Math 150

Midterm 2 ANSWERS

April 4, 2015

1. (20 points)

Answer:

a) Write the integer 1050 as a product of primes.

$1050 = (10)(105) = (5)(2)(5)(21) = (5^2)(2)(3)(7)$

b) Write the integer 319 as a product of primes. (Hint: $\sqrt{319} \approx 17.86$.)

Here you should check every prime up to 17. Doing so quickly gives $319 = (11)(29)$.

c) Convert the decimal (base-10) integer 131 into binary notation.

Notice that $128 = 2^7$, and 131 is 3 more than 128. So $131 = 2^7 + 3 = 2^7 + 2^1 + 2^0$, so in binary,

$$(131)_{10} = (10000011)_2.$$

d) Multiply the binary numbers 111 and 101, and convert your answer into decimal.

$(111)(101) = 11100 + 111 = 100011$. In decimal, this is $2^5 + 2^1 + 2^0 = 35$.

2. (30 points) Mark the following statements as True or False. If a statement is false, find a counterexample that shows why it is false. (If it is true, you do not need to explain why.) All variables represent integers.

Answer:

a) If $x \equiv 4 \pmod 6$ and $y \equiv 2 \pmod 6$, then $x + y \equiv 0 \pmod 6$.

This is true. (It is essentially Theorem 5 of Chapter 4.1 in the book.)

b) If $x \equiv 5 \pmod 6$ and $y \equiv -2 \pmod 6$, then $x \cdot y \equiv 2 \pmod 6$.

Also true. (Same theorem as before; just note that $-10 \equiv 2 \pmod 6$.)

c) If $x \equiv 2 \pmod 6$ and $y \equiv 2 \pmod 6$, then $\frac{x}{y} \equiv 1 \pmod 6$.

This is false. Division only works if the numbers you're dividing are relatively prime to the modulus. In this case, you can take, for example, $x = 8$ and $y = 2$. Then $\frac{x}{y} = 4$, and $4 \not\equiv 2 \pmod 6$.

d) If x is not divisible by 6, then $x^5 \equiv 1 \pmod 6$.

False. This would be Fermat's Little Theorem if 6 were prime. But 6 is not prime. A counterexample is $x = 2$, for which $2^5 = 32 \equiv 2 \pmod 6$.

e) There exists x such that $2x \equiv 1 \pmod 5$.

True. This is guaranteed by the fact that 2 and 5 are relatively prime.

f) There do not exist two different values of x such that $2x \equiv 1 \pmod 5$.

False. $x = 3$ and $x = 8$ are both solutions. The value of x is unique mod 5, but not unique as an integer. (And all variables represent integers, as stated above.)

3. (20 points)

Answer:

a) Use the Euclidean Algorithm to show that gcd(125,61)=1. Then find integers s and t such that $125s + 61t = 1$.

$125 = 61(2) + 3$
$61 = 3(20) + 1$
So $1 = 61 - 3(20) = 61 - (125 - 61(2))20 = 61 - 125(20) + 61(40) = 61(41) - 125(20)$. So $s = -20$ and $t = 41$.

b) Use your work above to solve the congruence $61x \equiv 4 \pmod{125}$. Find the smallest positive integer x that is a solution.

If $61x \equiv 4 \pmod{125}$, then $(41)(61x) \equiv (41)(4) \pmod{125}$. So $x \equiv 164 \pmod{125}$. But the smallest solution is $x = 164 - 125 = 39$.

4. (20 points)

Answer:

a) Write pseudocode for an algorithm that takes the list of integers $(a_1, a_2, \ldots, a_n)$ and returns a number equal to the number of positive integers in the list minus the number of negative integers in the list.

procedure PositiveMinusNegative($a_1, a_1, \ldots, a_n$: list of integers):
  pos := 0
  neg := 0
  for i in $(1, n)$ do
    if $(a_i > 0)$ then pos := pos + 1
    if $(a_i < 0)$ then neg := neg + 1
  return (pos - neg)

b) Suppose that $n = 3$, that is, that the list has three elements. What possible values could be returned by this function? (In mathematical language, what is the *range* of this function?) Give examples to support your answer.

The possible values returned are $\{-3, -2, -1, 0, 1, 2, 3\}$ For example, the input $(1, 1, 1)$ returns 3, $(1, 1, 0)$ returns 2, $(1, 0, 0)$ returns 1, $(0, 0, 0)$ returns 0, $(-1, 0, 0)$ returns -1, $(-1 - 1, 0)$ returns -2, and $(-1, -1, -1)$ returns -3.

5. (20 points)

Answer:

a) Compute 3^{7941} **mod** 7.

By Fermat's Little Theorem, $3^6 \equiv 1 \pmod 7$. We compute $7941 = 6(1323) + 3$. So

$$3^{7941} = 3^{6(1323)+3} \equiv 1^{1323} 3^3 \pmod 7.$$

Now we can finish the computation by simply computing $3^3 = 27$ and 27 **mod** $7 = 6$.

b) Compute 6^{17} **mod** 20.

This is best done by repeated squaring. We compute

$$6^2 = 36 \equiv 16 \pmod{20}$$

$$6^4 \equiv 16^2 \equiv (-4)^2 \equiv 16 \pmod{20}$$

and this is already enough information to realize that 6 raised to any power of 2 will be congruent to 16 mod 20. So

$$6^{17} = 6^{16} 6^1 \equiv (16)(6) \equiv 96 \equiv 16 \pmod{20}$$

and the answer is 16.

6. (30 points)

Answer:

a) Show that $f(n) = n^2 + 2n + 7$ is $O(n^2)$ from the definition of big-O notation, that is, by finding C and k that work.

Let $k = 1$, so that $n > 1$. Then $n^2 > 1$ also. So $2n < 2n^2$ and $7 < 7n^2$. So

$$f(n) = n^2 + 2n + 7 < n^2 + 2n^2 + 7n^2 = 10n^2.$$

Therefore $C = 10$.

b) Show that $g(n) = n^2$ is not $O(n)$.

Assume that n^2 is $O(n)$. Then $n^2 < Cn$ for all $n > k$ and some C. So dividing by n, we get that $n < C$ for all $n > k$. But this is a contradiction; simply take n larger than C and k. So n^2 is not $O(n)$.

c) Find the smallest integer k such that $h(n) = 1^5 + 2^5 + 3^5 + \cdots + n^5$ is $O(n^k)$, and show why this works.

The smallest integer is $n = 6$. We have

$$1^5 + \cdots + n^5 \leq n^5 + \cdots + n^5 = n(n^5) = n^6.$$

The hard part is seeing that $n = 5$ does not work (this was not required for credit on this problem). This was done in example 11 in Chapter 3.2 in the book, so the complete argument will not be repeated here. The idea of the argument is that if you add up half of the terms from 1^5 to n^5, the sum is $\Omega(n^6)$.