CS 1010 Discrete Structures Lecture 9: Modular Arithmetic Contd. & Counting Techniques

Maria Francis

January 21, 2021

Greatest Common Divisor

- Let $a, b \in \mathbb{Z}$ s.t. at least one of them is not zero.
- The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor, $gcd(a, b)$. Does it exist? The set of common divisors of these integers is nonempty and finite.
- One algorithm: find all the positive common divisors and take the largest divisor.
- $gcd(18, 9)$: Positive common divisors of 18 and 9 are $1, 3, 9$ so the greatest is 9.
- $gcd(4, 9)$: Positive common divisor is only 1. Such integers are said to be relatively prime/co-prime, i.e. $gcd(a, b)$ is 1.

Greatest Common Divisor

- The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime or co-prime if $gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
- Is $10, 17, 21$ pairwise co-prime? Yes, since $gcd(10, 17) = gcd(10, 21) = gcd(17, 21) = 1$.
- What about $10, 19, 24$? No, since $gcd(10, 24) = 2 > 1$ is not relatively prime.
- Another algo: Find prime factorizations of a and b.

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each $a_i, b_i \in \mathbb{N}$ and could be zeroes since we are including same primes on both sides.

$$gcd(a, b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \ldots p_n^{min(a_n,b_n)}.$$

Least Common Multiple

- Let $a, b \in \mathbb{N}$, the $lcm(a, b)$ is the smallest positive integer that is divisible by both a and b.
- Do they always exist? Yes because ab is a common multiple and every nonempty set of positive integer has a least element (WOP).

$$lcm(a, b) = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \cdots p_n^{max(a_n,b_n)}.$$

- Practice question: Let $a, b \in \mathbb{N}$. Then $ab = gcd(a, b) \cdot lcm(a, b)$.

Euclidean Algorithm

- Finding prime factorizations are time consuming, that is why we explore the Euclidean Algorithm.
- The idea behind the algorithm: Say we have to find $gcd(91, 287)$.

$$287 = 91 \cdot 3 + 14$$

$$\text{If } a \mid 91 \text{ and } a \mid 287 \text{ then } a \mid (287 - 91 \cdot 3 = 14)$$

$$gcd(287, 91) = gcd(91, 14).$$

$$91 = 14 \cdot 6 + 7,$$

$$\text{Same argument as above } gcd(91, 14) = gcd(14, 7).$$

$$14 = 7 \cdot 2.$$

$$7 \mid 14 \Rightarrow gcd(14, 7) = 7.$$

Euclidean Algorithm

- I.e. Use successive divisions to reduce the problem of finding gcd to the same problem with smaller integers, until one of the integers is zero.
- Lemma : Let $a = bq + r$, where a, b, q, r are integers. Then $gcd(a, b) = gcd(b, r)$.
- Proof Idea: If we can show that the common divisors of a and b are the same as the common divisors of b and r, then we are done because both pairs must have the same *greatest* common divisor.
- You need to show both directions : If there is a common divisor d that divides a and b then it divides b and r. Also, if there is a common divisor that divides b and r then it divides both a and b as well.

Euclidean Algorithm

procedure *gcd*(a, b: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return x {gcd(a, b) is x}

We analysed the algorithm and saw that the number of divisions required where $a \geq b$ is $\mathcal{O}(log\ b)$.

Bézout's Theorem

- If $a, b \in \mathbb{N}$, then there exist integers s, t such that $gcd(a, b) = sa + tb$, i.e. an integer linear combination of a and b. The equation is called Bézout's Identity, and s, t are called Bézout coefficients.
- We do not give the proof here but note that we can obtain these coefficients by going backwards through the divisions of the Euclidean algorithm – i.e. a forward and backward pass of the algorithm giving rise to the extended Euclidean algorithm.

Bézout's Theorem

- Express $gcd(252, 198) = 18$ as a l.c. of 252 and 198.

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18. \end{aligned}$$

- We do the backwards pass:
  - $18 = 54 - 1 \cdot 36$
  - Second division says that $36 = 198 - 3 \cdot 54$
  - Substituting for 36 we get $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
  - First division says that $54 = 252 - 1 \cdot 198$.
  - Substituting for 54, we get $18 = 4 \cdot 252 - 5 \cdot 198$.

Proof of Euclid's Lemma

- We can now give the proof of Euclid's Lemma, in fact we prove something more general.
- If a, b, c are positive integers s.t. $gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.
- Because $gcd(a, b) = 1$ (which is definitely the case of primes), by Bézout's theorem we know there are integers s, t s.t. $sa + tb = 1$.
- Multiplying with c on both sides, $sac + tbc = c$.
- a divides LHS and therefore $a \mid c$.
- We used Euclid's Lemma to show the uniqueness part of the FTA.

