UNIVERSITY OF MANITOBA
COURSE: MATH 2170
DATE & TIME: March 18, 2019, 16:30–17:15
TEST 2 Solutions
DURATION: 45 minutes

---

[6] 1. Which of the following numbers can be written as a sum of two squares?
If not, explain why not.
If it can be, find such a sum.

(a) $m = 360$ (b) $n = 375$

Solution: $360 = 6^2 \times 10$.
Clearly $10 = 1^2 + 3^2$, so $360 = 6^2 + 18^2$.

$375 = 3 \times 5^3$, so 3 occurs as a factor an odd number of times and therefore 375 cannot be written as a sum of two squares.

Remark: The best solutions to these two part were of relatively equal difficulty, and so the marks were split equally between the two parts.

[3] 2. (a) Find the prime power factorization of $\phi(140^2)$.

Solution: $140^2 = (4 \times 5 \times 7)^2 = 2^4 5^2 7^2$.
Therefore,

$\phi(140) = \phi(2^4)\phi(5^2)\phi(7^2) = 2^3 \times (5^2 - 5) \times (7^2 - 7) = 2^3 \times 20 \times 42 = 2^6 \times 3 \times 5 \times 7$.

[3] (b) Prove that if m is odd, then $\phi(4m) = 2\phi(m)$.

Solution: If m is odd then $(4, m) = 1$ so $\phi(4m) = \phi(4)\phi(m) = 2\phi(m)$.

UNIVERSITY OF MANITOBA
COURSE: MATH 2170
TEST 2 Solutions
DATE & TIME: March 18, 2019, 16:30–17:15
DURATION: 45 minutes

---

[6] 3. Find all solutions, if any, of each of the two following congruences.

(a) $60x \equiv 54 \pmod{90}$ (b) $42x \equiv 54 \pmod{90}$

Solution: $(60, 90) = 30$ but $30 \not| 54$, so congruence (a) does not have a solution.

$(42, 90) = 6$ and $6|54$ so we divide through by 6 and solve $7x \equiv 9 \pmod{15}$.

Many pathways to the answer are acceptable, but the fastest is (probably) to note that $2 \cdot 27 = 14 \equiv -1 \pmod{15}$ and so $-x \equiv 2 \cdot 9 = 18 \equiv 3 \pmod{15}$, or $x \equiv 12 \pmod{15}$.

Therefore $x \equiv 12$, 27, 42, 57, 72, or 87 $\pmod{90}$.

Remark: The best solution to part (a) is trivial, whereas part (b) genuinely requires several different steps of work. The marks are split $2 + 4$; part of what was being tested here was your ability to recognize the difference between the two parts.

An *essential part* of any answer lies in actually expressing the full answer modulo 90.

UNIVERSITY OF MANITOBA
COURSE: MATH 2170
DATE & TIME: March 18, 2019, 16:30–17:15
TEST 2 Solutions
DURATION: 45 minutes

---

[8] 4. Consider the congruence $x^2 + 12x + 14 \equiv 0 \pmod{21}$.

Solve this congruence by first reducing it to simpler congruences (modulo other bases) and then combining the solutions to solve the original problem.

Solution: $21 = 3 \times 7$ and $(3, 7) = 1$, so by the Chinese Remainder Theorem, this congruence is equivalent to the pair of congruences

$$x^2 + 12x + 14 \equiv x^2 + 2 \equiv 0 \pmod{3} \qquad (A)$$

and

$$x^2 + 12x + 14 \equiv x^2 + 5x \equiv x(x + 5) \equiv 0 \pmod{7} \qquad (B)$$

From the first congruence, $x \equiv 1 \pmod{3}$ or $x \equiv 2 \pmod{3}$, and so for some t, $x = 3t + 1$ or $x \equiv 3t + 2$.

From the second congruence, $x \equiv 0 \pmod{7}$ or $x \equiv 2 \pmod{7}$.

We can combine these in four ways.

If $x = 3t + 1$ and $x \equiv 0 \pmod{7}$ then $3t + 1 \equiv 0 \pmod{7}$, or $t \equiv 2 \pmod{7}$. Thus for some s, $x = 3(7t + 2) + 1 = 21t + 7$.

If $x = 3t + 1$ and $x \equiv 2 \pmod{7}$ then $3t + 1 \equiv 2 \pmod{7}$, or $t \equiv 5 \pmod{7}$. Thus for some s, $x = 3(7s + 5) + 1 = 21t + 16$.

