**UNIVERSITY OF MANITOBA**
COURSE: MATH 2170
DATE & TIME: April 12, 2019, 18:00–21:00
FINAL EXAMINATION
DURATION: 3 hours EXAMINER: T. Kucera

---

I understand that cheating is a serious offence:

**Signature**: ______________________________
(*In Ink*)

**Please read the instructions on the back of this page.**

**UNIVERSITY OF MANITOBA**
COURSE: MATH 2170
FINAL EXAMINATION
DATE & TIME: April 12, 2019, 18:00–21:00
DURATION: 3 hours
EXAMINER: T. Kucera

---

# INSTRUCTIONS

I. No texts, notes, or other aids are permitted, including progammable electronic calculators.

   No cellphones, electronic translators, or any WiFi enabled devices are permitted.

II. **Simple non-programmable calculators are permitted.**

III. This exam has 16 pages in all, including the cover page (identification page) and this instruction page. The reverse side of each question page is available for rough work or for the continuation of the work on that question page.

   Please **indicate clearly** on the question page if your work continues on the back.

   Please check that you have all the pages.

IV. The value of each question is indicated in the lefthand margin beside the statement of the question. The total value of all questions is 150 points.

V. **Answer all questions on the exam paper** in the space provided beneath the question, or clearly indicate that your solution continues on the reverse side of the same page. Show the details of your solutions, unless instructed otherwise.

VI. Unless stated otherwise, all numbers in this exam are assumed to be integers.

VII. If the QR codes on your exam paper are deliberately defaced, your exam may not be marked.

This page will not be marked. You can use it for rough work.

**UNIVERSITY OF MANITOBA**
COURSE: MATH 2170
DATE & TIME: April 12, 2019, 18:00–21:00
FINAL EXAMINATION
DURATION: 3 hours EXAMINER: T. Kucera

---

[45] 1. **Note**: Each question in this section is worth 3 points, for a total of 45. Write a definition, state a theorem or example, or do a short calculation. No other explanation is required. Definitions and statements of theorems should be brief, clear, and accurate, and should not include examples or extra explanations.

(a) Define, with the correct notation, "$a$ divides $b$".

**Solution:** $a|b$ iff for some $d$, $ad = b$.

(b) Define, with the correct notation, the *least common multiple* of $a$ and $b$.

**Solution:** The definition adopted in the lectures was:
$[a, b] = m$ if $m \geq 0$, $a|m$, $b|m$, and if $a|n$ and $b|n$ then $m|n$.

Alternatively, for two marks only, we proved that this was equivalent to the text book definition:
$[a, b] = m$ if $m$ is a positive common multiple of $a$ and $b$, and if $n$ is any positive common multiple of $a$ and $b$ then $m \leq n$.

(c) State *The Division Algorithm*.

**Solution:** Given integers $a$ and $b$ with $a > 0$ there are unique integers $q$ and $r$, $0 \leq r < a$, such that $b = qa + r$.

(d) State the *Fundamental Theorem of Arithmetic*.

> **Solution:** Every integer $n > 1$ can be written (essentially) uniquely as a product of primes.
>
> **Variations**: "essentially uniquely" can be expressed in several ways, e.g. "uniquely up to order". You can also state this result in terms of the prime power factorization.

(e) State a *reduced residue system* modulo 18 consisting of least positive residues modulo 18.

> **Solution:** $\{1, 5, 7, 11, 13, 17\}$.
>
> **Note**: for the question as stated, there is a unique solution. Any other (correct) reduced residue system will score 2 marks.

(f) Define "prime number".

> **Solution:** An integer $p > 1$ is a *prime number* if it has exactly two positive divisors, 1 and $p$.
>
> Also acceptable: An integer $p > 1$ is a *prime number* if it has no non-trivial divisors.

(g) Define *Euler's function* $\phi$.

> **Solution:** For an integer $n > 1$, $\phi(n)$ is the number of elements in a reduced residue system modulo $n$.

(h) State *Euler's Theorem*.

**Solution:** If $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$.

(i) Define *primitive Pythagorean triple*.

**Solution:** $\langle x, y, z \rangle$ is a *primitive Pythagorean triple* if $x, y, z > 0$ are pairwise relatively prime and $x^2 + y^2 = z^2$.

(j) Let $m > 1$ and $(a, m) = 1$.
Define "the order of $a$ modulo $m$".

