Group Work 2

Benjamin Belisle Ben Lannom Bennett Meacham Emma Owens

February 8, 2023

1.3.34

Suppose $n \in \mathbb{Z}$ and $n > 2$.

Suppose also that N is the set $\mathbb{Z} \cap [2, n]$.

$n!$ is the product of all integers within N, so $\forall z \in N\ z \mid n!$.

To prove that $a \nmid 1 \land a \mid b \Rightarrow a \nmid b - 1$

Suppose that $a \mid b$ and $a \mid b - 1$.

This means that there are integers c and d such that $ac = b$ and $ad = b - 1$.

$$\begin{aligned} ac &= b \\ ad &= b - 1 \\ a(c - d) &= 1 \end{aligned}$$

This means that $a \mid 1$.

Thus,

$$\begin{aligned} a \mid b \land a \mid b - 1 &\Rightarrow a \mid 1 \\ \neg(a \mid b \land a \mid b - 1) &\lor a \mid 1 \\ a \nmid b \lor a \nmid b - 1 &\lor a \mid 1 \\ a \mid 1 \lor a \nmid b &\lor a \nmid b - 1 \\ a \nmid 1 \land a \mid b &\Rightarrow a \nmid b - 1 \end{aligned}$$

For every $z \in N$, $z > 1$, so $z \nmid 1$.

$z \nmid 1$ and $z \mid n!$, so $z \nmid n! - 1$.

Thus, $n! - 1$ has no factors e such that $1 < e \leq n$.

$$\begin{aligned} 1 < e <\leq n &\Rightarrow e \nmid n! - 1 \\ e \mid n! - 1 &\Rightarrow (e \leq 1 \lor e > n) \end{aligned}$$

Since $n > 2$, and factorial is increasing, $n! > 2$, and $n! - 1 > 1$.

Since $n! - 1 > 1$, $n! - 1$ has a prime factor p.

Since $p \mid n! - 1$, $p \leq 1 \lor p > n$.

Since p is prime, it cannot be that $p \leq 1$, so $p > n$.

Since $p \mid n! - 1$ and $n! - 1 > 0$, $p \leq n! - 1$.

Thus, $n < p \leq n! - 1$.

There exists a prime p such that $n < p < n!$.

QED

1.3.36

To prove that, for any primes $p \geq 5, q \geq 5$, $3 \mid p^2 - q^2$.

To prove that, for any prime p, p^2 can be written as $3m + 1$ for some integer m.

Suppose prime number $p \geq 5$.

According to the Division Algorithm, p can be written as either $3n$, $3n + 1$, or $3n + 2$ for some integer n.

If $p = 3n$, this forms a contradiction since $3 \mid p$ and (since $p \geq 5$) $p \neq 3$.

If $p = 3n + 1$, then $p^2 = 3(3n^2) + 3(2n) + 1 = 3(3n^2 + 2n) + 1$. Thus, $p^2 = 3m + 1$ for some integer m.

If $p = 3n + 2$, then $p^2 = 3(3n^2) + 3(2n) + 4 = 3(3n^2 + 2n + 1) + 1$. Thus, $p^2 = 3m + 1$ for some integer m.

Suppose primes $p \geq 5, q \geq 5$.

There exist integers a and b for which $p^2 = 3a + 1$ and $q^2 = 3b + 1$.

$$\begin{aligned}
p^2 &= 3a + 1 \\
q^2 &= 3b + 1 \\
p^2 - q^2 &= 3a - 3b \\
p^2 - q^2 &= 3(a - b)
\end{aligned}$$

Since $a - b$ is an integer, $3 \mid p^2 - q^2$.

To prove that, for any primes $p \geq 5, q \geq 5$, $8 \mid p^2 - q^2$.

According to the Division Algorithm, p can be written either as $4n$, $4n + 1$, $4n + 2$, or $4n + 3$. Since p is prime and greater than 2, $p = 4n$ and $p = 4n + 2 = 2(2n + 1)$ both lead to contradictions. Thus $p = 4n + 1$ or $p = 4n + 3$.

Similarly, for some integer m, $q = 4m + 1$ or $q = 4m + 3$.

If $p = 4n + 1$ and $q = 4m + 1$, then

$$\begin{aligned}
p^2 &= 16n^2 + 8n + 1 \\
q^2 &= 16m^2 + 8m + 1 \\
p^2 - q^2 &= 16(n^2 - m^2) + 8(n - m) \\
&= 8(2(n^2 - m^2)) + 8(n - m) \\
&= 8(2(n^2 - m^2) + n - m) \\
8 &\mid p^2 - q^2
\end{aligned}$$

If $p = 4n + 3$ and $q = 4m + 3$, then

$$\begin{aligned}
p^2 &= 16n^2 + 24n + 9 \\
q^2 &= 16m^2 + 24m + 9 \\
p^2 - q^2 &= 16(n^2 - m^2) + 24(n - m) \\
&= 8(2(n^2 - m^2)) + 8(3(n - m)) \\
&= 8(2(n^2 - m^2) + 3(n - m)) \\
8 &\mid p^2 - q^2
\end{aligned}$$

Without loss of generality, swap p and q if $p = 4n + 1$ and $q = 4n + 3$.

$$\begin{aligned}
p &= 4n + 3 \\
q &= 4n + 1 \\
p^2 &= 16n^2 + 24n + 9 \\
&= 8(2n^2 + 3n + 1) + 1 \\
q^2 &= 16m^2 + 8m + 1 \\
&= 8(2m^2 + m) + 1 \\
p^2 - q^2 &= 8(2n^2 + 3n + 1 - 2m^2 - m) \\
8 &\mid p^2 - q^2
\end{aligned}$$

In all 3 cases, $8 \mid p^2 - q^2$.

Suppose primes $p \geq 5, q \geq 5$.

By earlier conclusions, $3 \mid p^2 - q^2$ and $8 \mid p^2 - q^2$.

Since $24 = [3, 8]$, by problem 1.2.32, $24 \mid p^2 - q^2$.

QED

2.1.19

Suppose $[a] = [b]$ in $\mathbb{Z}_n$.

Due to the division algorithm, a can be written as $nq_a + r_a$, and b can be written as $nq_b + r_b$, such that $0 \leq r_a < n$ and $0 \leq r_b < n$.

$$\begin{gathered}
b \in [b] \wedge [a] = [b] \\
b \in [a] \\
a \equiv b \\
n \mid a - b \\
n \mid nq_a + r_a - nq_b - r_b \\
nz = nq_a + r_a - nq_b - r_b \\
n(z - q_a + q_b) = r_a - r_b \\
n \mid r_a - r_b
\end{gathered}$$

Since $r_a < n$ and $0 \leq r_b$, $r_a - r_b$ can be at most n-1. Since $0 \leq r_a$ and $r_b < n$, $r_a - r_b$ must be at least -(n-1). Since $|r_a - r_b| < n$ and $n \mid r_a - r_b$, $r_a - r_b$ must be 0, and $r_a = r_b$.

Let an integer r be equal to r_a.

$$\begin{gathered}
a = nq_a + r \\
b = nq_b + r
\end{gathered}$$

With application of Euclid's algorithm,

$$\begin{gathered}
(a, n) = (r, n) \\
(b, n) = (r, n) \\
(a, n) = (r, n) = (b, n) \\
(a, n) = (b, n)
\end{gathered}$$

QED