CSCI 150 Discrete Mathematics
Homework 10

Saad Mneimneh, Computer Science, Hunter College of CUNY

Solution

1. Find the greatest common divisor of 100 and 254 using prime factorization. What is their least common multiple?

   Solution

   $$100 = 2^2 \cdot 5^2$$
   $$254 = 2 \cdot 127$$

   The greatest common divisor can be obtained by choosing the smallest power for each prime factor. We have $2^1 \cdot 5^0 \cdot 127^0 = 2$.

2. Find the greatest common divisor of 100 and 254 using the Euclidean algorithm and express it as a linear combination of 100 and 254 like this: $\gcd(254, 100) = 254r - 100s$, where $r, s \geq 0$.

   Solution

254	100	54	46	8	6	2	0
1	0	1	-1	2	-11	13	-50
0	1	-2	3	-5	28	-33	127

   We conclude that $\gcd(254, 100) = 254 \cdot 13 - 100 \cdot 33$.

3. Let F_n be the n^{th} Fibonacci number. What is $\gcd(F_{2024}, F_{2023})$?

   Solution

   We can easily argue that $\gcd(F_{2024}, F_{2023}) = 1$, because the remainder of the division of F_n by $F_{n-1} = F_{n-2}$, since $F_n = F_{n-1} + F_{n-2}$. Therefore, the Euclidean algorithm will produce a Fibonacci sequence in reverse, starting with F_{2024}.

   $$F_{2024}, F_{2023}, \ldots, 1, 0$$

4. What do the following pairs of integers have in common: two consecutive numbers, two consecutive odd numbers, two consecutive Fibonacci numbers, two prime numbers, a prime number p and an integer a such that $p \not| a$, and a prime number p and an integer $a < p$?

   Solution

   They are all co-prime.

   - If $d|n$ and $d|n+1$, then $d|(n+1) - n = 1$, so $d = 1$.
   - If $d|n$ and $d|n+2$, then $d|(n+2) - n = 2$, so $d \in \{1, 2\}$. But since n is odd, $d = 1$.
   - See above exercise for consecutive Fibs.
   - If p and q are both primes, then they only share one common divisor: 1.
   - If p is prime and $p \not| a$, then a and p share only 1 as a common divisor.
   - If p is prime and $a < p$, then p is prime and $p \not| a$ (see above).

5. Show that if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

   Solution

   Since $a|bc$, then bc is a multiple of a, and we can write $bc = ma$. By the Fundamental Theorem of Arithmetic, all prime factors of a must show up on the left. But since $\gcd(a, b) = 1$, these factors must all be contributed by c. Therefore, $a|c$.

6. Given $n > 1$, let p be a prime number such that $n < p < 2n$ (by the way, there is always a prime between n and $2n$). Does p divide $\binom{2n}{n}$? Explain.

Solution

The answer is Yes. Observe that p divides $(2n)! = 1 \dots p \dots 2n$, but p does not divide $n!n!$, since otherwise, p must divide one of the factors in $\{1, 2, 3, \dots, n\}$, which are all less than p. Therefore, p divides the ratio, since it divides the numerator but not the denominator.

7. Imagine you have points on a circle labeled $0, 1, 2, \dots, 126$, so point 126 is followed by point 0. You start at point 0, and you repeatedly jump by 5, so you first land on point 5, then 10, then 15, etc... How many jumps do you need to land on point 1? Try to think about the mathematical concept needed to figure this out without guessing.

   Solution

   This can be captured by $5x \equiv 1 \pmod{127}$. So all we need is to find the inverse of 5 modulo 127 (which exists since 5 and 127 are coprime). This can be done using the Euclidean algorithm:

127	5	2	1	0
1	0	1	-2	
0	1	-25	51	

   So the inverse of 5 modulo 127 is 51. We can verify: $5 \cdot 51 = 255 = 2 \cdot 127 + 1$.

