University of Wisconsin-Milwaukee

Seminar-Intro to the Language and Practice of Mathematics

Math 341

Class Notes, Homework, and Exams

Author	*Supervisor*
Theo Koss	Dr. Boris Okun

September-December 2020

Contents

1 Basic Notions and notation

1.1 Notation:

$\mathbb{N} = \{1, 2, 3, ...\}$ The set of all *natural* numbers.
$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ The set of all *integers*.
$n \in A$ means "n is an *element* of A" or "n is *in* A"

1.2 Definition:

Mathematical induction, let $A_1, A_2, A_3, ..., A_n, ...$ be a sequence of statements, each of which can be either true or false. Suppose, we know that A_1 is true. Also, suppose that for each natural number k we know that the statement "A_k is true" implies "A_{k+1} is true." Then all statements $A_1, A_2, A_3, ..., A_n, ...$ are true.

1.3 Example:

Prove by induction: for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof. Basis: $n = 1$. We check: $\sum_{i=1}^{i} i = 1 = \frac{1(1+1)}{2}$.
Inductive step. Assume the formula below holds for $n = k$:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}.$$

We must show it holds for $n = (k+1)$:

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}.$$

We start from the left-hand side, the sum splits as the sum of the first k terms and the last one:

$$\sum_{i=1}^{k+1} i = 1 + 2 + ... + k + (k+1) = \sum_{i=1}^{k} i + (k+1)$$

Using our assumption from before we can replace the $\sum_{i=1}^{k} i$ term with $\frac{k(k+1)}{2}$:

$$= \frac{k(k+1)}{2} + (k+1)$$

and simplify:

$$= \frac{k(k+1) + 2(k+1)}{2} = \frac{k^2 + 3k + 2}{2} = \frac{(k+1)(k+2)}{2}$$

as required. Therefore, by induction, the formula is true for all $n \in \mathbb{N}$.

All proofs by induction look the same: they have *Basis*, where you check the starting n, and *Inductive step*, where you make an assumption for n = k and prove the statement for n = k + 1. Somewhere in the proof you should use your assumption, and you should indicate that place. (If you don't use the assumption, then you don't need to make it, so you have a direct proof, not an inductive proof.) The last line finishes the proof by appealing to the mathematical induction, and often is omitted

1.4 Practice Problems

1.4.1 Problem 1.1

Prove by induction: $n(n+7) \vdots 2$ for any $n \in \mathbb{N}$.

*Proof. Basis:*If $n = 1$, check: $1(1+7) \vdots 2$.
Inductive step: Assume the statement is true for $n = k$. Then $k(k+7) \vdots 2$. Need to show that it is true for $n = k+1 : (k+1)(k+8) \vdots 2$:

$$k^2 + 9k + 8 = k(k+7) + (2k+8) = k(k+7) + 2(k+4)$$

We know by assumption that $k(k+7) \vdots 2$, and by definition of divisibility, $2(k+4)$ is divisible by 2 for any $k \in \mathbb{N}$. Therefore, the statement is true for all $n \in \mathbb{N}$. QED

1.4.2 Problem 1.3

Prove by induction: $7^n + 3^n \vdots 2$ for all $n \in \mathbb{N}$.

Proof. Basis: If $n = 1$, check: $7^1 + 3^1 = 10 \vdots 2$.
Inductive step. Assume the statement holds for $n = k$, $7^k + 3^k \vdots 2$, or $7^k + 3^k = 2d$. We must show that the statement is true for $n = k + 1$. So $7^{k+1} + 3^{k+1} \vdots 2$, or $7^{k+1} + 3^{k+1} = 2c$.

$$7^{k+1} + 3^{k+1} = 7 \cdot 7^k + 3 \cdot 3^k$$

Since $7^k + 3^k \vdots 2$, then $7^k + 3^k = 2d$, and $3^k = 2d - 7^k$. So:

$$= 7 \cdot 7^k + 3 \cdot (2d - 7^k) = 4 \cdot 7^k + 6d$$

We have 2 terms, $4 \cdot 7^k$ and $6d$. Since both are divisible by 2, the sum of them will always be divisible by 2, and since that equation is the same as $7^{k+1} + 3^{k+1}$, that means $7^{k+1} + 3^{k+1} \vdots 2$. Therefore, by induction, $7^n + 3^n \vdots 2$ for all $n \in \mathbb{N}$. QED

1.4.3 Problem 1.7

Prove: a number n is divisible by 5 iff its last digit is either 0 or 5.

Proof. ($\Longrightarrow$): All numbers n which end in 0 can be written as $n = 10k, k \in \mathbb{Z}$, since $10 \vdots 5$ always, $10k \vdots 5$, and therefore $n \vdots 5$ if n ends in 0. If a number n ends in 5 it can be expressed as $n = 10k + 5$, and since $10k + 5 = 5(k + 1)$, $10k + 5 \vdots 5$. Which means $n \vdots 5$ if n ends in 5.
($\Longleftarrow$): If n ends in any other number, then $n = 10k + a$, where $a \in S, S = \{1, 2, 3, 4, 6, 7, 8, 9\}$ since $10k \vdots 5$, we can remove it, so in essence, $n = a \pmod 5$. Since $a \neq 5l$ for $l \in \mathbb{Z}$, $10k + a \not\vdots 5$ and so $n \not\vdots 5$ if n ends in any a.
$\therefore n \vdots 5 \Longleftrightarrow n$ ends in 0 or 5. QED

2 Direct Proof, Proof by Contradiction

2.0.1 Problem 2.2

Prove: if $(a-b) \vdots c$, then $a \vdots c$ iff $b \vdots c$.