Canceling in a Congruence

- Let m be a positive integer and let a, b, c be integers. If $ac \equiv bc \bmod m$ and $gcd(c, m) = 1$, then $a \equiv b \bmod m$.
- $m \mid (ac - bc) = c(a - b)$.
- Since $gcd(c, m) = 1$ we have $m \mid (a - b)$.
- Topics we will not cover include: how to solve congruences, the Chinese Remainder Theorem. Very relevant in cryptography.
- Fermat's Little Theorem : practice question.

Counting

- Combinatorics – study of arrangement of objects, as old as 17th century.
- Counting problems arise in computer science and mathematics including in analysis of algorithms.
- How many leaves in a tree, minimal colorings of a graph, trees with a given set of vertices, five-card hands in a deck of fifty-two, stable marriages given boy's and girl's preferences, probabilities, and so on.

Counting Principles

- THE PRODUCT RULE :
  - Let a procedure be such that it can be broken down into a sequence of two tasks.
  - If there are n_1 ways to do the first task and for each of these ways of doing the first task, there are n_2 ways to do the second task,
  - then there are $n_1 n_2$ ways to do the procedure.
- Example: The chairs of an auditorium are to be labeled with an uppercase letter followed by a positive integer ≤ 100. What is the largest number of chairs that can be labeled differently?
  - Two tasks : assigning the seat one of the 26 uppercase English letters,
  - and then assigning to it one of the 100 possible integers.
  - The product rule tells us there are $26 \cdot 100 = 2600$ different ways that a chair can be labeled.

More Examples

- Extend it to m tasks:A procedure is carried out by performing the tasks $T_1, T_2, \cdots, T_m$ in sequence. If each task $T_i, i = 1, 2, \cdots, n$, can be done in n_i ways, regardless of how the previous tasks were done, then there are $n_1 \cdot n_2 \cdots n_m$ ways to carry out the procedure.
- How many different bit strings of length seven are there?
  - Each of the seven bits can be chosen in two ways, because each bit is either 0 or 1.
  - Product rule shows there are a total of $2^7 = 128$ different bit strings of length seven.
- Counting Functions How many functions are there from a set with m elements to a set with n elements?
  - A choice of one of the n elements in the codomain for each of the m elements in the domain means by the product rule there are $n \cdot n \cdots n = n^m$ functions.

More Examples

- Counting One-to-One Functions How many one-to-one functions are there from a set with m elements to one with n elements?
  - When $m > n$ there are no one-to-one functions. Else, suppose the elements in the domain are $a_1, a_2, \dots, a_m$.
  - There are n ways to choose the value of the function at a_1.
  - But the value at a_2 can be picked in $n-1$ ways. The value of the function at a_k can be chosen in $n-k+1$ ways.
  - By the product rule, there are $n(n-1)(n-2)\cdots(n-m+1)$ one-to-one functions.
- Counting Subsets of a Finite Set
  - One-to-one correspondence between subsets of S and bit strings of length $|S|$.
  - By the product rule, there are $2^{|S|}$ bit strings of length $|S|$. Hence, $|\mathcal{P}(S)| = 2^{|S|}$.

Counting Principles

- THE SUM RULE : If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.
- Either a member of the mathematics faculty or a student who is a mathematics major is chosen as a representative to a university committee.
- How many different choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student?
- By the sum rule it follows that there are $37 + 83 = 120$ possible ways to pick this representative.

Sum Rule

- Extending it to m tasks such that a task can be done in one of n_1 ways, in one of n_2 ways,. . ., or in one of n_m ways,where none of the set of n_i ways of doing the task is the same as any of the set of n_j ways,for all pairs i and j with$1 \leq i < j \leq m$. Then the number of ways to do the task is $n_1 + n_2 + \cdots + n_m$. For example:

```
k := 0
for i1 := 1 to n1
    k := k + 1
for i2 := 1 to n2
    k := k + 1
      .
      .
      .
for im := 1 to nm
    k := k + 1
```

Product Rule

But with nested loops it is the product rule, $n_1 \cdot n_2 \cdots n_m$.

```
k := 0
for i_1 := 1 to n_1
    for i_2 := 1 to n_2
            .
            .
            .
        for i_m := 1 to n_m
            k := k + 1
```

More Complex Counting Rules

- Sum rule can be expressed in terms of pairwise disjoint finite sets, $A_1, A_2, \ldots, A_m$

$$|A_1 \cup A_2 \cup \cdots A_m| = |A_1| + |A_2| + \cdots |A_m| \text{ when } A_i \cap A_j = \emptyset \forall i, j.$$

