Ve203 Discrete Mathematics

Sample Exercises for the First Midterm Exam

The following exercises are sample exercises of a difficulty comparable to those found the actual first midterm exam. The exam will usually include of 4 to 5 such exercises to be completed in 100 minutes.

Exercise 1. Find $x, y \in \mathbb{Z}$ such that $24x + 138y = \gcd(24, 138)$.
(1 Mark)

Solution. We apply the Euclidean algorithm:

$$\begin{aligned} 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 \end{aligned}$$

so $\gcd(24, 138) = 6$. Furthermore,

$$\begin{aligned} 6 &= 24 - 1 \cdot 18 \\ &= 24 - (138 - 5 \cdot 24) \\ &= 6 \cdot 24 - 1 \cdot 138 \end{aligned}$$

and we have $x = 6$, $y = -1$.

Exercise 2. Find all solutions of $140x \equiv 133 \pmod{301}$.
(2 Marks)

Solution. Since $140 = 2^2 \cdot 5 \cdot 7$ and $301 = 7 \cdot 43$, we see that $\gcd(140, 301) = 7$. Since $133 = 7 \cdot 19$, there exists seven solutions. We reduce the problem by dividng by 7, yielding,

$$20x \equiv 19 \pmod{43}$$

We now find an inverse of 20 modulo 43. using the Euclidean algorithm,

$$\begin{aligned} 43 &= 2 \cdot 20 + 3, \\ 20 &= 6 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1, \\ 1 &= 1 \cdot 1. \end{aligned}$$

We now find an inverse of 20 modulo 43. Using the Euclidean algorithm,

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - (20 - 6 \cdot 3) \\ &= -20 + 7 \cdot (43 - 2 \cdot 20) \\ &= 7 \cdot 43 - 15 \cdot 20 \end{aligned}$$

so -15 is the inverse. We then find

$$x \equiv (-15) \cdot 19 \equiv -285 \equiv 16 \pmod{43}$$

so 16 is the unique solution modulo 43. All solutions are given by

$$16, \qquad 59, \qquad 102, \qquad 145, \qquad 188, \qquad 231, \qquad 274.$$

Exercise 3. Calculate $3^{20} \bmod 99$.
(3 Marks)

Solution. We have $20 = 2^4 + 2^2$, so we calculate

$$\begin{aligned}
3^2 \bmod 99 &= 9 \bmod 99, \\
3^4 \bmod 99 &= 81 \bmod 99, \\
3^8 \bmod 99 &= 6561 \bmod 99 = 27 \bmod 99, \\
3^{16} \bmod 99 &= 729 \bmod 99 = 36 \bmod 99.
\end{aligned}$$

Then

$$3^{20} \bmod 99 = (3^{16} \bmod 99)(3^4 \bmod 99) \bmod 99 = 36 \cdot 81 \bmod 99 = 2916 \bmod 99 = 45 \bmod 99.$$

Exercise 4. Find all solutions of $140x \equiv 133 \pmod{301}$.
(2 Marks)

Exercise 5. Let A, B, C be statements. Are the following tautologies:

$$\begin{aligned}
\big((A \Rightarrow B) \Rightarrow C\big) &\Leftrightarrow \big(A \Rightarrow (B \Rightarrow C)\big), \\
\big((A \Rightarrow B) \wedge (C \Rightarrow \neg B)\big) &\Rightarrow (A \Rightarrow \neg C)?
\end{aligned}$$

Give proofs or counterexamples!
(2 + 2 Marks)

Exercise 6. Let A, B, C, D, E be statements. Prove that the argument

$$\begin{array}{rl}
& A \Rightarrow C \\
& D \vee E \\
& \neg E \Rightarrow \neg B \\
& (\neg B \wedge D) \Rightarrow A \\
& \neg E \\
\hline
\therefore & C
\end{array}$$

is valid by succesively applying known rules of inference.
(3 Marks)

Solution. We reduce the argument to syllogisms **(1/2 Mark)**:

$$\begin{array}{rl} & \neg E \Rightarrow \neg B \\ & \neg E \\ \hline \therefore & \neg B. \end{array}$$

(1/2 Mark) Furthermore,

$$\begin{array}{rl} & D \vee E \\ & \neg E \\ \hline \therefore & D. \end{array}$$

(1/2 Mark) Finally,

$$\begin{array}{rl} & \neg B \\ & D \\ \hline \therefore & \neg B \wedge D \end{array}$$

(1/2 Mark) Finally,

$$\begin{array}{rl} & (\neg B \wedge D) \Rightarrow A \\ & \neg B \wedge D \\ \hline \therefore & A \end{array}$$

(1/2 Mark) Finally,

$$\begin{array}{rl} & A \Rightarrow C \\ & A \\ \hline \therefore & C \end{array}$$

(1/2 Mark) and the argument is complete.