Proof. To prove iff, we must first prove “If A, then B” (forwards), then prove“if B, then A” (backwards).
($\Longrightarrow$): Assume that $a \vdots c$ is true, that is, $a = cn$. $(a-b) \vdots c$ implies that $(a-b) = cl, l \in \mathbb{Z}$. Rearranging for b we get $b = a - cl = cn - cl = c \cdot (n-l) \therefore$ if $a \vdots c, b \vdots c$.
($\Longleftarrow$): Assume that $b \vdots c$ is true, that is, $b = cm$. We know from above that $(a-b) = cl$. Rearranging for a we get $a = cl + b = cl + cm = c \cdot (l+m) \therefore$ if $b \vdots c, a \vdots c$. QED

2.0.2 Problem 2.3

Prove: If $a \vdots c$, then for any $b, (ab) \vdots c$.

Proof. $a \vdots c$ implies that $\exists n \in \mathbb{Z}$ s.t. $a = cn$. Thus, $a \cdot b = b(cn)$, and by the commutative property, $b(cn) = c(bn)$. Let $(bn) = m$, so $a \cdot b = cm, m \in \mathbb{Z}$, therefore $a \cdot b$ is divisible by c. QED

2.0.3 Problem 2.4

Prove: if $a \vdots b$ and $b \vdots c$, then $a \vdots c$.

Proof. $a \vdots b \Longrightarrow a = bn, n \in \mathbb{Z}$. Also, $b \vdots c \Longrightarrow b = cm$. Solving the first equation for b: $b = \frac{a}{n}$. Plugging it into the second: $\frac{a}{n} = cm$. So $a = cmn = c \cdot (mn)$. Therefore $a \vdots c$. QED

3 Mathematical Induction

3.0.1 Problem 3.1

Prove by induction: for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n}(2i-1) = n^2.$$

Proof. Basis: $n = 1$ Check: $\sum_{i=1}^{1}(2i-1) = 1 = n^2$.
Induction step: Assume the formula holds for $n = k$

$$\sum_{i=1}^{k}(2i-1) = k^2.$$

We must show it holds for $n = k + 1$:

$$\sum_{i=1}^{k+1}(2i-1) = (k+1)^2 = k^2 + 2k + 1.$$

The sum is the sum of the first k terms, plus the last one.

$$\sum_{i=1}^{k+1}(2i-1) = \sum_{i=1}^{k}(2i-1) + 2k + 1$$

Using assumption:

$$\sum_{i=1}^{k}(2i-1) + 2k + 1 = k^2 + 2k + 1 = (k+1)^2$$

As required. Therefore, by induction, the formula is true for all $n \in \mathbb{N}$ QED

3.0.2 Problem 3.2

Prove by induction: for all $n \in \mathbb{N}$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof. Basis: $n = 1$ Check: $\sum_{i=1}^{1} i^2 = 1 = \frac{1(1+1)(2+1)}{6}$
Induction step: Assume the formula holds for $n = k$:

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6} = \frac{2k^3 + 3k^2 + k}{6}$$

We must show it holds for $n = k + 1$:

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(k+2)(2k+3)}{6} = \frac{2k^3 + 9k^2 + 13k + 6}{6}$$

The sum on the left is equal to the sum from $i = 1$ to k, plus the term $i = k + 1$:

$$\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + k^2 + 2k + 1$$

Using assumption:

$$\sum_{i=1}^{k} i^2 + k^2 + 2k + 1 = \frac{k(k+1)(2k+1)}{6} + k^2 + 2k + 1$$

Simplifying:

$$= \frac{2k^3 + 3k^2 + k}{6} + \frac{6k^2 + 12k + 6}{6} = \frac{2k^3 + 9k^2 + 13k + 6}{6} = \sum_{i=1}^{k+1} i^2$$

$\therefore$ the formula is true for all $n \in \mathbb{N}$. QED

3.0.3 Problem 3.3

Prove by induction: for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i^3 = (\sum_{i=1}^{n} i)^2.$$

Proof. Basis: $n = 1$ Check: $\sum_{i=1}^{1} i^3 = 1 = (\sum_{i=1}^{1} i)^2$.
Induction step: Assume the formula holds for $n = k$:

$$\sum_{i=1}^{k} i^3 = (1 + 2 + 3 + ... + k)^2$$

Show that the formula holds for $n = k + 1$:

$$\sum_{i=1}^{k+1} i^3 = (1 + 8 + 27 + ... + k^3 + (k + 1)^3)$$

The sum from 1 to $k + 1$ is equal to the sum from 1 to k, plus the $i = k + 1$ term, so:

$$\sum_{i=1}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k + 1)^3$$

Using our assumption, and the fact that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$:

$$\sum_{i=1}^{k+1} i^3 = (1 + 2 + 3 + ... + k)^2 + (k + 1)^3 = (\frac{k(k + 1)}{2})^2 + (k + 1)^3$$

Simplifying:

$$(\frac{k(k + 1)}{2})^2 + (k + 1)^3 = \frac{k^2(k + 1)^2}{4} + (k + 1)^3 = \frac{k^2(k + 1)^2 + 4(k + 1)^3}{4}$$