- More complicated when sets have elements in common.
- Principle of inclusion-exclusion/THE SUBTRACTION RULE : If a task can be done in either n_1 ways or n_2 ways, then the number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways.
- Counting the number of elements in the union of two sets: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

Examples

- How many bit strings of length 8 that either start with a 1 bit or end with the two bits 00?
- We can construct a bit string of length 8 that starts with a 1 in $2^7 = 128$ ways.
- Ends with the two bits 00 can be done in $2^6 = 64$ ways
- Some of the ways to construct a bit string starting with a 1 are the same as the ways to construct a bit string that ends with 00.
- There are $2^5 = 32$ ways to construct such a string that starts with 1 and ends with 00. (How?)
- So the total number of ways : $128 + 64 - 32 = 160$.

More Complex Counting Rules

- THE DIVISION RULE: There are n/d ways to do a task if it can be done using a procedure that can be carried out in n ways, and for every way w, exactly d of the n ways correspond to way w.
- I.e. helps you ignore unimportant differences when you are counting things. You can count distinct objects, and then use the division rule to merge the ones that are same.
- Seating at a Round Table. In how many ways can King Arthur seat n knights at his round table?
- Two seatings are considered equivalent if one can be obtained from the other by rotation. For eg: if Arthur has only 4 knights, then there are 6 possibilities.
- We use square brackets in clockwise order, starting at an arbitrary point. For eg: [1234] and [4123] are same.

Division Rule

- We show using division rule that King Arthur can seat n knights at his round table in $(n-1)!$ ways.
- Let A be the set of ordering of n knights in a line. Let B be the set of orderings of n knights in a ring.
- Define $f : A \mapsto B$ by $f(x_1, x_2, \ldots, x_n) = [x_1 x_2 \ldots x_n]$, the clockwise arrangement of $x_1, x_2, \ldots, x_n$.
- What is $f^{-1}([x_1 x_2 \ldots x_n])$?
  $= \{(x_1, x_2, \ldots, x_n), (x_n, x_1, \ldots, x_{n-1}),$
  $(x_{n-1}, x_n, \ldots, x_{n-2}) \cdots, (x_2, x_3, \ldots, x_1)\}.$
- There are n tuples in that list.
- By division rule $|A| = n|B|$. $|A| = n!$ and so $|B| = (n-1)!$

Pigeonhole Principle

- Suppose that a flock of 20 pigeons flies into a set of 19 pigeonholes to roost. At least one of these 19 pigeonholes must have at least two pigeons in it.
- Why? If each pigeonhole had at most one pigeon in it, at most 19 pigeons, one per hole, could be accommodated.
- This illustrates the pigeonhole principle: If k is a positive integer and $k+1$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.
    - Use a proof by contraposition.
    - Suppose that none of the k boxes contains more than one object.
    - Then the total number of objects would be at most k. This is a contradiction, because there are at least $k+1$ objects.
- Also called the Dirichlet drawer principle, but he was not the first person to use this in his work.

Simple Applications

- A function f from a set with $k+1$ or more elements to a set with k elements is not one-to-one.
- Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.
- In any group of 27 English words, there must be at least two that begin with the same letter, because there are 26 letters in the English alphabet.

Not So Simple Applications

- In every set of 1000 integers, there are two integers x and y such that $573 \mid (x - y)$.
- Looks very hard! Our old friend induction seems to be useless here.
- To apply the Pigeonhole Principle, we must identify two things: pigeons and holes. Also, we must have more pigeons than holes. What about 1000 pigeons and 573 holes? Consider numbering the holes $0, 1, \ldots, 572$ and putting a hole n all integers congruent modulo 573.

Not So Simple Applications

- Let S be a set of 1000 integers and let $M = \{0, 1, \ldots 572\}$ and $f(n) = n \bmod 573$.
- Since $|S| \gneq |M|$ we have x and y in S s.t. $f(x) = f(y)$. Therefore, $x \bmod 573 = y \bmod 573$ and $573 \mid (x - y)$.
- Nothing special about 1000 and 573, we only need $n > m$ then in every set of n integers there are two integers x and y such that $m \mid (x - y)$.

Not So Simple Applications

- S.T. any given set containing 10 distinct positive numbers < 100, there exists two disjoint subsets sum to the same quantity.
- The numbers all vary between 1 and 99. Therefore the maximum sum of any 10 chosen numbers is $90 + 91 + 92 + \cdots + 99 = 945$.
- So the sums vary from 1 and 945.
- The number of different subsets of the 10 numbers is $2^{10} - 1$ (excluding the null set) $= 1023$.
- We have 1023 pigeons and 945 holes.
- Using the pigeonhole principle, we can argue that two different subsets map to the same sum. If these subsets have a common number or numbers, we can always remove the common numbers to produce disjoint subsets that sum to the same quantity.

