MATH 150: Solutions to Practice Midterm 2, Fall 2010

Jonathan Pakianathan

November 14, 2014

1 Solutions

1(a) [6 points] Find the prime factorization for 630.

Answer: $630 = 2(315) = (2)(5)(63) = (2)(5)(3)(21) = (2)(5)(3)(7)(3) = 2^1 3^2 5^1 7^1$.

(b)[6 points] Find gcd(5040,1000).

Answer:

$$(5040) = 5(1000) + 40$$
$$(1000) = 25(40) + 0$$

$gcd(5040, 1000)$ is the last nonzero remainder 40.

(c)[6 points] Find the binary and hexadecimal representation for the number with decimal representation 151.

Answer:

$$151 = (2)(75) + 1$$
$$75 = (2)(37) + 1$$
$$37 = (2)(18) + 1$$
$$18 = (2)(9) + 0$$
$$9 = (2)(4) + 1$$
$$4 = (2)(2) + 0$$
$$2 = (2)(1) + 0$$

We stop when the quotient is < 2. Using this last quotient and the remainders read from the bottom up, we get if $(x)_{10} = 151$ then $(x)_2 = 10010111$. To change from binary to hexadecimal, group the binary digits in groups of 4 and convert to single hexadecimal digit (as one hexadecimal digit has 16 values just like 4 binary digits). Thus $(x)_{16} = 97$.
(d)[7 points]

$$B(m,n) = \begin{cases} m + nB(m+1, n-1) \text{ if } n > 1 \\ 2m \text{ if } n = 1 \end{cases}$$

Find $B(3,3)$.

Answer: $B(3,3) = 3 + 3B(4,2)$.
$B(4,2) = 4 + 2B(5,1) = 4 + 2(2(5)) = 24$.
Putting this into the top line we get $B(3,3) = 3 + 3(24) = 75$ as the final answer.

2. (a)[9 points] The following is the Euclidean Algorithm applied to the integers 29 and 12:

$$\begin{aligned} (29) &= 2(12) + 5 \\ (12) &= 2(5) + 2 \\ (5) &= 2(2) + 1 \\ (2) &= 2(1) + 0 \end{aligned}$$

Run the algorithm "backwards" to write 1=29s + 12t for suitable integers s and t.

Answer:

$$\begin{aligned} 1 &= 1(5) - 2(2) \\ 1 &= 1(5) - 2(1(12) - 2(5)) = 5(5) - 2(12) \\ 1 &= 5(1(29) - 2(12)) - 2(12) = -12(12) + 5(29) \end{aligned}$$

Thus $s = 5, t = -12$ work.

(b)[8 points] Use part (a) to find the multiplicative inverse for 12 modulo 29, i.e., the integer m such that

$$12m \equiv 1 \text{ modulo } 29.$$

Use the canonical representative modulo 29 as your answer. Thus your answer should be between 0 and 28 inclusive.

Answer: From (a), $m = -12$ is a multiplicative inverse of 12 modulo 29. Thus $m \equiv -12 + 29 \equiv 17$ modulo 29 also works and is the canonical representative modulo 29 of the multiplicative inverse of 12.

(c)[8 points] We describe a coding method used in Agency X. First we convert letters into numbers via
A=0,B=1,C=2,D=3,E=4,F=5,G=6,H=7,I=8,J=9,K=10,L=11,M=12,N=13,
O=14,P=15,Q=16,R=17,S=18,T=19,U=20,V=21,W=22,X=23,Y=24,Z=25.

Then the agency codes these via the function

$$f(x) = 7x + 10 \text{ modulo } 26.$$

Thus C is coded as 24 since $7(2) + 10 = 24$ and H is coded as 7 since $7(7) + 10 = 59 \equiv 7$ modulo 26.

As an agent of Agency X, you receive a coded letter to signal your next action. The coded number is 11. Use that 15 is the inverse of 7 modulo 26 to **find the original letter** by solving

$$11 = 7x + 10 \text{ modulo } 26.$$

Answer: $11 \equiv 7x + 10$ modulo 26. First note that this is the same as $1 \equiv 7x$ modulo 26. Now we can multiply both sides of the equation by the multiplicative inverse of 7, i.e., 15 to get:
$15 \equiv (15)(7x)$ modulo 26 which is the same as $15 \equiv x$ modulo 26 as $(7)(15) \equiv 1$ modulo 26. Thus $x = 15$ and so the original letter was P.

3(a)[6 points] **Fill in the table below.**

y	$a_1 = y \mod 2$	$a_2 = y \mod 7$
0	0	0
1	1	1
2	0	2
3	1	3
4	0	4
5	1	5
6	0	6
7	1	0
8	0	1
9	1	2
10	0	3
11	1	4
12	0	5
13	1	6

(b)[7 points] Use the Chinese Remainder Theorem to find a formula for an integer y in the range 0 to 13 with remainders a_1 modulo 2 and a_2 modulo 7 respectively. More specifically $y = Ca_1 + Da_2 \mod 14$ for certain integers C and D, find C and D. **You should use the Chinese Remainder Formula to get your answer to receive full credit.**

Answer:

We have $m_1 = 2, m_2 = 7$. Computing we get $M = (2)(7) = 14, M_1 = 7, M_2 = 2$.