More simplifying:

$$\frac{k^2(k + 1)^2 + 4(k + 1)^3}{4} = \frac{k^4 + 6k^3 + 13k^2 + 12k + 4}{4} = \frac{(k + 1)^2(k + 2)^2}{4}$$

Factoring out a square:

$$\frac{(k + 1)^2(k + 2)^2}{4} = (\frac{(k + 1)(k + 2)}{2})^2$$

And since $(\frac{(k+1)(k+2)}{2})^2$ Is equal to $(\sum_{i=1}^{k+1} i)^2$, we have proven the induction case, and therefore the formula is true for all $n \in \mathbb{N}$. QED

3.0.4 Problem 3.4

Find:

$$\sum_{k=1}^{n} k(k!)$$

Let $f(n) = \sum_{k=1}^{n} k(k!)$

n	$f(n)$
1	1
2	5
3	23
4	119
5	719

Conjecture: $\sum_{k=1}^{n} k(k!) = (n+1)! - 1, n \in \mathbb{N}$.

Proof. Basis: Check $n = 1$: $\sum_{k=1}^{1} k(k!) = 1 = (1+1)! - 1$
Inductive step: Assume the conjecture holds for $k = n$:

$$\sum_{k=1}^{n} k(k!) = (n+1)! - 1$$

Show the conjecture holds for $k = n + 1$:

$$\sum_{k=1}^{n+1} k(k!) = (n+2)! - 1$$

The sum from 1 to $n+1$ includes the entire sum from 1 to n, plus the $k = n+1$ term:

$$\sum_{k=1}^{n+1} k(k!) = \sum_{k=1}^{n} k(k!) + (n+1)((n+1)!)$$

Using our assumption:

$$\sum_{k=1}^{n+1} k(k!) = (n+1)! - 1 + (n+1)((n+1)!)$$

Note that:

$$(n+1)! = (n+1) \times n \times (n-1) \times ... \times 1$$

For simplicity's sake, let $x = (n+1)$:

$$\sum_{k=1}^{n+1} k(k!) = x! - 1 + x \times x! = (x+1) \times x! - 1$$

By the definition of a factorial:

$$(x+1) \times x! = (x+1)!$$

So:

$$\sum_{k=1}^{n+1} k(k!) = (x+1) \times x! - 1 = (x+1)! - 1$$

Substitute $(n+1)$ for x:

$$\sum_{k=1}^{n+1} k(k!) = (n+2)! - 1.$$

As required, $\therefore$ our conjecture is true, $\sum_{k=1}^{n} k(k!) = (n+1)! - 1, n \in \mathbb{N}$. QED

3.0.5 Problem 3.5

Prove *Bernoulli's inequality*: if $a > -1$ then $(1+a)^n \geq 1 + na$ for all $n \in \mathbb{N}$

Proof. Basis: $n = 1$ Check: $(1+a)^1 = 1 + a$.
Inductive step: Assume the inequality holds for $n = k$:

$$(1+a)^k \geq 1 + ka$$

Prove it holds for $n = k + 1$:

$$(1+a)^{k+1} \geq 1 + (k+1)a$$

Splitting up the exponent:

$$(1+a)^{k+1} = (1+a)^k \times (1+a)$$

Using our assumption $(1+a)^k \geq 1 + ka$:

$$(1+a)^k \times (1+a) \geq (1+ka)(1+a)$$

Simplifying:

$$(1+ka)(1+a) = 1 + (k+1)a + ka^2$$

And since

$$(1+a)^{k+1} \geq 1 + (k+1)a + ka^2$$

It must also be greater than $1+(k+1)a$, as required. Therefore by induction, the inequality is true for $a > -1$ QED

3.0.6 Problem 3.6

Prove by completing the square:

$$2n + 1 < n^2 : n \geq 3$$

Proof. Moving everything to one side:

$$n^2 - 2n - 1 > 0 : n \geq 3$$

Completing the square:

$$(n-1)^2 - 2 > 0 : n \geq 3$$

Getting n alone:

$$(n-1)^2 > 2 : n \geq 3$$

The absolute smallest that $(n-1)^2$ can be is 4, when $n = 3$, which is greater than 2. Therefore, $(n-1)^2 > 2 : n \geq 3$, and similarly:

$$2n + 1 < n^2 : n \geq 3$$

QED

3.0.7 Problem 3.7

Prove by induction: $2^n \geq n^2 : n \geq 4$

Proof. Basis: $n = 4$ Check:

$$2^4 \geq 4^2$$

Indeed it is, *Induction step*: Assume the conjecture holds for $n = k$:

$$2^k \geq k^2 : k \geq 4$$

Show it holds for $n = k + 1$:

$$2^{k+1} \geq (k+1)^2 : k \geq 3$$

Splitting up the exponent:

$$2^k \times 2 \geq k^2 + 2k + 1$$

Using our assumption $2^k \geq k^2$:

$$2^k \times 2 \geq 2k^2 \geq k^2 + 2k + 1 = (k+1)^2 : (k \geq 3)$$

And since

$$2^k \times 2 = 2^{k+1}$$

The following must be true:

$$2^{k+1} \geq (k+1)^2 : (k \geq 3)$$

As required. Therefore, by induction the inequality is true. QED

4 Divisibility

4.1 Notation:

$a \vdots b$ Means “a is *divisible* by b.”
$a \not\vdots b$ Means “a is *not divisible* by b.”

4.2 Definition:

$a \in \mathbb{Z}$ is *divisible* by $b \in \mathbb{N}$ (denoted by $a \vdots b$) if there exists $c \in \mathbb{Z}$ such that $a = bc$.