**Solution:** "the order of $a$ modulo $m$" is the least positive integer $t$ such that $a^t \equiv 1 \pmod{m}$.

(k) Let $m > 1$ and $(a, m) = 1$.
Define "$a$ is a primitive root modulo $m$".

**Solution:** "$a$ is a primitive root modulo $m$" if the order of $a$ modulo $m$ is $\phi(m)$.

---

(l) Let $m > 1$. Define "$a$ is a quadratic residue modulo $m$".

> **Solution:** "$a$ is a quadratic residue modulo $m$" if the congruence $x^2 \equiv a \pmod{m}$ has a solution.

(m) State Gauss's *Quadratic reciprocity law.*

> **Solution:** If $p$ and $q$ are distinct odd primes, then
> $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

(n) Let $f$ and $g$ be arithmetic functions. Define the *convolution* $f * g$.

> **Solution:**
> $$(f * g)(n) = \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right).$$
> Alternatively,
> $$(f * g)(n) = \sum_{d_1 d_2 = n} f(d_1) g(d_2).$$

(o) Let $f$ be an arithmetic function. Define "$f$ is multiplicative".

> **Solution:**
> $f$ is multiplicative if $f$ is not the constant function $0$ and for all $m$, $n$, if $(m, n) = 1$, then $f(mn) = f(m)f(n)$.

**. . . end of Question 1**

**UNIVERSITY OF MANITOBA**
COURSE: MATH 2170
DATE & TIME: April 12, 2019, 18:00–21:00
FINAL EXAMINATION
DURATION: 3 hours EXAMINER: T. Kucera

---

[12] 2. Find $d = (\,19822,\, 13838\,)$ and two integers $x$ and $y$ such that $19822x + 13838y = d$, using the algorithm as presented in the text and in class.

*Part of the point of this question is to test your knowledge and understanding of the algorithm. A "correct" solution by other methods will not receive full marks.*

**Solution:**

**Note:** A statement of the algorithm is included in this solution for completeness, but you did not have to write it out to receive full credit. The marks are for the table and computations following.

We learned the following formulas: $r_{-1} = a$, $r_0 = b$, $q_{i+1}$ is determined by division: $r_{i-1} = r_i q_{i+1} + r_{i+1}$, $0 \leq r_{i+1} < r_i$, so we get rules as follows (with $x_{-1} = 1$, $y_{-1} = 0$, $x_0 = 0$, and $y_0 = 1$):

$$\begin{cases} r_k &= r_{k-2} - q_k r_{k-1} \\ x_k &= x_{k-2} - q_k x_{k-1} \\ y_k &= y_{k-2} - q_k y_{k-1} \end{cases}$$

Therefore in this case:

| $q_{i+1}$ | $r_i$ | $x_i$ | $y_i$ |
|---|---|---|---|
| | 19822 | 1 | 0 |
| 1 | 13838 | 0 | 1 |
| 2 | 5984 | 1 | −1 |
| 3 | 1870 | −2 | 3 |
| 5 | 374 | 7 | −10 |
| | 0 | | |

Therefore $d = 374 = 7 \times 19822 - 10 \times 13838$.

Or, rather than writing an equation, $d = 374$, $x = 7$, $y = 10$.

[8] 3. Prove the following:

If $(a, m) = 1$, then there is $x$ such that $ax \equiv 1 \pmod{m}$, and any two such $x$ are congruent modulo $m$. If $(a, m) > 1$, then there is no such $x$.

**Solution:**

If $(a, m) = 1$, then there are $x$ and $y$ such that $ax+my = 1$. Thus $ax \equiv 1 \pmod{m}$.

If as well $ax' \equiv 1 \pmod{m}$ then $a(x - x') \equiv 0 \pmod{m}$, that is, $m|a(x - x')$.
Since $(a, m) = 1$, $m|(x - x')$, that is, $x \equiv x' \pmod{m}$,.

And finally, if there is an $x$ such that $ax \equiv 1 \pmod{m}$, then $m|(ax - 1)$;
that is, for some $y$, $my = ax - 1$, so $1 = ax - my$ and therefore $(a, m) = 1$.

**Alternatively** (for the last step) if $(a, m) = d > 1$ then $d$ is the least positive integer for which we can find $x$ and $y$ such that $ax + by = d$, and therefore in particular we cannot solve $ax + by = 1$.

