gcd(102,70) &= \gcd(20,32) \\ &= \gcd(32,6) \\ &= \gcd(6,2) \\ &= \gcd(2,0) \\ &= 2 \end{aligned}$$

Running the following python code, we have

```
def extended_gcd(a, b):
        if a < b:
                a, b = b, a

        old_r, r = a, b
        old_s, s = 1, 0
        old_t, t = 0, 1

        while r != 0:
                quotient = old_r // r
                old_r, r = r, old_r - quotient * r
                old_s, s = s, old_s - quotient * s
                old_t, t = t, old_t - quotient * t

        print("B zout coefficients:", (old_s, old_t))
        print("greatest common divisor:", old_r)
        print("quotients by the gcd:", (t, s))

extended_gcd(663, 234)
```

Bézout coefficients: (-1, 3)
greatest common divisor: 39
quotients by the gcd: (-17, 6)
Therefore, $-1 \times 663 + 3 \times 234 = \gcd(663,234) = 39$ □

Problem 2

Prove that a number is divisible by 3 if and only if the sum of its digits is divisible by 3.

Solution.
Let $n \in \mathbb{N}$, and let $n = \sum_{k=0}^{m} a_k 10^k$ be the decimal representation of n. We need to show

$$n \equiv 0 \mod 3 \iff \sum_{k=0}^{m} a_k \equiv 0 \mod 3$$

In fact,

$$\begin{aligned} n &= \sum_{k=0}^{m} a_k 10^k \\ &= \sum_{k=0}^{m} a_k (3 \times 3 + 1)^k \\ &\equiv \sum_{k=0}^{m} a_k \mod 3 \end{aligned}$$

which is sufficient. □

Problem 3

Prove that all numbers in the sequence

$$1007, 10017, 100117, 1001117, \cdots$$

are divisible by 53.

Solution.
The numbers in this sequence can be formulated as

$$a_n = 100 \times 10^n + \sum_{k=0}^{n-1} 10^k + 6$$

$$\iff 10(a_n - 6) + 6 + 1 = 100 \times 10^{n+1} + \sum_{k=0}^{n} 10^k + 6 = a_{n+1}$$

$$\iff a_{n+1} = 10a_n - 53$$

Thus $a_{n+1} = 10a_n \mod 53$. $a_0 = 1007 = 19 \times 53 \equiv 0 \mod 53$. By induction, $a_{n+1} = 0 \mod 53, \forall n \in \mathbb{N}$. □

Problem 4

4.A robot walks around a two-dimensional grid. It starts out at (2,0) and is allowed to take four different types of steps as:

1. $(+2, -1)$
2. $(+1, -2)$
3. $(+1, +4)$
4. $(-3, 0)$

Prove that this robot can never reach $(0, -1)$.

Solution.
Note that the moves of the robot satisfying commutative.
Let a, b, c, d be the number of moves of $1, 2, 3, 4$. we have system of equation

$$\begin{cases} 2 + 2a + b + c - 3d &= 0 \\ -a - 2b + 4c &= -1 \end{cases} \tag{2}$$

Act mod 3 on this system, we have

$$\begin{cases} -a + b + c &= 1 \\ -a + b + c &= -1 \end{cases} \tag{3}$$

which is contradiction. Thus the original system has no solution at all, which implies that the robot has no way to reach $(0, -1)$. □

Problem 5

NIM is a famous game in which two players take turns removing items from a pile of n items. For every turn, the player can remove one, two, or three items at a time. The player removing the last item loses. Prove that if each player plays the best strategy possible, the first player wins if $n \not\equiv 1(\mod 4)$ and the second player wins if $n \equiv 1(\mod 4)$. (For your interest, refer to the general NIM game at this link).

Solution. If $n \equiv 1 \mod 4$, the first player can only change n so that n divided by 4 remains $1-1, 1-2$ or $1-3$ which are $0, 3, 2$ excluding 1. Then in the second turn, the second player can pick a number of items n so that $n \equiv 1 \mod 4$ again. At the end of the game, it will always be the first player taking the last item.
Therefore, if $n \equiv 1 \mod 4$, the second player wins. Since the NIM game has no draw, under optimal strategy, in any other cases for n, the first player wins. $\square$

Problem 6

Find all solutions, if any, to the system:

$$\begin{cases} x \equiv 5 \mod 6 \\ x \equiv 3 \mod 10 \\ x \equiv 8 \mod 15 \end{cases} \tag{4}$$

Solution.
By the divisibility of primes, the system can be reduced as

$$\begin{cases} x \equiv 5 \mod 2 \\ x \equiv 5 \mod 3 \\ \\ x \equiv 3 \mod 2 \\ x \equiv 3 \mod 5 \\ \\ x \equiv 8 \mod 3 \\ x \equiv 8 \mod 5 \end{cases} \tag{5}$$

After Simplification.

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \end{cases} \tag{6}$$

By Chinese remainder theorem, It has an unique solution in $\mathbb{Z}/30\mathbb{Z}$. After enumeration,

$$x \equiv 23 \mod 30$$

□

Problem 7

Show with the help of Fermat's little theorem that if n is a positive integer, then $42|n^7 - n$.

Solution.
By divisibility of prime, we need only to show $2|n^7 - n$, $3|n^7 - n$, and $7|n^7 - n$.
By Fermat's Little Theorem ($n^p \equiv n \mod p, \forall p \in \text{prime}$),

$$7|n^7 - n$$

. Likewise,

$$n^7 = n^2n^2n^2n \equiv nnnn = n^2n^2 \equiv nn = n^2 = n \mod 2$$

Also,

$$n^7 = n^3n^3n \equiv nnn = n^3 \equiv n \mod 3$$

Thus the proof is as desired. □