4.3 Example:

$-12 \vdots 3$ since $-12 = 3 * (-4)$, but $-12 \not\vdots -4$ since $-4 \notin \mathbb{N}$.

4.4 Example:

Prove: If $a \vdots c$ and $b \vdots c$, then $(a + b) \vdots c$.

Proof. If $a \vdots c$, then by definition $\exists n \in \mathbb{Z} \mid a = cn$ and $c \in \mathbb{N}$. Similarly, if $b \vdots c$, then $\exists m \in \mathbb{Z} \mid b = cm$. Then $a + b = cn + cm = c(n + m)$, so $(a + b) \vdots c$ by definition. QED

4.5 Practice problems

4.5.1 Problem 4.1

Prove: if $a \vdots b$ and $b \vdots c$, then $(a - b) \vdots c$.

Proof. If $a \vdots c$, then by definition, $\exists n \in \mathbb{Z}$ s.t. $a = cn$. Similarly, if $b \vdots c$, then by definition, $\exists m \in \mathbb{Z}$ s.t. $b = cm$. ($a, b \in \mathbb{Z}$, and $c \in \mathbb{N}$). Then $(a - b) = cn - cm = c(n - m)$, since $(n - m) \in \mathbb{Z}$, $(a - b) = cl$, $\therefore (a - b) \vdots c$. QED

4.5.2 Problem 4.2

Prove: if $(a - b) \vdots c$, then $a \vdots c$ iff $b \vdots c$.

Proof. To prove iff, we must first prove “If A, then B” (forwards), then prove“if B, then A” (backwards).
($\Longrightarrow$): Assume that $a \vdots c$ is true, that is, $a = cn$. $(a-b) \vdots c$ implies that $(a-b) = cl, l \in \mathbb{Z}$. Rearranging for b we get $b = a - cl = cn - cl = c \cdot (n-l) \therefore$ if $a \vdots c, b \vdots c$.
($\Longleftarrow$): Assume that $b \vdots c$ is true, that is, $b = cm$. We know from above that $(a-b) = cl$. Rearranging for a we get $a = cl + b = cl + cm = c \cdot (l+m) \therefore$ if $b \vdots c, a \vdots c$. QED

4.5.3 Problem 4.3

Prove: If $a \vdots c$, then for any $b, (ab) \vdots c$.

Proof. $a \vdots c$ implies that $\exists n \in \mathbb{Z}$ s.t. $a = cn$. Thus, $a \cdot b = b(cn)$, and by the commutative property, $b(cn) = c(bn)$. Let $(bn) = m$, so $a \cdot b = cm, m \in \mathbb{Z}$, therefore $a \cdot b$ is divisible by c. QED

4.5.4 Problem 4.4

Prove: if $a \vdots b$ and $b \vdots c$, then $a \vdots c$.

Proof. $a \vdots b \Longrightarrow a = bn, n \in \mathbb{Z}$. Also, $b \vdots c \Longrightarrow b = cm$. Solving the first equation for b: $b = \frac{a}{n}$. Plugging it into the second: $\frac{a}{n} = cm$. So $a = cmn = c \cdot (mn)$. Therefore $a \vdots c$. QED

4.5.5 Problem 4.5

Prove by induction: $n(n+7) \vdots 2$ for any $n \in \mathbb{N}$.

Proof. *Basis:*If $n = 1$, check: $1(1+7) \vdots 2$.
Inductive step: Assume the statement is true for $n = k$. Then $k(k+7) \vdots 2$. Need to show that it is true for $n = k+1 : (k+1)(k+8) \vdots 2$:

$$k^2 + 9k + 8 = k(k+7) + (2k+8) = k(k+7) + 2(k+4)$$

We know by assumption that $k(k+7) \vdots 2$, and by definition of divisibility, $2(k+4)$ is divisible by 2 for any $k \in \mathbb{N}$. Therefore, the statement is true for all $n \in \mathbb{N}$. QED

4.5.6 Problem 4.6

Prove by induction: $7^n + 3^n \vdots 2$ for all $n \in \mathbb{N}$.

Proof. Basis: If $n = 1$, check: $7^1 + 3^1 = 10 \vdots 2$.
Inductive step. Assume the statement holds for $n = k$, $7^k + 3^k \vdots 2$, or $7^k + 3^k = 2d$. We must show that the statement is true for $n = k + 1$. So $7^{k+1} + 3^{k+1} \vdots 2$, or $7^{k+1} + 3^{k+1} = 2c$.

$$7^{k+1} + 3^{k+1} = 7 \cdot 7^k + 3 \cdot 3^k$$

Since $7^k + 3^k \vdots 2$, then $7^k + 3^k = 2d$, and $3^k = 2d - 7^k$. So:

$$= 7 \cdot 7^k + 3 \cdot (2d - 7^k) = 4 \cdot 7^k + 6d$$

We have 2 terms, $4 \cdot 7^k$ and $6d$. Since both are divisible by 2, the sum of them will always be divisible by 2, and since that equation is the same as $7^{k+1} + 3^{k+1}$, that means $7^{k+1} + 3^{k+1} \vdots 2$. Therefore, by induction, $7^n + 3^n \vdots 2$ for all $n \in \mathbb{N}$. QED

4.5.7 Problem 4.7

Prove: a number n is divisible by 5 iff its last digit is either 0 or 5.

