Mock Exam 1 Solution

Which of the following linear combination has integer solutions for s and t?

- $1 = 104\,s + 76\,t$
- $2 = 104\,s + 76\,t$
- $3 = 104\,s + 76\,t$
- √ $4 = 104\,s + 76\,t$
- $6 = 104\,s + 76\,t$

Used the equation below to determine the multiplicative inverse of 23 mod 87 in the least non-negative residue form. $1 = 9 * 87 - 34 * 23$

- 9
- √ 53
- -34
- 73
- 71

The three simultaneous congruences

$$x \equiv 0 \pmod{3}$$
$$x \equiv 0 \pmod{9}$$
$$x \equiv 0 \pmod{27}$$

- are equivalent to simply writing $x \equiv 0 \pmod{3}$.
- cannot be solved since 3, 9, and 27 are not (pairwise) relatively prime.
- are equivalent to simply writing $x \equiv 0 \pmod{9}$.
- cannot be solved since x^(-1) does not exist, since 0 has no inverse.
- √ are equivalent to simply writing $x \equiv 0 \pmod{27}$.

Suppose x satisfies the two simultaneous linear congruences $x \equiv 4 \pmod{17}$ and $3x \equiv 1 \pmod{10}$.

- Then $x \equiv 7 \pmod{10}$.
- Then $x \equiv 7 \pmod{27}$.
- Then $x \equiv 12 \pmod{17}$.
- Then $x \equiv 67 \pmod{70}$.
- √ Then $x \equiv 157 \pmod{170}$.

According to Fermat's Little Theorem, which of the following is an inverse of 7^7 (mod 79)?

- 7^9
- 7^69
- 7^70
- √ 7^71
- 7^72

Simplifying 3^703 (mod 71) can be done

- using Fermat's Little Theorem, and it's congruent to -27 (mod 71).
- using Fermat's Little Theorem, and it's congruent to -11 (mod 71).
- √ using Fermat's Little Theorem, and it's congruent to -44 (mod 71).
- using Bézout's Theorem, and it's congruent to -44 (mod 71).
- using Bézout's Theorem, and it's congruent to -11 (mod 71).

Let P(n) be "1 + 2 + 3 + … + 2n = n(2n+1) whenever n is a positive integer". In order to prove P(n), we need to show that P(1) is true, and if P(k) is true then P(k+1) is true. Which of the following represent the P(k+1) statement?

- 1 + 2 + 3 … + 2k = k(2k+1)
- 1 + 2 + 3 … + 2k + (2k+1) = k(2k+1) + (2k+1)
- 1 + 2 + 3 … + 2k + (2k+1) = (k+1)(2k+3)
- 1 + 2 + 3 … + 2k + (2k+2) = (k+1)(2k+3)
- √ 1 + 2 + 3 … + 2k + (2k+1) + (2k+2) = (k+1)(2k+3)

If f(x) = O(1), (big-O of 1)

- f(x) must be a non-zero constant.
- f(x) must be equal to zero for all x.
- √ f(x) is bounded but can be larger than 1.
- f(x) must be between -1 and 1.
- f(x) = little-o(1) also.

If f(x) = o(x) (little-o of x), then f(x) could be equal to

- x - 2021x^2
- -2021 x log(x)
- x/2021
- x^2021
- √ 2021/x

The statement "Any simple polygon with at least four sides can be drawn as n-2 triangles", where n represents the number of sides of the polygon, can be proved by induction.
You are not being asked to prove this, but if you had to give a proof,
a) what would the Induction Hypothesis (also known as the Induction Assumption) be? State it clearly.
b) And then clearly state what would be the following statement that you would need to prove to complete the induction. (But don't prove anything.)

Answer:

a) Assume simple polygon with k sides can be drawn as k-2 triangles for k >= 4.
b) Want to show simple polygon with k+1 sides can be drawn as k-1 triangles.

Prove by induction, that for every positive integer n, $13^n \equiv 1 + 3n \ (mod\ 9)$.
Provide your full argument in the space below. Make sure to show all of your steps clearly.
*** You can use the equal sign as the congruence notation.**

Answer:

Basis Step: n = 1, 13^1 = 1 + 3 * 1 (mod 9)
13 = 4 (mod 9)
4 = 4 (mod 9)

Inductive Step: IH: Assume 13^k = 1 + 3k (mod 9) for k >= 1.
Want to show 13^(k+1) = 1 + 3(k+1) (mod 9)
13^k * 13 = 1 + 3k + 3 (mod 9)
13^k * 4 = 3k + 4 (mod 9)
by IH, (1 + 3k) * 4 = 3k + 4 (mod 9)
12k + 4 = 3k + 4 (mod 9)
3k + 4 = 3k + 4 (mod 9)

Prove by induction that (2n)! > (n!)(n!) for all positive integer n.
Provide your full argument in the space below. Make sure to show all of your steps clearly.

Answer:

Basis Step: n = 1, (2*1)! > (1!)(1!)