8. For each of these relations, specify whether it is reflective, symmetric, anti-symmetric, and transitive.

   - The subset relation on the power set of some set S
   - The relation $\leq$ on $\mathbb{R}$
   - The relation $<$ on $\mathbb{Z}$
   - The relation "shared a class with" on the set of students at Hunter College, where two students share a class if there is a class they are both enrolled in this semester.
   - The relation given by

     $$\{(a, c), (a, f), (a, h), (b, h), (c, f), (c, h), (d, h), (e, h), (f, h), (g, h)\}$$

   - The relation R on $\mathbb{N}$ where $(a, b) \in R$ means $a|b$
   - The relation R on $\mathbb{N}$ where $(x, y) \in R$ means $x < y + 2$

Solution

I will not provide proofs for the following claims:

- Reflexive, anti-symmetric, transitive.
- Reflexive, anti-symmetric, transitive.
- Not reflexive, anti-symmetric, transitive.
- Reflexive, symmetric, not transitive.
- Not reflexive, anti-symmetric, transitive.
- Reflexive, anti-symmetric, transitive.
- Reflexive, not anti-symmetric, not symmetric, not transitive.

9. Consider the following relation on $\mathbb{N} \times \mathbb{N}$ (the set of ordered pairs of positive integers):

$$(a, b) \equiv (c, d) \Leftrightarrow ab = cd$$

Prove that this is an equivalence relation and prove that for any integer $n \in \mathbb{N}$, there exist classes of equivalence of size n. *Hint*: Think about why this is the same as saying that there exist integers that have n divisors.

Are there finitely many or infinitely many classes of equivalence of size 1? of size 2?

Solution

This relation is reflexive since $(a, b) \equiv (a, b)$. It is also symmetric, since $(a, b) \equiv (b, a)$. Finally, it is transitive since, if $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$, then $(a, b) \equiv (e, f)$.

Now, consider the set of powers of 2: $\{1, 2, 4, 8, \ldots\}$. Each number is of the form 2^{n-1}, for $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$. The integer 2^{n-1} has n divisors $\{1, 2, 4, \ldots, 2^{n-1}\}$. This means there are n pairs of integers whose product is equal to 2^{n-1} (this is true when n is even and when n is odd). Here are some examples:

$n = 4, \{1, 2, 4, 8\} : (1, 8), (8, 1), (2, 4), (4, 2)$

$n = 5, \{1, 2, 4, 8, 16\} : (1, 16), (16, 1), (2, 8), (8, 2), (4, 4)$

So for every n, there is a class of equivalence of size n. There is only 1 class of equivalence of size 1: $\{(1, 1)\}$. There are infinitely many classes of equivalence of size 2: $\{(1, 2), (2, 1)\}, \{(1, 3), (3, 1)\}, \ldots$ (primes).

10. Every non-empty subset of $\mathbb{N}$ (whether it's finite or infinite) has a minimum. One can't say the same about $\mathbb{Z}$. Find a total order relation $\prec$ on $\mathbb{Z}$ such that every non-empty subset of $\mathbb{Z}$ has a minimum under the $\prec$ relation.

Solution
Consider the following relation on $\mathbb{Z}$:

$$x \prec y \Leftrightarrow \begin{cases} |x| < |y|, \text{or} \\ \\ |x| = |y| \text{ and } x < y \end{cases}$$

This is anti-symmetric:

$$x \prec y \Rightarrow$$

$$\text{(either) } |x| < |y| \Rightarrow |x| \neq |y| \text{ and } |y| \not< |x| \Rightarrow y \not\prec x$$

$$\text{(or) } |x| = |y| \text{ and } x < y \Rightarrow |y| = |x| \text{ and } y \not< x \Rightarrow y \not\prec x$$

This is also transitive: if $x \prec y$ and $y \prec z$, then (4 cases)

- $|x| < |y|$ and $|y| < |z| \Rightarrow |x| < |z| \Rightarrow x \prec z$
- $|x| < |y|$ and $|y| = |z| \Rightarrow |x| < |z| \Rightarrow x \prec z$
- $|x| = |y|$ and $|y| < |z| \Rightarrow |x| < |z| \Rightarrow x \prec z$
- $|x| = |y|$ and $x < y$ and $|y| = |z|$ and $y < z \Rightarrow |x| = |z|$ and $x < z \Rightarrow x \prec z$

Therefore, the relation $\prec$ is a partial order relation (in fact it is total since every pair of integers is ordered by $\prec$). Under this relation, every subset of $\mathbb{Z}$ has a minimum, since the absolute value cannot decrease indefinitely and for any given absolute value, there are at most two integers that can achieve it.

Note: Another solution to this problem is to consider any bijection $f : \mathbb{Z} \to \mathbb{N}$, and define the relation $\prec$ on $\mathbb{Z}$ as:

$$x \prec y \Leftrightarrow f(x) < f(y)$$