Due Friday 3 March, *before* 1:00pm

Note: solutions may be incomplete, and meant to be used as guidelines only. We encourage you to ask follow-up questions on the course forum or during office hours.

1. [6 marks] Number theory.

(a) [2 marks] Prove that $\forall n \in \mathbb{Z}, \gcd(9n+1, 10n+1) = 1$.

HINT: Use some of the facts from the Week 4 worksheets for a very short proof.

Solution

In the proof, we make use of the following fact from Worksheet 6 (Week 4, Hr2):

> For every pair of integers a and b, if at least one of them is non-zero, then $\gcd(a, b)$ is the *smallest positive integer* that can be written in the form $pa + qb$, where p and q are integers.

Proof. Let $n \in \mathbb{Z}$.
Then $9n + 1 \neq 0$ (by contradiction, if $9n + 1 = 0$, then $n = -\frac{1}{9} \notin \mathbb{Z}$).
Now consider:

$$10(9n + 1) - 9(10n + 1) = 90n + 10 - 90n - 9 = 1,$$

and note that 1 is the smallest positive integer.
Hence, the fact from Worksheet 6 applies, with $a = 9n + 1$, $b = 10n + 1$, $p = 10$ and $q = -9$, and allows us to conclude that $\gcd(9n + 1, 10n + 1) = 1$.
(Note: Since the Course Notes define the gcd function as taking natural number arguments, we allow the statement to be proven for $n \in \mathbb{N}$ instead of $n \in \mathbb{Z}$.) □

(b) [4 marks]
Prove the following statement:

$$\forall m, n \in \mathbb{Z}, n \mid m \land Prime(n) \Rightarrow n \nmid (m + 1)$$

Solution

We present a *proof by contradiction*. This can be argued in a few ways, but we present just one here.

Proof. We want to consider the proposition:

$$\forall m, n \in \mathbb{Z}, n \mid m \land Prime(n) \Rightarrow n \nmid (m + 1)$$

Suppose that this statement is False.
That is, suppose the following statement is True:

$$\exists m, n \in \mathbb{Z}, n \mid m \land Prime(n) \land n \mid (m + 1)$$

Let $m, n \in \mathbb{Z}$ be such that $n \mid m \land Prime(n) \land n \mid (m + 1)$.
Since $n \mid m$, we know $m = r \cdot n$ for some $r \in \mathbb{Z}$.
Since $n \mid (m + 1)$, we know $m + 1 = s \cdot n$ for some $s \in \mathbb{Z}$.
It follows then that $(m + 1) - m = s \cdot n - r \cdot n$, or $1 = (s - r) \cdot n$.

Since $(s-r) \in \mathbb{Z}$, it follows that $n \mid 1$.

The only integer divisors of 1 are 1 and -1, and so n must be 1 or -1.

Since $Prime(n)$, we must have that $n > 1$. This contradicts our deduction that n must be 1 or -1.

Hence, our supposition must be False, that is, the original proposition is True. $\square$

2. **[6 marks] Floors and ceilings.** For all proofs in this question, you may use the following fact from a worksheet:

$$\forall x \in \mathbb{R}, 0 \leq x - \lfloor x \rfloor < 1, \tag{1}$$

and its generalization to the ceiling function:

$$\forall x \in \mathbb{R}, 0 \leq \lceil x \rceil - x < 1. \tag{2}$$

(a) **[2 marks]** Prove that

$$\forall x \in \mathbb{Z}, \left\lceil \frac{x-1}{2} \right\rceil = \left\lfloor \frac{x}{2} \right\rfloor$$

Solution

Students came up with many different correct proofs. Here is one correct proof.

Proof. Let $x \in \mathbb{Z}$. Then, either x is even or x is odd.

Case 1: Assume x is even, i.e., $\exists k \in \mathbb{Z}, x = 2k$. Then,

$$\begin{aligned} \left\lceil \frac{x-1}{2} \right\rceil &= \left\lceil \frac{2k-1}{2} \right\rceil \\ &= \left\lceil k - \frac{1}{2} \right\rceil \end{aligned}$$

Consider the number $k - \frac{1}{2}$, where $k \in \mathbb{Z}$.

Since $-\frac{1}{2} < 0$, we know that $k - \frac{1}{2} < k$. Hence, by the definition of the ceiling function, and since $k \in \mathbb{Z}$, $\left\lceil k - \frac{1}{2} \right\rceil \leq k$.

Also, since $-1 < -\frac{1}{2}$, we know that $k - 1 < k - \frac{1}{2}$. Hence, by the definition of the ceiling function, $k - 1 < \left\lceil k - \frac{1}{2} \right\rceil$. We can conclude that $k \leq \left\lceil k - \frac{1}{2} \right\rceil$, since $k - 1$ and k are consecutive integers.

Since $\left\lceil k - \frac{1}{2} \right\rceil \leq k$ and $k \leq \left\lceil k - \frac{1}{2} \right\rceil$, it follows that $\left\lceil k - \frac{1}{2} \right\rceil = k$.

