Assignment Two

Logan Hunt

January 25, 2023

Contents

1 Section 1.3

1.1 Question 3

701, 1009, 1949, 1951 are all prime

1.2 Question 7

$$\begin{aligned} p|a \Rightarrow np &= a \\ p|a + bc \Rightarrow mp &= a + bc \\ mp &= np + bc \\ mp - np &= bc \\ p(m-n) &= bc \end{aligned}$$

Since bc is a multiple of p, and p is prime, by Theorem 1.5, $p|b$ or $p|c$.

1.3 Question 15

If $p|a^n \Rightarrow p|a \cdot a \ldots a$ then by corollary 1.6, $p|a$. Then, $a = pm$ and $a^n = p^n \cdot m^n$. p^n is a factor of a^n and thus $p^n|a^n$.

1.4 Question 17

From the Fundamental Theorem of Arithmetic, both a and b must be a product of primes such that $a = (p \cdot p_1 \cdot p_2 \ldots p_i)$ and $b = (p \cdot q_1 \cdot q_2 \ldots q_j)$ with each p_i and q_j being prime.
Then, $a^2 = (p \cdot p_1 \cdot p_2 \ldots p_r) \cdot (p \cdot p_1 \cdot p_2 \ldots p_r)$ and $b^2 = (p \cdot q_1 \cdot q_2 \ldots q_j) \cdot (p \cdot q_1 \cdot q_2 \ldots q_j)$. p^2 is then a common factor of a^2 and b^2, and since each other factor (p_i^2, q_i^2) is a square of a prime, there can be no other greater common divisor than p^2.
Therefore, $(a, b) = p \Rightarrow (a^2, b^2) = p^2$ when p is prime.

1.5 Question 30

1.5.1 a

Firstly assume that there are $a, b \ni a^2 = 2b^2$. Then, $a^2 = p_1 p_2 \ldots p_r$ and $2b^2 = q_1 q_2 \ldots q_s$, and by the Fundamental Theorem of Arithmetic, every $p_i = \pm q_j$. Since a^2 is even as it is equal to $2b^2$, let p_1 be the factor corresponding to a power of 2. Then $p_1 = 2^n$ and n must be a multiple of 2 since $a^2 = 2^n \ldots \Rightarrow a = 2^{\frac{n}{2}} \ldots$
However, $2b^2 = \pm 2^n \ldots$ implies that $b^2 = \pm 2^{n-1} \ldots$ and from similar reasoning $n - 1$ must also be a multiple of 2.
This is a contradiction - not both n and $n - 1$ can be multiples of 2!

1.5.2 b

Just reformat it:

$$\sqrt{2} = \frac{a}{b} \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2$$

2 Section 2.1

2.1 Question 2

2.1.1 a

$$6k + 5 \equiv_4 6 + 5 \equiv_4 11 \equiv_4 3$$

2.1.2 b

$$2r + 3s \equiv_{10} 2(3) + 3(-7) \equiv_{10} 6 - 21 \equiv_{10} -15 \equiv_{10} 5$$

2.2 Question 3b

$$\begin{aligned}
&10(0) + 9(0) + 8(3) + 7(1) + 6(1) + 5(0) + 4(5) + 3(5) + 2(9) + 5 \\
&\equiv_{11} 24 + 7 + 6 + 20 + 15 + 18 + 5 \\
&\equiv_{11} 95 \\
&\equiv_{11} 7
\end{aligned}$$

Invalid ISBN

2.3 Question 5

2.3.1 a

Theorem 2.2 states that if $a \equiv_4 b$, and $c \equiv_4 d$, then $ac \equiv_4 bd$.
Since $5 \equiv_4 1$ and $5 \cdot 5 \equiv_4 1 \cdot 1$, then $5 \cdot 5 \cdot 5 \equiv_4 1 \cdot 1 \cdot 1$.
We can continue chaining these together until we find $5^{2000} \equiv_4 1^{2000}$, and thus $[5^{2000}] = [1]$ in $\mathbb{Z}_4$.

2.3.2 b

By repeating the same process as in a, $4 \equiv_5 4$ and $4^2 \equiv_5 1$. Then, $4^3 \equiv_5 4 \cdot 1$. Then, $4^4 \equiv_5 4^2 \Rightarrow 4^4 \equiv_5 1$.
In general as we keep chaining on and because of Theorem 2.2, even powers of 4 will be equivalent mod 5 to 1, and odd powers of 4 will be equivalent mod 5 to 4.
Therefore, $4^{2001} \equiv_5 1$ and $[4^{2001}] = [1]$ in $\mathbb{Z}_5$.

2.4 Question 7

If $a \in \mathbb{Z}$ then $a \equiv_4 m$ with $m \in 1, 2, 3, 4$. Then, by Theorem 2.2 again, $a^2 \equiv_4 m^2$.
$[m^2] \in \mathbb{Z}_4$ must be equivalent to any $[1^2], [2^2], [3^2], [4^2] = [1], [0], [1], [0]$.
Therefore, $[a^2]$ cannot be in $[3], [4] \subset [2], [3], [4]$

2.5 Question 14

2.5.1 a

A simple python script will prove this is false:

```
seen = set()
for n in range(1, 10):
  for a in range(0, 10):
    for b in range(0, 10):
      seenfoo = (a, b, n) in seen or (b, a, n) in seen
      if (a * b) % n == 0 and a % n != 0 and b % n != 0 and not seenfoo:
        seen.add((a, b, n))
        print(f"a={a}, b={b}, n={n}")
```

And we receive several counterexamples:

```
a=2, b=2, n=4
a=2, b=6, n=4
a=6, b=6, n=4
a=2, b=3, n=6
a=2, b=9, n=6
...
a=2, b=4, n=8
a=4, b=6, n=8
a=3, b=3, n=9
```

```
a=3, b=6, n=9
a=6, b=6, n=9
```

2.5.2 b

If $ab \equiv_n 0$, then $ab = mn + 0$ for some $m \in \mathbb{Z}$ by definition.
Then, $ab = mn$ implies that ab is a multiple of n, and since n is prime, then by Theorem 1.8, $n|ab$ implies that $n|a$ or $n|b$.