**Remarks:** There was quite a bit of misunderstanding and confusion about what was needed for the proof of this fundamental theorem (Theorem 2.9 in Section 2.1). You cannot use the results of Section 2.2 (which depend on this result!) to prove it.

[5] 4. Prove the following:

Let $p$ be a prime number. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

**Solution:**

$x^2 \equiv 1 \pmod{p}$

if and only if $x^2 - 1 \equiv (x - 1)(x + 1) \equiv 0 \pmod{p}$

if and only if $p|(x - 1)(x + 1)$

if and only if (since $p$ is a prime) $p|x - 1$ or $p|x + 1$

if and only if $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

**Remark**: Note that $(\pm 1)^2 = 1$ always, and does not need proof!

---

[2] 5. (a) Complete the following by filling in the blanks:
The congruence $ax \equiv b \pmod{m}$ has solutions iff ________________________ ,

in which case there are ________________________ solutions.

**Solution:** The congruence $ax \equiv b \pmod{m}$ has solutions iff $(\,a,\, m\,)\,|b$ ,

in which case there are $(\,a,\, m\,)$ solutions.

[10] (b) Find the number of solutions to each of the following, and if there are solutions, find all the solutions.

$(a)$ $60x \equiv 140 \pmod{180}$ $(b)$ $35x \equiv 140 \pmod{180}$

**Solution:** Here, $(\,60,\, 180\,) = 60$ and $60 \not| 140$ , but $(\,35,\, 180\,) = 5$ and $5|140$ .
So $(a)$ has no solutions, but $(b)$ has 5 solutions.

The solutions, when they exist, are obtained by dividing through by the gcd: so for $(b)$ we need to solve $7x \equiv 28 \pmod{36}$ .
That is, $x \equiv 4 \pmod{36}$ .
Thus the solutions modulo 180 are 4, 40, 76, 112, and 148 .

[10] 6. Find all solutions to $\left\{ \begin{array}{rcl} x & \equiv & 5 \pmod{7} \\ x & \equiv & 3 \pmod{10} \end{array} \right\}$.

**Solution:**

[Chinese Remainder Theorem]

[I always find it most efficient to start with the largest modulus, but that is not a rule.]

$$\begin{array}{rcl} \therefore \quad x & = & 10k+3 \quad \text{for some } k \\ 10k+3 & \equiv & 5 \pmod{7} \\ 3k & \equiv & 2 \equiv 9 \pmod{7} \\ k & \equiv & 3 \pmod{7} \\ \therefore \quad k & = & 7t+3 \quad \text{for some } t \\ x & = & 10(7t+3)+3 \\ & = & 70t+33 \\ \therefore \quad x & \equiv & 33 \pmod{70} \end{array}$$

And the other way...

$$\begin{array}{rcl} \therefore \quad x & = & 7k+5 \quad \text{for some } k \\ 7k+5 & \equiv & 3 \pmod{10} \\ 7k & \equiv & -2 \equiv 28 \pmod{10} \\ k & \equiv & 4 \pmod{10} \\ \therefore \quad k & = & 10t+4 \quad \text{for some } t \\ x & = & 7(10t+4)+5 \\ & = & 70t+33 \\ \therefore \quad x & \equiv & 33 \pmod{70} \end{array}$$

---

[15] 7. Consider the system of linear diophantine equations

$$\begin{cases} 3x & +3y & +2z & = & 15 \\ 2x & +2y & +4z & = & 18 \end{cases}$$

Using the matrix method as taught in class and in the text, find all positive solutions.

*Part of the point of this question is to test your knowledge and understanding of the algorithm. A "correct" solution by other methods will not receive full marks.*

**Solution:** Reduce an augmented matrix by column operations and row operations. At each stage, choose your "pivot" point as the coefficient entry with the least positive absolute value, and furthest to the left.

"There are usually several valid pathways to a solution, but this problem is so straightforward that most of you should find the same solution." **Ha!** Fooled myself! There were 14 out of 18 mostly correct solutions, and I think there were 14 different ways of presenting the answer, including finding either x or y corresponding to the parameter!