Proof. ($\Longrightarrow$): All numbers n which end in 0 can be written as $n = 10k, k \in \mathbb{Z}$, since $10 \vdots 5$ always, $10k \vdots 5$, and therefore $n \vdots 5$ if n ends in 0. If a number n ends in 5 it can be expressed as $n = 10k + 5$, and since $10k + 5 = 5(k + 1)$, $10k + 5 \vdots 5$. Which means $n \vdots 5$ if n ends in 5.
($\Longleftarrow$): If n ends in any other number, then $n = 10k + a$, where $a \in S, S = \{1, 2, 3, 4, 6, 7, 8, 9\}$ since $10k \vdots 5$, we can remove it, so in essence, $n = a$ (mod 5). Since $a \neq 5l$ for $l \in \mathbb{Z}$, $10k + a \not\vdots 5$ and so $n \not\vdots 5$ if n ends in any a.
$\therefore n \vdots 5 \Longleftrightarrow n$ ends in 0 or 5. QED

5 Division with Remainder

5.1 Practice Problems

5.1.1 Problem 5.1

Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Suppose a is divided by b with remainder r and quotient q. Divide $a + 1$ by b with remainder.

Proof. By definition of divisibility with remainder,

$$a = bq + r \text{ and } 0 \leq r < b$$

Also by theorem 4.1, $q, r \in \mathbb{Z}$ are unique $\forall a$. So

$$a + 1 = bq' + r'$$

There are 2 cases:

1. $r \in \{0, 1, ...b - 2\}$: In this case $r' = r + 1$, and since $r \leq b - 2$ we know $r' \leq b - 1$ and thus $r' < b$. Also because we haven't "overflowed*" so to speak, $q' = q$.
   (* By this I mean since $r' < b$, q remains the same, whereas if $r' = b$, then $q' = q + 1$.)

2. $r = b - 1$: In this case, $r' = b$, since $r' = r + 1 = (b - 1) + 1 = b$. And since $r' = b$, this is division with remainder 0, (or normal division). Also since $r' = b$, $q' = q + 1$.

So $a + 1 = bq + r + 1$ when $r \in \{0, 1, ...b - 2\}$.
And $a + 1 = b(q + 1) + 0$ when $r = b - 1$. QED

5.1.2 Problem 5.3

Let $b \in \mathbb{N}$ and let $a \in \mathbb{Z}^{<}$. Prove the existence of $q, r \in \mathbb{Z}$, such that $a = bq+r$ and $0 \leq r < b$.

Proof. By definition, $a = bq+r$, and $0 \leq r < b$, then $-a = bq'+r'$, $0 \leq r < b$. $q' = -q$, however r' can be one of two things, either:

1. $r' = b - r$: In this case, $-a = bq' + r' = -bq + b - r = -b(q - 1) - r$. Therefore $q, r \in \mathbb{Z}$ exist for $-a$.

2. $r' = b + r$: In this case, $-a = bq' + r' = -bq + b + r = -b(q-1) + r$. Therefore q, r exist, and are unique, for $-a$.

QED

5.1.3 Problem 5.4

Let $b \in \mathbb{N}$ and suppose $-b < r < b$. Prove that if $r \vdots b$, then $r = 0$.

Proof. Recall that by definition of divisibility, $r \vdots b \implies r = bn,$ for some $n \in \mathbb{Z}$. Also since $-b < r < b$, then

$$-b < bn < b$$

again where $n \in \mathbb{Z}$. We can divide everything by b to get:

$$-1 < n < 1, n \in \mathbb{Z}$$

There are no integers n between -1 and 1, except 0. Thus $n = 0$ and since $r = bn$, $r = 0$. QED

6 Prime Numbers

6.1 Practice Problems

6.1.1 Problem 6.1

Find all prime numbers p such that $p+1$ is prime.
$p = 2$.

Proof.

Theorem 1. *For any odd numbers n, a, $n + a$ is even. Recall the definition of an odd number is some number $n = 2k+1, k \in \mathbb{Z}$, or $a = 2k_1 + 1, k_1 \in \mathbb{Z}$. An even number $m = 2l, l \in \mathbb{Z}$. So $n + a = 2k + 2k_1 + 2 = 2(k + k_1 + 1)$, and since $(k + k_1 + 1) \in \mathbb{Z}$, $n + a$ is even.*

Theorem 2. *Any positive even integer $n > 2$ is composite, since $n = 2k$, for some $k > 1 \in \mathbb{N}$, therefore 2 divides n, and since $2 \neq 1$ and $2 \neq n$, by definition n is composite.*

Corollary 2.1. *All prime numbers $p \neq 2$ are odd.*

There are 2 cases for this problem:

1. Case 1: $p = 2$, if $p = 2$, $p + 1 = 3$ is prime. So this case is a solution.

2. Case 2: p is a prime number greater than 2. Thus, by Theorem 1, $p + 1 = n$, where n is some some positive even integer > 2. And by Theorem 2, any positive even integer greater than 2 is composite, thus every prime number greater than 2 does not work.

QED

6.1.2 Problem 6.5

Prove that for any $n \in \mathbb{N}$, n and $n+1$ are relatively prime.

Proof.

Remark. *Two numbers $a, b \in \mathbb{N}$ are relatively prime if* $\gcd(a, b) = 1$.