Generalized Pigeon Hole Principle

- If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.
  - Proof by contraposition.
  - Suppose that none of the boxes contains more than $\lceil N/k \rceil - 1$ objects.
  - Then the total number of objects is at most,

$$k(\lceil N/k \rceil - 1) < k((N/k + 1) - 1) = N,$$

where the inequality $\lceil N/k \rceil < (N/k) + 1$ has been used. This is a contradiction since there are a total of N objects.

Applications

- Typically we ask for the minimum number of objects such that at least r of these objects must be in one of k boxes. When we have N objects, the generalized pigeonhole principle tells us there must be at least r objects in one of the boxes as long as $\lceil N/k \rceil \geq r$.
- Among 100 people there are at least $\lceil 100/12 \rceil = 9$ who were born in the same month.
- What is the minimum number of students required in a discrete mathematics class to be sure that at least six will receive the same grade, if there are five possible grades, A, B, C, D and F? $\lceil N/5 \rceil = 6$. The smallest such integer is $N = 5 \cdot 5 + 1 = 26$.

Elegant Applications

- A clever application shows the existence of an increasing or a decreasing subsequence of a certain length in a sequence of distinct integers.
- Suppose that $a_1, a_2, \ldots, a_N$ is a sequence of real numbers. A subsequence of this sequence is a sequence of the form $a_{i_1}, a_{i_2}, \ldots, a_{i_m}$, where $1 \leq i_1 < i_2 < \cdots < i_m \leq N$.
- A sequence is called strictly increasing if each term is larger than the one that precedes it, and it is called strictly decreasing if each term is smaller than the one that precedes it.
- Every sequence of $n^2 + 1$ distinct real numbers contains a subsequence of length $n + 1$ that is either strictly increasing or strictly decreasing.

Proof

- Let $a_1, a_2, \ldots, a_{n^2+1}$ be a sequence of n^2+1 distinct real numbers.
- Associate an ordered pair with each term of the sequence, i.e. (i_k, d_k) to the term a_k, where i_k is the length of the longest increasing subsequence starting at a_k and d_k is the length of the longest decreasing subsequence starting at a_k.
- Suppose that there are no increasing or decreasing subsequences of length $n+1$.
- Then i_k and d_k are $\leq n$, for $k = 1, 2, \ldots, n^2+1$. By product rule, there are n^2 choices for (i_k, d_k).

Proof

- By the pigeonhole principle, two of these $n^2 + 1$ ordered pairs are equal. I.e. there exist terms in the sequence a_s and a_t with $s < t$ such that $i_s = i_t$ and $d_s = d_t$.
- Since terms in the sequence are distinct, either $a_s < a_t$ or $a_s > a_t$.
- If $a_s < a_t$ then because $i_s = i_t$ an increasing subsequence of length i_{t+1} can be built starting at a_s, by taking a_s followed by an increasing sequence of length i_t beginning at a_t. A contradiction.
- If $a_s > a_t$ the same reasoning shows that d_s must be greater than d_t, which is a contradiction.

Ramsey Theory

- The generalized pigeonhole principle can be applied to an important part of combinatorics called Ramsey theory, after the English mathematician F. P. Ramsey.
- Ramsey theory deals with the distribution of subsets of elements of sets.
- Assume that in a group of 6, each pair of individuals consists of two friends or two enemies. Show that there are either three mutual friends or three mutual enemies in the group.
  - A: one of the 6 people.
  - Of the 5 other people in the group, there are either 3 or more who are friends of A, or 3 or more who are enemies of A.
  - Since from the generalized pigeonhole principle, we have when 5 objects are divided into 2 sets, one of the sets has at least $\lceil 5/2 \rceil = 3$ elements.
  - And from this formulate the proof.

Ramsey Theory

- The Ramsey number $R(m, n)$, where m and $n \geq 2$, denotes the minimum number of people at a party such that there are either m mutual friends or n mutual enemies, assuming that every pair of people at the party are friends or enemies.
- What we saw is that $R(3, 3) \leq 6$.
- Some useful properties of Ramsey numbers:
  - $R(m, n) = R(n, m)$.
  - $R(2, n) = n$ for every positive integer $n \geq 2$.
  - The exact values of only nine Ramsey numbers $R(m, n)$ with $3 \leq m \leq n$ are known including $R(4, 4) = 18$.
  - Only bounds are known for many other Ramsey numbers, including $R(5, 5)$ which is known to satisfy $43 \leq R(5, 5) \leq 49$.