We need to solve for y_1 such that $M_1 y_1 \equiv 1$ modulo m_1 or in other words such that $7y_1 \equiv 1$ modulo 2 or in other words $y_1 \equiv 1$ modulo 2. Clearly $y_1 = 1$ works.

We need to solve for y_2 such that $M_2 y_2 \equiv 1$ modulo m_2 or in other words

such that $2y_1 \equiv 1$ modulo 7. $y_2 = 4$ works as $(2)(4) = 8 \equiv 1$ modulo 7.

Thus we obtain solution $y = M_1 y_1 a_1 + M_2 y_2 a_2 = (7)(1)a_1 + (2)(4)a_2 = 7a_1 + 8a_2$ modulo $M = 14$.

One can check this answer against the table in (a) to see that it does recover the original input modulo 14. Other answers are possible if one uses different valid y_1, y_2 so just make sure to check that your answer inverts the table in (a), i.e. recovers the original y modulo 14 from a_1 and a_2.

(c)[12 points] Use Fermat's little theorem to find the canonical representatives for 2^{323} modulo 5 and modulo 11. (**Show your work!**)

Answer: Fermat's little theorem says that $2^{5-1} = 2^4 \equiv 1$ modulo 5 as $p = 5$ is a prime and p does not divide $a = 2$. Then we note that $2^{323} = 2^{4(80)+3} = (2^4)^{80} * 2^3 \equiv 1^{80} * 2^3 \equiv 8$ modulo 5.

Fermat's little theorem says that $2^{11-1} = 2^{10} \equiv 1$ modulo 11 as $p = 11$ is a prime and p does not divide $a = 2$. Then we note that $2^{323} = 2^{(10)(32)+3} = (2^{10})^{32} * 2^3 \equiv 1^{32} 2^3 \equiv 8$ modulo 11.

4(a)[10 points] Prove the following equality for all integers $n \geq 1$ using the Principle of Mathematical Induction:

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = (\frac{n(n+1)}{2})^2$$

Answer: Denote the equality above by $P(n)$. Note that
$P(1) : 1^3 = (\frac{1(1+1)}{2})^2 = 1^2$ is true.

Now proceeding by a proof by induction, we assume $P(n)$ has been proven true (inductive hypothesis) and will use it to show $P(n+1)$ is also true.

Starting with the left hand side (LHS) of $P(n+1)$ we have:

$$1^3 + 2^3 + 3^3 + \cdots + n^3 + (n+1)^3$$

which equals the LHS of $P(n)$ plus an extra $(n+1)^3$ so using the inductive

hypothesis we have

$$\begin{aligned} 1^3 + 2^3 + 3^3 + \cdots + n^3 + (n+1)^3 &= (\frac{n(n+1)}{2})^2 + (n+1)^3 \\ &= \frac{(n+1)^2}{4}[n^2 + 4(n+1)] \\ &= \frac{(n+1)^2}{4}[(n+2)^2] \\ &= (\frac{(n+1)(n+2)}{2})^2 \end{aligned}$$

which is the desired right hand side (RHS) of P(n+1). Thus we have confirmed $P(n) \to P(n+1)$ for all $n \geq 1$ and $P(1)$ and so by the principle of mathematical induction, have proven $P(n)$ is true for all $n \geq 1$.

(b)[5 points] Let $P(n)$ be the statement that postage of n cents can be formed using just 4-cent and 5-cent stamps. State which of the statements $P(1), P(2), \ldots, P(14), P(15)$ are true and which are false.

Answer: $P(1), P(2), P(3), P(6), P(7), P(11)$ are false. P(4) (use one 4-cent), P(5) (use one 5-cent), P(8) (use two 4-cent), P(9) (use one of each), P(10) (use two 5-cent), P(12) (use three 4-cent), P(13) (use two 4-cent, one 5-cent), P(14) (use one 4-cent, two 5-cent), P(15) (use three 5-cent) are true.

(c)[10 points] Based on your results in (b), prove that $P(n)$ is true for all $n \geq N$ for suitable N. State what N is and prove your result by a form of induction.

Answer: $N = 12$, We have $P(12), P(13), P(14), P(15)$ true by (b). Then note that if $P(n)$ is true then $P(n+4)$ is true as we can add another 4-cent stamp to go from n cents of postage to $n+4$ cents of postage. This gives for all $n \in \mathbb{Z}_+, P(n) \to P(n+4)$ and so we get:
$P(12) \to P(16) \to P(20) \to \cdots \to P(12+4k) \to \ldots$
$P(13) \to P(17) \to P(21) \to \cdots \to P(13+4k) \to \ldots$
$P(14) \to P(18) \to P(22) \to \cdots \to P(14+4k) \to \ldots$
$P(15) \to P(19) \to P(23) \to \cdots \to P(15+4k) \to \ldots$

As $12, 13, 14, 15$ are equivalent to $0, 1, 2, 3$ modulo 4 and every integer is congruent to either $0, 1, 2, 3$ modulo 4, we see that every integer ≥ 12 can be obtained by adding a (nonnegative) multiple of 4 to one of $12, 13, 14, 15$ and so by the process above, we have proven $P(n)$ is true for every $n \geq 12$ using this "generalized form of mathematical induction".