Also recall the Euclidean Algorithm, by definition 5.1 using Euclidean Alg. on $(n + 1, n)$, we achieve:

$$n + 1 = n \cdot 1 + 1$$

$$n = 1 \cdot n + 0$$

The Euclidean Algorithm is over, and it states that $\gcd(n+1, n) = 1$, therefore $n+1, n$ are relatively prime. QED

6.1.3 Problem 6.9

True or false: for any $n \in \mathbb{N}, n^2 + n + 41$ is prime. False.

Proof. Counterexample: Let $n = 40$, $40^2 + 40 + 41 = 1681$, and $1681 = 41 \cdot 41$ $\therefore$ by definition, since $41 \in \mathbb{N}$, the number is composite and the proposition is false. QED

7 Prime Numbers cont.

7.1 Practice Problems

7.1.1 Problem 7.4

True or False: There are infinitely many primes.
True.

Proof. Suppose $p_1 = 2 < p_2 = 3 < ... < p_n$ are all the primes. Let P be the product of all the primes plus one ($P = p_1p_2...p_n + 1$). Then P is either prime or it is not. If P is prime, then it is a prime that wasn't in our list. If P is composite, then there exists some p such that $P \vdots p$. Notice p can not be any of $p_1 = 2 > p_2 = 3 > ... > p_n$, otherwise p would divide 1, which is impossible. So then p is some prime which is not on our list. So there must exist at least one prime not in our list, for any list of primes, so there are infinitely many primes. QED

7.1.2 Problem 7.5

Describe $\gcd(a, b)$ in terms of the prime factorizations of a and b.

Proof.

Remark. *Let the infinite product $n = 2^{n_2}3^{n_3}5^{n_5}...p^{n_p}...$ be the prime factorization of n. For example $n = 18 = 2^1 \cdot 3^2 \cdot 5^0 \cdot ...p^0...$*

Let $a = 2^{a_2}3^{a_3}5^{a_5}...p^{a_p}...$ and $b = 2^{b_2}3^{b_3}5^{b_5}...p^{b_p}...$, then $\gcd(a, b) =$ some $c = 2^{c_2}3^{c_3}5^{c_5}...p^{c_p}...$, where $c_p = \min(a_p, b_p)$. Since the minimum power of each prime which is shared between a_p, b_p is c_p, and when a, b share prime factors, the product of those shared factors is the gcd. QED

7.1.3 Problem 7.6

Find $\text{lcm}(1, 2, 3, ..., 20)$. Prime factorizations:

1. $1 = 1$
2. $2 = 2$
3. $3 = 3$
4. $4 = 2 * 2$

5. $5 = 5$

6. $6 = 2 * 3$

7. $7 = 7$

8. $8 = 2 * 2 * 2$

9. $9 = 3 * 3$

10. $10 = 2 * 5$

11. $11 = 11$

12. $12 = 2 * 2 * 3$

13. $13 = 13$

14. $14 = 2 * 7$

15. $15 = 3 * 5$

16. $16 = 2 * 2 * 2 * 2$

17. $17 = 17$

18. $18 = 2 * 3 * 3$

19. $19 = 19$

20. $20 = 2 * 2 * 5$

Highest amount that each prime occurs: $19 \cdot 17 \cdot 13 \cdot 11 \cdot 7 \cdot 5 \cdot 3^2 \cdot 2^4 = 232,792,560$

8 Set Theory

8.1 Practice Problems

8.1.1 Problem 8.3

Let $f : X \to Y$ and $g : Y \to Z$ be maps, prove that if the composition $g \circ f$ is injective then f is injective.

Proof. Consider the injective composition $g \circ f : X \to Z$, and suppose $x_1 \neq x_2$ this implies $g(f(x_1)) \neq g(f(x_2))$. By the definition of a function, this implies that $f(x_1) \neq f(x_2)$, thus f is an injection. QED

8.1.2 Problem 8.9

Construct a bijection from $\mathbb{N}$ to $2\mathbb{Z}^+$ (the set of positive, even integers).

Proof. Consider a function $f : \mathbb{N} \to 2\mathbb{Z}^+$, defined by $f(n) = 2n$. This is the mapping, $(1 \to 2), (2 \to 4), (3 \to 6), ...$
N2S (need to show): f is bijective, or f is both injective and surjective.

Remark. *Recall that a function $g : X \to Y$, is injective if $\forall x_1 \neq x_2 \in X$, $g(x_1) \neq g(x_2)$.*

Remark. *A function $g : X \to Y$, is surjective if $\forall y \in Y$, $\exists x \in X$ such that $g(x) = y$.*

1. Injectivity: $\forall n_1 \neq n_2 \in \mathbb{N}$, then the mapping is $f(n_1) = 2n_1$ and $f(n_2) = 2n_2$, if $f(n_1) = f(n_2)$ then $2n_1 = 2n_2 \implies 2(n_1 - n_2) = 0$. However since the integers have no nontrivial zero divisors, $(n_1 - n_2)$ must be equal to zero, therefore $n_1 = n_2$. And since this is true, the contrapositive must be true (if $n_1 \neq n_2$, then $f(n_1) \neq f(n_2)$), as required. Therefore the function f is injective.

2. Surjectivity: $\forall z \in 2\mathbb{Z}^+$, $\exists n \in \mathbb{N}$ such that $f(n) = z$. If we choose some arbitrary $z \in 2\mathbb{Z}^+$, by definition, $z = 2n$, and since z is a positive, even integer, we can write this as $z = f(n)$. Therefore f is surjective.