You can always verify that a solution is correct by substituing the values obtained into the original equations, and computing.

$$\begin{array}{rrr|l} 3 & 3 & 2 & 15 \\ \boxed{2} & 2 & 4 & 18 \\ \hline 1 & 0 & 0 & x \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & z \end{array} \qquad C_2 - C_1,\ C_3 - 2C_1$$

$$\begin{array}{rrr|l} 3 & 0 & -4 & 15 \\ \boxed{2} & 0 & 0 & 18 \\ \hline 1 & -1 & -2 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array} \qquad R_1 - R_2$$

$$\begin{array}{rrr|l} \boxed{1} & 0 & -4 & -3 \\ 2 & 0 & 0 & 18 \\ \hline 1 & -1 & -2 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array} \qquad R_2 - 2R_1$$

$$\begin{array}{rrr|l} \boxed{1} & 0 & -4 & -3 \\ 0 & 0 & 8 & 24 \\ \hline 1 & -1 & -2 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{array} \qquad C_3 + 4C_1$$

Since $8|24$, there are solutions.

$$\begin{array}{rrr|r l}
1 & 0 & 0 & -3 & \qquad C_2 \leftrightarrow C_1 \\
0 & 0 & 8 & 24 & \qquad (1/8)R_2 \\
\hline
1 & -1 & 2 & & \\
0 & 1 & 0 & & \\
0 & 0 & 1 & &
\end{array}$$

$$\begin{array}{rrr|c}
1 & 0 & 0 & -3 \\
0 & 1 & 0 & 3 \\
\hline
1 & 2 & -1 & x \\
0 & 0 & 1 & y \\
0 & 1 & 0 & z \\
\hline
u & v & w &
\end{array}$$

So we take $w$ as a parameter and get $u = -3$, $v = 3$, $x = u + 2v - w = 3 - w$, $y = w$, $z = v = 3$.

For positive solutions, $y = w > 0$ and $x = 3 - w > 0$, so $0 < w < 3$.

The positive solutions are

$$\langle x, y, z \rangle = \langle 2, 1, 3 \rangle , \langle 1, 2, 3 \rangle .$$

---

[6] 8. Prove that every integer $n \geq 3$ appears as one or the other of the first two numbers in a Pythagorean triple.

**Solution:** A typical Pythagorean triple has the form $\langle\, x,\, y,\, z \,\rangle$ where for some $r > s$ ,

$$x = r^2 - s^2 \,, \qquad y = 2rs \qquad z = r^2 + s^2 \,.$$

Note that $(k+1)^2 - k^2 = 2k+1$ .

So if $n = 2k+1 \geq 3$ is odd, take $r = k+1$ and $s = k$ to get $x = n$ .

On the other hand, if $n = 2k \geq 3$ is even, then $k \geq 2$ and so we can take $r = k$ and $s = 1$ to get $y = n$ .

**Remark** So the two resulting triples are $\langle\, 2k+1,\, 2k(k+1),\, 2k^2+2k+1 \,\rangle$ and $\langle\, k^2-1,\, 2k, k^2+1 \,\rangle$ .

**Remark**: This really did depend on knowing the general form of a Pythagorean triple for an efficient solution. Some of you found much longer and more involved solutions.

[6] 9. Suppose that $g$ is a primitive root modulo $p$ , $p$ an odd prime.

Show that $g$ is *not* a quadratic residue modulo $p$ .

**Solution:** Suppose that $g \equiv a^2 \pmod{p}$ , where $a \not\equiv 0 \pmod{p}$ .

Since $g$ is a primitive root, for some $t$ , $a \equiv g^t \pmod{p}$ and so $g \equiv g^{2t} \pmod{p}$ .

But then $2t \equiv 1 \pmod{p-1}$ .

However, $(2, p-1) = 2$ and $2 \nmid 1$ , so $2t \equiv 1 \pmod{p-1}$ does not have any solutions.

**Solution:** There is a less elementary solution, using *Euler's criterion*, Theorem 2.38: the congruence $x^2 \equiv g \pmod{p}$ has a solution if and only if $g^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ .

But if $g$ is a primitive root, then $g$ has order $p-1$ , and so since $\frac{p-1}{2} < p-1$ , $g^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ .

---

10. Given: 3 is a primitive root modulo 31 .

[3] (a) Find the least positive residue of $3^{15}$ modulo 31.

There is a short and easy answer worth 3 points using theory; and a long and tedious solution by calculation worth only one point.

