Final Review: Number Theory, Recurrences

Discrete Structures
(Final scheduled for Wednesday, April 28, 2021)

You must justify all your answers to recieve full credit

---

3 Number Theory

Divisibility, GCM and LCM, congruences, multiplicative inverses, exponentiation.

3.(a). **GCD preserved in arithmetic series.** Given an arithmetic series find when will it repeat (modulo m). Also, for what values of n, a_n takes some remainder (modulo m), if ever.

3.(b). **Bezout identity.** Given positive integers a, b, c, solve integer equations $ax + by = c$ (or show that it cannot be solved).

3.(c). **Multiplicative inverse.** Given m and a, compute $\overline{a}$ such that $a \cdot \overline{a} \equiv 1 \pmod{m}$. Also solve other linear congruences $ax \equiv b \pmod{m}$. Identify cases when there are no solutions.

3.(d). **Solve CRT with a linear formula.** Given a set of 3 mutual primes m_1, m_2, m_3 and a system of congruences (possibly, with parametrized values), write a solution for the system as a linear expression modulo $m_1 m_2 m_3$.

3.(e). **Primitive roots and multiplicative orders.** Given a prime p and a number a not divisible by p, check if a is a primitive root or find those k for which $a^k \equiv 1 \pmod{p}$. Also simplify other congruences with powers using Little Fermat theorem and Euler theorem.

3.(f). **Square congruences, discrete logarithms.** Given a primitive root a modulo p (and a list of powers a^k, $k = 1, \ldots, p-1$), solve some congruences involving powers (inverses, roots and/or discrete logarithms).

3.(a). Define a recurrent sequence: $a_0 = 17$; $a_n = a_{n-1} + 48$.
Find three smallest positive values k such that a_k (in decimal notation) ends with these four digits `0017`.

3.(b). Find some integers x, y that satisfy the equation:

(a) $123x + 171y = 3$.

(b) $123x + 171y = 4$.

(c) $123x + 171y = 6$.

Show your steps (for example as extended Euclidean algorithm or Blankinship's algorithm).

3.(c). Given positive integers x and m, find the multiplicative inverse: a number $\overline{x}$ satisfying congruence $\overline{x}x \equiv 1 \pmod{m}$ (or show that the inverse does not exist).

(a) $x = 8$, $m = 27$.

(b) $x = 8$, $m = 28$.

(c) $x = 8$, $m = 29$.

Show your steps to find the inverse elements.

3.(d). Consider the following system of congruences:

$$\begin{cases} x \equiv a \pmod{13} \\ x \equiv b \pmod{14} \\ x \equiv c \pmod{15} \end{cases} \tag{1}$$

From here we can find the multiplicative inverses of $14 \cdot 15$, $13 \cdot 15$ and $13 \cdot 14$ modulo 13, 14, or 15 respectively. We provide these values just to save your time:

$$\begin{cases} 7 \cdot (14 \cdot 15) \equiv 1 \pmod{13} \\ 13 \cdot (13 \cdot 15) \equiv 1 \pmod{14} \\ 8 \cdot (13 \cdot 14) \equiv 1 \pmod{15} \end{cases} \tag{2}$$

(a) Express the general solution of system (1) as a single congruence.

(b) Find the solution, if $(a, b, c) = (7, 1, 12)$. Express this solution as an arithmetic progression (k_n) (specify the first term k_0 and the common difference d).

3.(e). We compute the first 18 powers of number 10 (modulo 19). They are listed from 10^1 to 10^{18}:

```
>>> list(map(lambda x: (10**x) % 19, range(1,19)))
[10, 5, 12, 6, 3, 11, 15, 17, 18, 9, 14, 7, 13, 16, 8, 4, 2, 1].
```

(a) What is the smallest positive integer k for which $5^k \equiv 1 \pmod{19}$? Is number 5 a primitive root (modulo 19)?

(b) What is the smallest positive integer k for which $2^k \equiv 1 \pmod{19}$? Is number 2 a primitive root (modulo 19)?

3.(f). We can compute the first 18 powers of number 2 (modulo 19). They are listed from 2^1 to 2^{18}:

```
>>> list(map(lambda x: (2**x) % 19, range(1,19)))
[2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1].
```

(a) Show how to find the multiplicative inverses for numbers $x = 13$, $x = 7$, $x = 14$ (modulo 19); locate them in the sequence of powers 2^k.