Since $f(n) = z$ is both injective and surjective, then it is a bijection from $\mathbb{N} \to 2\mathbb{Z}^+$, As required. QED

8.1.3 Problem 8.10

Prove that there is a bijection $\mathbb{N} \to \mathbb{Z}$.

Proof. Consider $f : \mathbb{N} \to \mathbb{Z}$, defined by $f(n) = \begin{cases} k & n = 2k \\ -k & n = 2k+1 \end{cases}$

This maps $(1 \to 0), (2 \to 1), (3 \to -2), (4 \to 2), ...$

Remark. *A function $f : X \to Y$ is injective iff $f(x) = f(y) \implies x = y$.*

N2S: Bijectivity

1. Injectivity: For some $n_1, n_2 \in \mathbb{N}$, suppose $f(n_1) = f(n_2)$. Then there are 3 cases:

   (a) If they are both even, then $f(n_1) = k$, where $n_1 = 2k$. Also $f(n_2) = k$, where $n_2 = 2k$, it is clear that, $n_1 = n_2 = 2k$.

   (b) If they are both odd, then $f(n_1) = -k$, where $n_1 = 2k+1$. Also $f(n_2) = -k$, where $n_2 = 2k+1$, again it is clear that $n_1 = n_2 = 2k+1$.

   (c) If one is even and one is odd, then $f(n_1) = k$, where $n_1 = 2k$ and $f(n_2) = -k$, where $n_2 = 2k+1$. However in this case $n_1 \neq n_2$, because one is $2k$, and one is $2k+1$. $2k \neq 2k+1$, clearly. ↯

   Therefore f is an injection.

2. Surjectivity: $\forall z \in \mathbb{Z}$, $\exists n \in \mathbb{N}$ s.t. $f(n) = z$. Take some $z \in \mathbb{Z}$, z has a sign (positive or negative), or it is 0.

   (a) If z is positive, then z is produced by $f(2n)$. Ex. $(z = 1, n = 2$, $(z = 2, n = 4)$,...

   (b) If z is negative, then z is produced by $f(2n+1)$. Ex. $(z = -1, n = 3)$, $(z = -2, n = 5)$,...

   (c) If $z = 0$, it is produced by $f(1)$.

   And since each z has a unique producer in terms of n, the function f is surjective.

Since f is both injective and surjective, then it is a bijection from $\mathbb{N} \to \mathbb{Z}$, as required. QED

9 Equivalence Relations

9.1 Practice Problems

9.1.1 Problem 9.1

Give 3 examples of nonequivalence relations

1. Let $S = Z$ and $R(x, y) =$ "$x < y$". This is not an equivalence relation because it is not symmetric, because $x < y$ does not imply $x > y$.

2. Let $S = Z$ and $R(x, y) =$ "$x > y$". This is not an equivalence relation because it is not symmetric, because $x > y$ does not imply $x < y$.

3. Let $S = Z$ and $R(x, y) =$ "x is a child of y". This is not an equivalence relation because it is not reflexive, because if $x =$ me, I am not a child of myself.

9.1.2 Problem 9.8

Find $6^{2020} + 8^{2019} \mod 7$.
Since $6 \equiv -1 \mod 7$ and $8 \equiv 1 \mod 7$: $6^{2020} + 8^{2019} \equiv -1^{2020} + 1^{2019} \mod 7$. And since 2020 is even, $-1^{2020} = 1$. And obviously, $1^{2019} = 1$. So $6^{2020} + 8^{2019} \equiv 1 + 1 = 2 \mod 7$.

10 Modular Arithmetic, Mult. inverses

10.1 Practice Problems

10.1.1 Problem 10.1

Let $a, n \in \mathbb{N}$, $n > 1$ be relatively prime. Prove that $[a]_n$ has a multiplicative inverse in Z_n.

Proof. Since gcd can be written as a linear combination, and a, n being relatively prime implies $\gcd(a, n) = 1$, then

$$ax + ny = 1$$

Is true. We can take both sides modulo n:

$$(ax + by) \mod n = 1 \mod n$$

This can be rewritten as:

$$[a]_n[x]_n + [n]_n[y]_n = [1]_n$$

Since $n \equiv 0 \mod n$,

$$[a]_n[x]_n + [n]_n[y]_n = [a]_n[x]_n + 0 \cdot [y]_n = [1]_n$$

Then, by definition,

$$[a]_n[x]_n = [1]_n$$

As required, $x \in \mathbb{Z}_n$ is the inverse of a. QED

10.1.2 Problem 10.3

Find all the invertible elements of $\mathbb{Z}_{10}$.

Remark. *By problem 10.1, an element $a \in \mathbb{Z}_x$ is invertible iff $\gcd(a, x) = 1$, that is to say that the only invertible elements are relatively prime to the modulus x.*

Therefore the invertible elements in $\mathbb{Z}_{10}$ are $\{1, 3, 7, 9\}$. We can also check that this is correct because Euler's Totient function, $\phi(10) = 4$, which is the number of elements relatively prime to 10. :)

10.1.3 Problem 10.4

Let p be a prime, find all invertible elements of $\mathbb{Z}_p$.
As described above, invertible elements are all of the elements $a \in \mathbb{Z}_p$ such that $\gcd(a, p) = 1$. Since p is prime, it is relatively prime to every number smaller than it, so the invertible elements of $\mathbb{Z}_p$ are: $\{1, 2, ..., p-1\}$.

