Quiz 2 – Solutions
Concepts in Abstract Mathematics
MAT246 LEC0101 Winter 2020

Each tutorial had a different version of the quiz.

- TUT0101 (Monday 13:00–14:00, TA: Hubert Dubé)
- TUT0201 (Monday 16:00–17:00, TA: Debanjana Kundu)
- TUT0301 (Tuesday 15:00–16:00, TA: Robin Gaudreau)
- TUT0401 (Wednesday 13:00–14:00, TA: Robin Gaudreau)

TUT0101

Question 1 (5 points)

State Fermat's Little Theorem.

Solution. If p is a prime number and a is any natural number that is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Question 2 (10 points)

Let p be prime and let $a, b \in \mathbb{N}$. Show, without using the Fundamental Theorem of Arithmetic, that if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Solution. If $p \mid a$, then we are done. Hence, suppose that p does not divide a. We want to show that $p \mid b$. Since p is prime and does not divide a, they are relatively prime. Then, by the Euclidean Algorithm, there exist $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Multiplying both sides by b yields $abx + pby = b$. Since $p \mid ab$, we have $p \mid abx$. So, p divides both abx and pby, and hence it divides their sum, which is b.

Question 3 (10 points)

Let $a = 46$ and $b = 39$. Use the Euclidean Algorithm to find the greatest common divisor of a and b, and express the result as a linear combination of a and b.

Solution. We have

$$\begin{aligned} 46 &= 39 \cdot 1 + 7 \\ 39 &= 7 \cdot 5 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0, \end{aligned}$$

so $\gcd(46, 39) = 1$. Working backwards, we find

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 \\ &= 4 - (7 - 4 \cdot 1) \cdot 1 \\ &= 4 \cdot 2 - 7 \cdot 1 \\ &= (39 - 7 \cdot 5) \cdot 2 - 7 \cdot 1 \\ &= 39 \cdot 2 - 7 \cdot 11 \\ &= 39 \cdot 2 - (46 - 39 \cdot 1) \cdot 11 \\ &= 39 \cdot 13 - 46 \cdot 11. \end{aligned}$$

TUT0201

Question 1 (5 points)

State Fermat's Little Theorem.

Solution. If p is a prime number and a is any natural number that is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Question 2 (10 points)

Let $a, b, c \in \mathbb{N}$ and let $d = \gcd(a, b)$. Show that the linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$.

Solution. Suppose that there is a solution, i.e. $ax+by = c$ for some $x, y \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$ we have $d \mid ax$ and $d \mid by$, so $d \mid ax + by$ and hence $d \mid c$.

Conversely, suppose that $d \mid c$ and write $c = dk$ for some $k \in \mathbb{Z}$. By the Euclidean Algorithm, there exist $s, t \in \mathbb{Z}$ such that $as + bt = d$. Then, multiplying both sides by k, we get $ask + btk = dk = c$, so by letting $x = sk$ and $y = tk$ we have $ax + by = c$ and hence (x, y) is a solution.

Question 3 (10 points)

Let $a = 48$ and $b = 43$. Use the Euclidean Algorithm to find the greatest common divisor of a and b, and express the result as a linear combination of a and b.

Solution. We have

$$\begin{aligned} 48 &= 43 \cdot 1 + 5 \\ 43 &= 5 \cdot 8 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

so $\gcd(48, 43) = 1$. Working backwards, we find

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (5 - 3 \cdot 1) \cdot 1 \\ &= 3 \cdot 2 - 5 \cdot 1 \\ &= (43 - 5 \cdot 8) \cdot 2 - 5 \cdot 1 \\ &= 43 \cdot 2 - 5 \cdot 17 \\ &= 43 \cdot 2 - (48 - 43 \cdot 1) \cdot 17 \\ &= 43 \cdot 19 - 48 \cdot 17. \end{aligned}$$

TUT0301

Question 1 (5 points)

State Wilson's Theorem.

Solution. If p is a prime number, then $(p-1)! + 1 \equiv 0 \pmod{p}$.

Question 2 (10 points)

Let p be prime and let $a, b \in \mathbb{N}$. Show, without using the Fundamental Theorem of Arithmetic, that if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Solution. If $p \mid a$, then we are done. Hence, suppose that p does not divide a. We want to show that $p \mid b$. Since p is prime and does not divide a, they are relatively prime. Then, by the Euclidean Algorithm, there exist $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Multiplying both sides by b yields $abx + pby = b$. Since $p \mid ab$, we have $p \mid abx$. So, p divides both abx and pby, and hence it divides their sum, which is b.

Question 3 (10 points)

Let $a = 49$ and $b = 26$. Use the Euclidean Algorithm to find the greatest common divisor of a and b, and express the result as a linear combination of a and b.

Solution. We have

$$\begin{aligned} 49 &= 26 \cdot 1 + 23 \\ 26 &= 23 \cdot 1 + 3 \\ 23 &= 3 \cdot 7 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

so $\gcd(49, 26) = 1$. Working backwards, we find

$$\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
&= 3 - (23 - 3 \cdot 7) \cdot 1 \\
&= 3 \cdot 8 - 23 \cdot 1 \\
&= (26 - 23 \cdot 1) \cdot 8 - 23 \cdot 1 \\
&= 26 \cdot 8 - 23 \cdot 9 \\
&= 26 \cdot 8 - (49 - 26 \cdot 1) \cdot 9 \\
&= 26 \cdot 17 - 49 \cdot 9.
\end{aligned}$$

TUT0401

Question 1 (5 points)

State Wilson's Theorem.

Solution. If p is a prime number, then $(p-1)! + 1 \equiv 0 \pmod{p}$.

Question 2 (10 points)

Let $a, b, c \in \mathbb{N}$ and let $d = \gcd(a, b)$. Show that the linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$.

Solution. Suppose that there is a solution, i.e. $ax+by = c$ for some $x, y \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$ we have $d \mid ax$ and $d \mid by$, so $d \mid ax + by$ and hence $d \mid c$.

Conversely, suppose that $d \mid c$ and write $c = dk$ for some $k \in \mathbb{Z}$. By the Euclidean Algorithm, there exist $s, t \in \mathbb{Z}$ such that $as + bt = d$. Then, multiplying both sides by k, we get $ask + btk = dk = c$, so by letting $x = sk$ and $y = tk$ we have $ax + by = c$ and hence (x, y) is a solution.

Question 3 (10 points)

Let $a = 43$ and $b = 35$. Use the Euclidean Algorithm to find the greatest common divisor of a and b, and express the result as a linear combination of a and b.

Solution. We have

$$\begin{aligned}
43 &= 35 \cdot 1 + 8 \\
35 &= 8 \cdot 4 + 3 \\
8 &= 3 \cdot 2 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

so $\gcd(43, 35) = 1$. Working backwards, we find

$$\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
&= 3 - (8 - 3 \cdot 2) \cdot 1 \\
&= 3 \cdot 3 - 8 \cdot 1 \\
&= (35 - 8 \cdot 4) \cdot 3 - 8 \cdot 1 \\
&= 35 \cdot 3 - 8 \cdot 13 \\
&= 35 \cdot 3 - (43 - 35 \cdot 1) \cdot 13 \\
&= 35 \cdot 16 - 43 \cdot 13.
\end{aligned}$$