**Solution:** $(3^{15})^2 = 3^{30} \equiv 1 \pmod{31}$ by Fermat's Theorem, and $3^{15} \not\equiv 1 \pmod{31}$ since 3 is a primitive root, so $3^{15} \equiv -1 \pmod{13}$ .

[7] (b) 1. Which powers of 3 are square roots of $3^{15}$ modulo 31?
2. Which powers of 3 are fifth roots of $3^{15}$ modulo 31?

Explain your answers.

**Solution:** Since 15 is odd, $3^{15}$ has no square roots modulo 31.

Since $(5, 30) = 5$ and $5|15$ , $5t \equiv 15 \pmod{30}$ has a solution (modulo $6 = 30/5$) and there are 5 of them modulo 30 , namely 3, 9, 15, 21, 27 . So the fifth roots of $3^{15}$ modulo 31 are $3^3$ , $3^9$ , $3^{15}$ , $3^{21}$ , and $3^{27}$ .

[10] 11. Calculate the value of the Legendre symbol $\left(\frac{-33}{67}\right)$.

**Solution:**

$$\begin{aligned}
\left(\frac{-33}{67}\right) &= \left(\frac{-1}{67}\right)\left(\frac{3}{67}\right)\left(\frac{11}{67}\right) \\
&= (-1)\left(\frac{67}{3}\right)(-1)^{\left(\frac{67-1}{2}\right)\left(\frac{3-1}{2}\right)}\left(\frac{67}{11}\right)(-1)^{\left(\frac{67-1}{2}\right)\left(\frac{11-1}{2}\right)} \\
&= (-1)\left(\frac{1}{3}\right)(-1)\left(\frac{1}{11}\right) \\
&= -1
\end{aligned}$$

**Solution:**

$$\begin{aligned}
\left(\frac{-33}{67}\right) &= \left(\frac{34}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{17}{67}\right) \\
&= (-1)^{\frac{67^2-1}{8}}\left(\frac{67}{17}\right)(-1)^{\left(\frac{67-1}{2}\right)\left(\frac{17-1}{2}\right)} \\
&= (-1)\left(\frac{16}{17}\right)(1) \\
&= -1
\end{aligned}$$

Explanation of the calculation of $(-1)^{\frac{67^2-1}{8}}$.

We showed in general that if $m$ is odd then $8|(m^2-1)$.

Furthermore, in regards to this particular calculation, all that we care about is whether the fraction is odd or even. If we write $m = 8q + r$, $0 < r < 8$, we know that $r$ is odd and that $m^2 - 1 = 16(4q^2 + qr) + (r^2 - 1)$, so whether $(m^2-1)/8$ is odd or even only depends on whether $(r^2-1)/8$ is odd or even.

In this case, $67 = 8 \times 8 + 3$, and $(3^2-1)/8 = 1$ is odd.

---

12. Suppose that $F(n) = \sum_{d|n} f(d)$ for all positive integers $n$.

[3] (a) Define the *Möbius function* $\mu$.

**Solution:**

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is square-free} \\ 0 & \text{otherwise} \end{cases}$$

where $\omega(n)$ is the number of distinct prime divisors of $n$.

[3] (b) State the Möbius inversion formula.

**Solution:** If $F(n) = \sum\limits_{d|n} f(d)$ then $f(n) = \sum\limits_{d|n} \mu(d)F(n/d)$.

Alternatively:
If $F(n) = \sum\limits_{d|n} f(d)$ then $f(n) = \sum\limits_{d_1 d_2 = n} \mu(d_1)F(d_2)$.

Alternatively: If $F = f * 1$, then $f = \mu * F$.

[5] (c) Suppose that $f$ is multiplicative and for all primes $p$ and $k > 0$, $F(p^k) = p^{k-1}$. Find $f(72)$.

**Solution:** $f(72) = f(8)f(9)$ since $f$ is multiplicative.
Note that for $k \geq 2$, $\mu(p^k) = 0$ since trivially $p^k$ is not square free. So:
$f(8) = f(2^3) = \mu(1)F(8) + \mu(2)F(4) = F(8) - F(4) = 4 - 2 = 2$
and
$f(9) = f(3^2) = \mu(1)F(9) + \mu(3)F(3) = F(9) - F(3) = 3 - 1 = 2$,
by part (b) and the definition of $F$.
So $f(72) = 2 \cdot 2 = 4$.