(b) Solve the congruence equations $x^2 \equiv 6 \pmod{19}$ and $x^2 \equiv 12 \pmod{19}$ (or show that they do not have solutions).

(c) Solve the congruence equation $13^x \equiv 14 \pmod{19}$ or show that it does not have a solution.
Note. The solution x is named the discrete logarithm or the index of $a = 14$ to the base $r = 13$ modulo $m = 19$.

4 Recurrent Sequences

Proving periodicity, 1st and 2nd order recurrences, divide-and-conquer recurrences, Master theorem.

4.(a). **Periodicity in repetitive processes.** Given a definition for a recurrent sequence, prove some property (such as congruence) by induction or use periodicity arguments.

4.(b). **Closed expression for a sequence.** Given a definition for a recurrent sequence and a closed formula, prove the correctness of its closed formula.

4.(c). **1st order recurrences.** Given a (non-homogeneous) 1st order linear recurrence (e.g. $a_n = c_1 a_{n-1} + c_2$), solve it.

4.(d). **2nd order recurrences.** Given a 2nd order linear recurrence (e.g. $a_n = c_1 a_{n-1} + c_2 a_{n-2}$), solve it. (Assume that the characteristic equation does not have complex roots.)

4.(e). **Define recurrent sequence.** Given a word problem (strings following some rules, the Tower of Hanoi, tilings, etc.) define a recurrence and/or solve it by finding and proving a closed formula.

4.(f). **Master theorem for divide-and-conquer.** Given a divide-and-conquer type algorithm, write the recurrence for its time complexity and solve with Master theorem.

4.(a). Define the following recurrent sequence:

$$L_n := \begin{cases} 2, & \text{if } n = 0; \\ 1, & \text{if } n = 1; \\ L_{n-1} + L_{n-2}, & \text{if } n > 1. \end{cases}$$

(a) Write the first 8 numbers of this sequence ($L_0, \ldots, L_7$).

(b) Prove that $L_{n+4} - L_n$ is divisible by 5.

4.(b). Let X be a random variable that takes value 1 with probability 1/2; value 2 with probability 1/4; value 3 with probability 1/8 and so on. Assume that you want to compute the expected value $E(X)$ using the following recurrent sequence:

$$\begin{cases} a_1 = 1 \cdot \frac{1}{2} \\ a_n = a_{n-1} + n \cdot \frac{1}{2^n} \end{cases}$$

Prove that the following closed formula is true for all positive integers n:

$$a_n = 2 - \frac{n+2}{2^n}.$$

4.(c). Solve the recurrence $a_n = 5a_{n-1} + 3$, where $n \geq 1$; and $a_0 = 1$. (Provide a closed formula for a_n and justify why it is correct.)

4.(d). Solve the recurrence $a_n = 5a_{n-1} - 6a_{n-2}$, where $n \geq 2$; and a_0, a_1 can be anything. (You can use a_0, a_1 as parameters in your closed formula.)

4.(e). A rectangle of size $2 \times n$ should be filled with n non-overlapping tiles of size 1×2. Every tile can be either white or blue, and they can be placed horizontally or vertically. Figure 1 shows a possible way to tile a rectangle 2×8.

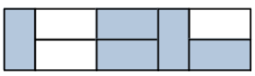

Figure 1: Filling a rectangle with 1×2 tiles.

(a) Define the number of ways to tile a rectangle $2 \times n$ (where $n \geq 1$) as a recurrent sequence a_n.

(b) Find a closed formula for a_n and prove that it is correct.

4.(f). Somebody has invented a new operation $a \otimes b$ for strings a, b (both have the same length n). Assume that s/he knows how to express $a \otimes b$ using 7 operations $a_i \otimes b_i$ (where $i = 1, 2, \ldots, 7$, and all a_i, b_i have size $\lceil n/2 \rceil$, i.e. half the size of the original operands a, b).

Find the best Big-O-Notation estimate for the time needed to compute $a \otimes b$, if a, b are both of size n.
Note. Assume that one can compute $a \otimes b$ for arguments a, b of length 1 in constant time. One can also split a and b into a_i and b_i into constant time.