Exercise 7. Prove the following statement using induction in n:

$$\sum_{j=1}^{n} x^{n-j} y^{j-1} = \frac{x^n - y^n}{x - y}, \qquad\qquad x, y \in \mathbb{R},\ x \neq y,\ n \geq 1.$$

(4 Marks)

Solution. Award **1/2 Mark** for checking that the statement is true for $n = 1$:
$A(n = 1)$: $\quad \sum\limits_{j=1}^{1} x^{1-j} y^{j-1} = x^0 y^0 = 1 = \frac{x^1 - y^1}{x-y}$
Award **1/2 Mark** for saying that "Assuming the statement is true for n, we now show that it is true for $n + 1$" or some equivalent remark. Award **2 Marks** for then succesfully proving this as follows:
$A(n) \Rightarrow A(n + 1)$:

$$\begin{aligned} \sum_{j=1}^{n+1} x^{n+1-j} y^{j-1} &= x \sum_{j=1}^{n+1} x^{n-j} y^{j-1} = x\Big(x^{-1} y^n + \sum_{j=1}^{n} x^{n-j} y^{j-1}\Big) \\ &= y^n + x \frac{x^n - y^n}{x - y} = \frac{y^n (x - y) + x^{n+1} - x y^n}{x - y} = \frac{x^{n+1} - y^{n+1}}{x - y} \end{aligned}$$

Exercise 8. We define the set $S \subset \mathbb{Z}^2$ by the following properties

- $(3, 5) \in S$
- $(x, y) \in S \Rightarrow (x + 2, y) \in S$
- $(x, y) \in S \Rightarrow (-x, y) \in S$
- $(x, y) \in S \Rightarrow (y, x) \in S$

Show that $S = T$, where

$$T = \{(x, y) \in \mathbb{Z}^2 \colon \underset{m,n\in\mathbb{Z}}{\exists} : (x, y) = (2m + 1, 2n + 1)\}.$$

Hint: show that $S \subset T$ and $T \subset S$.
(6 Marks)

Solution. i) We first show that $S \subset T$ by structural induction. In particular, we show that if $(x, y) \in S$, then there exist m, n such that $(x, y) = (2m + 1, 2n + 1)$. **(1 Mark)**

For $(x, y) = (3, 5)$ we choose $m = 1$, $n = 2$. **(1/2 Mark)** Next, assume that $(x, y) = (2m + 1, 2n + 1)$ for $m, n \in \mathbb{Z}$. Then

a) $(x + 2, y) = (2(m + 1) + 1, 2n + 1)$,
b) $(-x, y) = (2(-m - 1) + 1, 2n + 1)$,
c) $(y, x) = (2n + 1, 2m + 1)$.

Thus we can find $m', n' \in \mathbb{Z}$ such that $(x + 2, y), (-x, y)$ and (y, x) can be written as $(2m' + 1, 2n' + 1)$. This shows that $S \subset T$. **(3/2 Marks)**

ii) We first show that for any $m \in \mathbb{N}$, $(x, y) = (2m + 1, 5) \in T$ is also in S. First, we show that $(1, 5) \in S$. For this, we start with $(3, 5)$, apply step b) above, followed twice by step a):

$$(3, 5) \in S \underset{\text{a)}}{\Rightarrow} (-3, 5) \in S \underset{\text{b)}}{\Rightarrow} (-1, 5) \in S \underset{\text{b)}}{\Rightarrow} (1, 5) \in S.$$

Next, assume that $(2m+1, 5) \in S$. Then, by Step a), $(2(m+1)+1, 5) = (2m+1+2, 5) \in S$. This shows that $(2m + 1, 5) \in S$ for $m \in \mathbb{N}$. By Step b), we obtain $(2m + 1, 5) \in S$ for $m \in \mathbb{Z}$. **(1 Mark)**

We now claim that for any $n \in \mathbb{N}$ and for any $m \in \mathbb{Z}$, $(2n + 1, 2m + 1) \in S$. We prove this by induction in n. For $n = 0$, we need to show that $(1, 2m + 1) \in S$ for any $m \in \mathbb{Z}$. By our previous result and Step c), we know that $(5, 2m + 1) \in S$ for any m. Applying Step b) followed by Step a) three times, we see that $(1, 2m + 1) \in S$ for any $m \in \mathbb{Z}$. **(1/2 Mark)**