2 > 1

Induction Step: IH: Assume (2k)! > (k!)(k!) for k >= 1.

Want to show [2(k+1)]! > (k+1)! * (k+1)!

(2k + 2)! > (k!) (k+1) (k!) (k+1)

(2k)! * (2k+1) (2k+2) > (k!)(k!) (k+1) (k+1)

by IH, (2k)! > (k!)(k!) and (2k+1) (2k+2) > (k+1) (k+1) for k >= 1

Thus, (2k)! * (2k+1) (2k+2) > (k!)(k!) (k+1) (k+1)

or

[2(k+1)]! = (2k + 2)! = (2k)! * (2k+1) (2k+2)

by IH, > (k!)(k!) (2k+1) (2k+2)

> (k!)(k!) (k+1) (k+1) = (k+1)! * (k+1)!

Do there exist functions f(x) and g(x) such that f(x) = O(g(x)) and g(x)=o(x^2)?
If yes, give an example of the pair f(x) and g(x) in the space below and clearly identify which is f(x) and which is g(x).
If it's not possible, briefly explain why that's the case.

Answer: f(x) = x, g(x) = x.

f(x) = O(g(x)) means lim f(x)/g(x) is bounded

g(x)=o(x^2) means lim g(x)/x^2 = 0, which g(x) could be x.

If g(x) = x, we want lim f(x)/x to be bounded, f(x) could be x as well. since lim x/x = 1, which is bounded.

Arrange the following functions in a list so that each function is big-O of the next function. Label the functions from A to F in order, where A as the slowest growing and F as the fastest. Answer:

2021n log(n)	A. 2021/n
n^2021	B. n/2021
n/2021	C. 2021n log(n)
(2021n)!	D. n^2021
(2021)^n	E. 2021^n
2021/n	F. (2021n)!

a) Find all values of x in congruence notation such that when x divided by 4, the remainder is 3; when x divided by 5, the remainder is 2; and when x divided by 7, the remainder is 1.
b) Find all the numbers between 2021 to 2345 that satisfied the conditions in part a.

Answer:

a) x = 3 (mod 4) = 7
   x = 2 (mod 5) = 7   x = 7 (mod 20) = -13
   x = 1 (mod 7) = -13   x = -13 (mod 140)   → x = 127 (mod 140)

b) 127 + 140*15 = 127 + 2100 = 2227
   2227 – 140 = 2087
   2227 + 140 = 2367   → 2087, 2227

Find the multiplicative inverse of 65(mod 67).
Make sure your answer is in the least non-negative residue form. Show all your work and the calculations.
Answer:
Find gcd(65, 67) using Euclidean Algorithm:

$67 = 65(1) + 2$
$65 = 2 (32) + 1$

gcd(65,67) = 1, thus inverse of 65(mod 67) exists.
Find $65s + 67t = 1$ using extended Euclidean Algorithm:

$1 = 65(1) + 2(-32)$
$= 65(1) + [67(1) + 65(-1)](-32)$
$= 65(33) + 67(-32)$

Inverse of 65(mod 67) = 33 (mod 67).

Solve for all values of x where $18x \equiv 6 \pmod{46}$.
Make sure your answer is in the least non-negative residue form. Show all your work and the calculations.
Answer:
Find gcd(18, 46) using Euclidean Algorithm:

$46 = 18(2) + 10$
$18 = 10(1) + 8$
$10 = 8(1) + 2$
$8 = 2(4) + 0$

gcd(18, 46) = 2, 2|6, the solutions exist.
Find $18s + 46t = 2$ using extended Euclidean Algorithm:

$2 = 10(1) + 8(-1)$
$= 10(1) + [18(1) + 10(-1)](-1)$
$= 10(2) + 18(-1)$
$= [46(1) + 18(-2)](2) + 18(-1)$
$= 18 (-5) + 46 (2)$

Scale $18x + 46k = 6$

$[18 (-5) + 46 (2) = 2] * 3$
$18 (-15) + 46 (6) = 6$

$x = -15 \pmod{46/2}$
$x = -15 \pmod{23}$
$x = 8 \pmod{23}$

Solve for x in the least non-negative residue form that $x \equiv (4321)^{601} \pmod{31}$.
Show all your work and the calculations.
Answer:
$4321 - 3100 \rightarrow 1221 - 1240 \rightarrow -19 + 31 \rightarrow 12$
4321 (mod 31) = 12, 31 is a prime and gcd(12, 31) = 1, FLT applies.
By FLT, 12^30 = 1 (mod 31).
4321^601 (mod 31) = 12^601 = (12^30)^20 * 12^1 = 1^20 * 12 = 12 (mod 31)

The following statement is either True or False. If it's always True, write True below and very briefly explain why it must be True. If it is not always True, write False below and show it is False by an example:
If a divides bc but a does not divide b, then a must divides c.
Answer: This statement is False, let a = 12, b = 3, and c = 4.
12|3*4, but 12 does not divide 3 and 4.