So, we have

$$\begin{aligned} \left\lceil \frac{x-1}{2} \right\rceil &= \left\lceil k - \frac{1}{2} \right\rceil \\ &= k \\ &= \lfloor k \rfloor \\ &= \left\lfloor \frac{2k}{2} \right\rfloor \\ &= \left\lfloor \frac{x}{2} \right\rfloor \end{aligned}$$

Case 2: Assume x is odd, i.e., $\exists k \in \mathbb{Z}, x = 2k+1$. Then,

$$\begin{aligned}\left\lceil \frac{x-1}{2} \right\rceil &= \left\lceil \frac{(2k+1)-1}{2} \right\rceil \\ &= \left\lceil \frac{2k}{2} \right\rceil \\ &= \lceil k \rceil \\ &= k\end{aligned}$$

We also have

$$\begin{aligned}\left\lfloor \frac{x}{2} \right\rfloor &= \left\lfloor \frac{2k+1}{2} \right\rfloor \\ &= \left\lfloor k + \frac{1}{2} \right\rfloor\end{aligned}$$

Consider the number $k + \frac{1}{2}$, where $k \in \mathbb{Z}$.
Since $0 < \frac{1}{2}$, we know that $k < k + \frac{1}{2}$. Hence, by the definition of the floor function, and since $k \in \mathbb{Z}$, $k \leq \left\lfloor k + \frac{1}{2} \right\rfloor$.
Also, since $\frac{1}{2} < 1$, we know that $k+\frac{1}{2} < k+1$. Hence, by the definition of the floor function, $\left\lfloor k + \frac{1}{2} \right\rfloor < k+1$. That is, $\left\lfloor k + \frac{1}{2} \right\rfloor \leq k$, since k and $k+1$ are consecutive integers.
Since $k \leq \left\lfloor k + \frac{1}{2} \right\rfloor$ and $\left\lfloor k + \frac{1}{2} \right\rfloor \leq k$, it follows that $\left\lfloor k + \frac{1}{2} \right\rfloor = k$.
We have that $\left\lceil \frac{x-1}{2} \right\rceil = k$ and $\left\lfloor \frac{x}{2} \right\rfloor = k$, and so $\left\lceil \frac{x-1}{2} \right\rceil = \left\lfloor \frac{x}{2} \right\rfloor$, as required.

$\square$

(b) **[4 marks]** Prove or disprove each of the following. In each case, first write down in symbolic notation the exact statement you are attempting to prove (either the original statement or its negation).

i. $\forall x \in \mathbb{R}, \lceil x - 1 \rceil = \lceil x \rceil - 1$

Solution

Recall that by definition, $\lceil x \rceil$ is the *smallest* integer that satisfies $\lceil x \rceil \geq x$, i.e.,

$$\forall k \in \mathbb{Z}, k \geq x \Rightarrow k \geq \lceil x \rceil. \tag{3}$$

We prove the statement.

Proof. Let $x \in \mathbb{R}$. And let $n \in \mathbb{Z}$ be such that $n = \lceil x \rceil$.
Since $n-1$ and n are consecutive integers, and since $n = \lceil x \rceil$, we have that $n - 1 < x \leq n$.
Subtracting 1 from each side, we have $n - 2 < x - 1 \leq n - 1$.
Since $n - 2 < x - 1$, $n - 2 < \lceil x - 1 \rceil$. It follows that $n - 1 \leq \lceil x - 1 \rceil$, since $n - 2$ and $n - 1$ are consecutive integers.
Since $x - 1 \leq n - 1$, we have from the definition of the ceiling function that $\lceil x - 1 \rceil \leq n - 1$.
Since $n - 1 \leq \lceil x - 1 \rceil$ and $\lceil x - 1 \rceil \leq n - 1$, it follows that $\lceil x - 1 \rceil = n - 1$. Substitutiting

$n = \lceil x \rceil$ gives $\lceil x - 1 \rceil = \lceil x \rceil - 1$, as required. □

ii. $\forall x, y \in \mathbb{R}, \lceil xy \rceil = \lceil x \rceil \lfloor y \rfloor$

Solution

Proof. We disprove this statement, whose negation is:

$$\exists x, y \in \mathbb{R}, \lceil xy \rceil \neq \lceil x \rceil \lfloor y \rfloor$$

Let $x = 1.1$ and $y = 2$. Then $x, y \in \mathbb{R}$ and $\lceil xy \rceil = \lceil 2.2 \rceil = 3$. Also $\lceil x \rceil \lfloor y \rfloor = 2 \cdot 2 = 4$. Since $3 \neq 4$, $\lceil xy \rceil \neq \lceil x \rceil \lfloor y \rfloor$, as required. □

3. [8 marks] Induction.

(a) [**3 marks**] Prove that for all natural numbers n, $9 \mid 11^n - 2^n$.