If $x = 3t + 2$ and $x \equiv 0 \pmod{7}$ then $3t + 2 \equiv 0 \pmod{7}$, or $t \equiv 4 \pmod{7}$. Thus for some s, $x = 3(7t + 4) + 2 = 21t + 14$.

If $x = 3t + 2$ and $x \equiv 2 \pmod{7}$ then $3t + 2 \equiv 2 \pmod{7}$, or $t \equiv 0 \pmod{7}$. Thus for some s, $x = 3(7t) + 2 = 21t + 2$.

The four solutions are $x \equiv 2 \pmod{21}$, $x \equiv 7 \pmod{21}$, $x \equiv 14 \pmod{21}$, and $x \equiv 16 \pmod{21}$.

Remarks: One of the most common errors was failing to reduce the coefficients modulo 3 and modulo 7 in equations (A) and (B). The coefficients were chosen so that the simplified congruences would be trivial to solve.

We learned systematic methods for solving these kinds of problems, and although I was willing to accept "trial and error", most attempted solutions by this method had a lot of errors or were incomplete.

UNIVERSITY OF MANITOBA
COURSE: MATH 2170
TEST 2 Solutions
DATE & TIME: March 18, 2019, 16:30–17:15
DURATION: 45 minutes

---

[6] 5. Find all solutions in positive integers to $11x + 5y = 82$.

For full marks, your solution must demonstrate the formal method learned in class.

Solution: Set up a small augmented matrix and do some column reductions.

11	$\boxed{5}$	82	$C_1 - 2C_2$
1	0	x	
0	1	y	
$*$	$*$		

$\boxed{1}$	5	82	$C_2 - 5C_1$
1	0	x	
-2	1	y	
$*$	$*$		

1	0	82
1	-5	x
-2	11	y
u	v	

We have new variables u and v. The first line of the reduced matrix gives $u = 82$, and then we take v as a parameter.

We get $x = 82 - 5v$ and $y = -164 + 11v$.

Remark: This is enough for full marks for the solution; I did not ask for a solution in vector form or for a "reduction of constants". You should be prepared for a question with those requirements on the final exam.

For positive solutions we need $82 - 5v > 0$ or $16 \geq v$, and $-164 + 11v > 0$ or $v \geq 15$. This gives two positive solutions: $\langle\, x,\, y \,\rangle = \langle\, 2,\, 12 \,\rangle$ and $\langle\, x,\, y \,\rangle = \langle\, 7,\, 1 \,\rangle$.

Remarks: To reduce the constants, $-164 = 11(-15) + 1$, so set $v = k + 15$ to get $x = 7 - 5k$ and $y = 1 + 11k$.

In vector form the two forms of the general solution that we have found are:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 82 \\ -164 \end{bmatrix} + v \begin{bmatrix} -5 \\ 11 \end{bmatrix} = \begin{bmatrix} 7 \\ 1 \end{bmatrix} + k \begin{bmatrix} -5 \\ 11 \end{bmatrix}$$

UNIVERSITY OF MANITOBA
COURSE: MATH 2170
DATE & TIME: March 18, 2019, 16:30–17:15
TEST 2 Solutions
DURATION: 45 minutes

---

[4] 6. Given that $5 \cdot 19 \equiv 1 \pmod{48}$ and that $a^{19} \equiv 2 \pmod{65}$, find a (as a least residue modulo 65).

There is an important named theorem that you must mention at one point in your solution.

Solution: Only one student noticed the serious error in the statement of this question: in fact, $5 \cdot 19 \equiv -1 \pmod{48}$.

It is still possible to solve the problem using the corrected statement (for then the multiplicative inverse of 19 modulo 48 is $-5 \equiv 43 \pmod{48}$. But that would require a lot more computation than I had intended for this test.

Remark: It is of course entirely possible to generate an "answer" by the standard method that we learned. Almost half of you did so, correctly, as follows:

Solution: By Euler's Theorem, if $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Note that $65 = 5 \times 13$, so $\phi(65) = 4 \times 12 = 48$.

So $19 \times 5 = \phi(65)k + 1$ for some k

Then $(a^{19})^5 \equiv a^{\phi(65)k} a \equiv a \pmod{65}$.

Therefore $a \equiv 2^5 = 32 \pmod{65}$.

Remark: The correct version of this question would have "19" replaced everywhere by "29".