Next, if $(2n + 1, 2m + 1) \in S$ for any $m \in \mathbb{Z}$, we see that $(2(n + 1) + 1, 2m + 1) = (2n + 1 + 2, 2m + 1) \in S$ for any $m \in \mathbb{Z}$ by applying Step a). This establishes that for any $n \in \mathbb{N}$ and for any $m \in \mathbb{Z}$, $(2n + 1, 2m + 1) \in S$. **(1 Mark)**

By Step b), we finally have $(2m + 1, 2n + 1) \in S$ for $m, n \in \mathbb{Z}$. This proves $T \subset S$. **(1/2 Mark)**

Exercise 9.

i) Solve the system of congruences

$$x \equiv 2 \mod 3, \qquad x \equiv 5 \mod 7, \qquad x \equiv 6 \mod 8.$$

ii) Solve the congruence $x^2 \equiv 29 \mod 35$.

(4+4 Marks)

Solution.

i) We set $m = 3 \cdot 7 \cdot 8 = 168$, $M_1 = 56$, $M_2 = 24$, $M_3 = 21$. An inverse of 56 mod 3 is given by $y_1 = 2$, of 24 mod 7 by $y_2 = 5$ and of 21 mod 8 by $y_3 = 5$. Thus the solution is

$$2 \cdot 56 \cdot 2 + 5 \cdot 24 \cdot 5 + 6 \cdot 21 \cdot 5 = 224 + 600 + 630 = 1454 \bmod 168 = 110 \bmod 168$$

(4 Marks)

ii) Note that

$$x^2 \equiv 29 \bmod 35 \qquad \Leftrightarrow \qquad x^2 \equiv 29 \bmod 5 \quad \wedge \quad x^2 \equiv 29 \bmod 7$$

We first solve $x^2 \equiv 29 \mod 7 = 1 \bmod 7$ giving $x = \pm 1 \bmod 7$, so $x_1 = 1$ and $x_2 = 6$. Then, we solve $x^2 \equiv 29 \mod 5 = 4 \bmod 5$, giving $x = \pm 2 \bmod 5$, so $x_1 = 2$, $x_2 = 3$. We then have x determined through the following congruences:

$$x \equiv 1 \bmod 7, \qquad x \equiv 2 \bmod 5$$

giving $x = 22 \bmod 35$;

$$x \equiv 6 \bmod 7, \qquad x \equiv 2 \bmod 5$$

yielding $x \equiv 62 \bmod 35 = 27 \bmod 35$;

$$x \equiv 1 \bmod 7, \qquad x \equiv 3 \bmod 5$$

giving $x \equiv 8 \bmod 35$;

$$x \equiv 6 \bmod 7, \qquad x \equiv 3 \bmod 5$$

yielding $x \equiv 48 \bmod 35 = 13 \bmod 35$. We hence have the four roots

$$x_1 \equiv 8 \mod 35, \quad x_2 \equiv 13 \mod 35, \quad x_3 \equiv 22 \mod 35, \quad x_4 \equiv 27 \mod 35.$$

(1 Mark for each root)

Exercise 10. Let M_q be an integer of the form $a^q - 1$, where a and q are natural numbers. M_q is called a *Mersenne number*. When M_q is prime and $a = 2$, M_q is called a *Mersenne prime*.

i) Prove that $(a-1) \mid (a^q - 1)$.

ii) Conclude that if M_q is prime then $a = 2$ or $q = 1$.

iii) Prove that if M_q is a Mersenne prime, then q is prime.

(2+2+3 Marks)

Solution.

i) Let a and q be two natural integers. Then

$$a^q - 1 = (a-1)(a^{q-1} + a^{q-2} + \ldots + a^2 + a + 1)$$

Since both $a-1$ and $\sum_{i=0}^{q-1} a^i$ are integers, $a-1$ divides $a^q - 1$.

ii) Suppose that $M_q = a^q - 1$ is prime.

From the previous question we know that $a-1$ divides M_q, therefore if M_q is prime, then either $a - 1 = a^q - 1$ or $a - 1 = 1$.

In the first case $a - 1 = a^q - 1$, that is $a = a^q$. This is only possible if $a \in \{0, 1\}$ or $q = 1$. However if $a \in \{0, 1\}$, then $M_q \in \{-1, 0\}$ and M_q is not prime. Thus $q = 1$.

In the second case $a - 1 = 1$ yields $a = 2$.

iii) Let $M_q = 2^q - 1$ be a Mersenne prime and $a, b > 1$ be two integers such that $q = ab$ is composite. Then from the first question we have

$$\begin{aligned} 2^q - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1 \\ &= (2^a - 1)\left((2^a)^{b-1} + (2^a)^{b-2} + \ldots + 2^{2a} + 2^a + 1\right) \end{aligned}$$

This non-trivial factorisation of M_q contradicts its primality. Therefore q must be prime.