Solution

Let us define the predicate: $P(n)$: "$9 \mid 11^n - 2^n$", where $n \in \mathbb{N}$.
We will prove the statement $\forall n \in \mathbb{N},\ P(n)$ using induction.

Proof. **Base case**: Prove $P(n)$ for $n = 0$.
Let $n = 0$.
Then

$$\begin{aligned} 11^n - 2^n &= 11^0 - 2^0 \\ &= 1 - 1 \\ &= 0 \\ &= 0 \cdot 9 \\ &= s \cdot 9, \end{aligned}$$

for $s = 0$. Hence, $9 \mid 11^n - 2^n$, and $P(0)$ is True, as required.

Induction step: Let $k \in \mathbb{N}$ and assume that $P(k)$ is True. We'll prove that $P(k+1)$ is True.

Since $P(k)$ is assumed True, we know that $11^k - 2^k = t \cdot 9$ for some $t \in \mathbb{Z}$.
Then

$$\begin{aligned} 11^{k+1} - 2^{k+1} &= (11^k \cdot 11) - (2^k \cdot 2) \\ &= (11^k \cdot (9+2)) - (2^k \cdot 2) \\ &= (11^k \cdot 9) + (11^k \cdot 2) - (2^k \cdot 2) \\ &= (11^k \cdot 9) + ((11^k - 2^k) \cdot 2) \\ &= (11^k \cdot 9) + (t \cdot 9 \cdot 2) \qquad \text{(By the Induction Hypothesis)} \\ &= (11^k + 2t) \cdot 9 \\ &= s \cdot 9, \end{aligned}$$

for $s \in \mathbb{Z}$ with $s = 11^k + 2t$. Hence, $9 \mid 11^{k+1} - 2^{k+1}$, and $P(k+1)$, as required. □

(b) [**5 marks**] Recall the definition of **Pierre Numbers** from Problem Set 1:

> A natural number p is said to be a "Pierre Number" when it can be expressed as $2^{2^k} + 1$ for some integer k.

Consider the sequence of Pierre numbers $p_n = 2^{2^n} + 1$, for $n \in \mathbb{N}$. Prove that for all $n \in \mathbb{N}$,

$$p_n = \prod_{i=0}^{n-1} p_i + 2$$

(**Hint**: You may find it easier to expand the product.)

Solution

Let us define the predicate: $P(n)$: "$p_n = \left(\prod_{i=0}^{n-1} p_i\right) + 2$", where $n \in \mathbb{N}$ and $p_n = 2^{2^n} + 1$.

We will prove the statement $\forall n \in \mathbb{N},\ P(n)$ using induction.

Proof. **Base case**: Prove $P(n)$ for $n = 0$.
Let $n = 0$.
Then

$$\begin{aligned} p_n &= p_0 \\ &= 2^{2^0} + 1 \\ &= 2^1 + 1 \\ &= 2 + 1 \\ &= 3 \end{aligned}$$

and

$$\begin{aligned} \left(\prod_{i=0}^{n-1} p_i\right) + 2 &= \left(\prod_{i=0}^{0-1} p_i\right) + 2 \\ &= \left(\prod_{i=0}^{-1} p_i\right) + 2 \\ &= 1 + 2 \qquad \text{(since an empty product has value 1)} \\ &= 3 \end{aligned}$$

We can conclude $P(0)$ is True, since $p_n = \left(\prod_{i=0}^{n-1} p_i\right) + 2$ when $n = 0$.

Induction step: Let $k \in \mathbb{N}$ and assume that $P(k)$ is True. We'll prove that $P(k+1)$ is True.

Since $P(k)$ is assumed True, we know that $p_k = \left(\prod_{i=0}^{k-1} p_i\right) + 2$.

Then

$$\begin{aligned}
p_{k+1} &= 2^{2^{k+1}} + 1 \\
&= 2^{2^{k}\cdot 2} + 1 \\
&= (2^{2^k})^2 + 1 \\
&= ((2^{2^k})^2 - 1) + 2 \\
&= (2^{2^k} + 1)(2^{2^k} - 1) + 2 \\
&= (2^{2^k} + 1)((2^{2^k} + 1) - 2) + 2 \\
&= p_k(p_k - 2) + 2 \\
&= p_k\Big(\big(\big(\prod_{i=0}^{k-1} p_i\big) + 2\big) - 2\Big) + 2 \qquad \text{(By the Induction Hypothesis)} \\
&= p_k\big(\prod_{i=0}^{k-1} p_i\big) + 2 \\
&= \big(\prod_{i=0}^{k} p_i\big) + 2 \\
&= \big(\prod_{i=0}^{(k+1)-1} p_i\big) + 2.
\end{aligned}$$

We have that $p_{k+1} = \big(\prod_{i=0}^{(k+1)-1} p_i\big) + 2$, and so $P(k+1)$ is True, as required. $\square$