11 Modular Arithmetic, Wilson's Theorem, Fermat's little theorem

11.1 Practice Problems

11.1.1 Problem 11.1

Let p be prime, solve the equation $x^2 \equiv 1$ in $\mathbb{Z}_p$. (Find all solutions, and prove that there are no other solutions.)

Proof.

$$x^2 = 1 \Longrightarrow x^2 - 1 = 0 \Longrightarrow (x+1)(x-1) = 0$$

Assume $(x+1)$ is nonzero, because we are in $\mathbb{Z}_p$, all nonzero elements are invertible. So multiplying by $(x+1)^{-1}$:

$$(x+1)(x+1)^{-1}(x-1) = 0(x+1)^{-1} \Longrightarrow (x-1) = 0, \text{ so } x = 1$$

Now assume $(x-1)$ is nonzero. Again, $(x-1)$ is invertible, so multiplying by $(x-1)^{-1}$ yields a similar result:

$$(x-1)(x-1)^{-1}(x+1) = 0(x-1)^{-1} \Longrightarrow (x+1) = 0, \text{ so } x = -1$$

These are the only 2 cases for which this is true, $x = 1, -1$. QED

11.1.2 Problem 11.4

Let p be prime, let $S = \mathbb{Z}_p - \{0\} = \{[1]_p, [2]_p, ..., [p-1]_p\}$. Prove that for $y \neq 0$, L_y restricts to a bijective map $L_y|_S : S \to S$. (Prove that there are no 0 divisors in $\mathbb{Z}_p$)

Proof. N2S: $\nexists x \in S$, such that $L_y(x) = 0$. To the contrary, assume such an x does exist.
Suppose

$$L_y(x) = 0$$

then

$$yx = 0$$

Since $y \in S$, it is invertible, ($\exists y' \in S$ s.t. $yy' = 1$). Multiply by y' on both sides:

$$yy'x = 0y'$$

This yields: $x = 0$ ↯ Because $0 \notin S$. So L_y restricts to a bijective map $S \to S$. QED

11.1.3 Problem 11.7

Find $2019^{2020} \mod 43$.
By FlT, (Fermat's Little Theorem) Since 43 is prime, any $a^{42} = 1 \mod 43$.

$$2020 = 42 \cdot 48 + 4, \text{ and } 2019 = -2 \mod 43$$

$$2019^{2020} = (-2^{42})^{48}(-2^4)$$

As stated above, by FlT,

$$(-2^{42})^{48} = 1^{48} = 1 \mod 43$$

So

$$(-2^{42})^{48}(-2^4) = 1 \cdot -2^4 = 16 \mod 43$$

12 Modular Arithmetic, Euler's ϕ function, Euler's Theorem

12.1 Practice Problems

12.1.1 Problem 12.1

Prove that for every $n \geq 0$, $11^{12n+6} + 1 \vdots 13$.

Proof. N2S: $11^{12n+6} \equiv -1 \mod 13$. By definition,

$$11^{12n+6} = (11^{12})^n \cdot (11)^6$$

And by FlT, $a^{12} \equiv 1 \mod 13$, so

$$(11^{12})^n \cdot (11)^6 \equiv (1)^n \cdot (11)^6 \mod 13$$

For $n \geq 0$, $1^n = 1$. Also, $11 \equiv -2 \mod 13$ So

$$(1)^n \cdot (11)^6 = (-2)^6 = 64 \equiv -1 \mod 13$$

As required. QED

12.1.2 Problem 12.3

Let p be an odd prime. Prove that

$$\sum_{n=1}^{p-1} n \vdots p$$

Proof. Since p is odd, it must be of the form $p = 2k+1$, for some $k \in \mathbb{Z}$. By example 1.1,

$$\sum_{n=1}^{p-1} n = \frac{(p-1)(p)}{2}$$

So

$$2\sum_{n=1}^{p-1} n = p(p-1)$$

Using $p = 2k+1$,

$$p(p-1) = p(2k) = 2kp$$

Since twice the sum is equal to $2kp$, the sum must be equal to kp. By definition, $kp \vdots p$, As required. QED

12.1.3 Problem 12.6

Solve $x^{21} \equiv 6 \mod 7$.

Proof. Using FlT, $x^6 \equiv 1 \mod 7$. Since $x^{18} = (x^6)^3$, $x^{18} \equiv 1 \mod 7$. So $x^{21} \equiv x^3 \mod 7$.
We N2S that $x^3 - 6 \equiv 0 \mod 7$, in other words, $x^3 - 6 = 7n$, for some $n \in \mathbb{N}$.

$$x^3 - 6 = 7n$$

$$x^3 = 7n + 6$$

$$x = \sqrt[3]{7n+6}$$

If $n = 3, 17, 30$, clearly $x \equiv 3, 5, 6 \mod 7$ are solutions, respectively. They are also the only solution because it is clear that $\nexists n \in \mathbb{N}$ such that:

$$0 = 7n + 6$$

$$1 = 7n + 6$$

$$8 = 7n + 6$$

$$64 = 7n + 6$$

And since these are all of the $x \in \mathbb{Z}_7$, we have found all the solutions and proven that there are no others. QED

13 Modular Arithmetic, Euler's Thm cont.

13.1 Practice Problems

13.1.1 Problem 13.1

Find all $\phi(n)$ for $n \leq 12$.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

13.1.2 Problem 13.2

Let p be prime, find $\phi(p)$.

Proof. By definition, because p is prime, there are no numbers smaller than p which evenly divide it. Therefore, since all numbers $\{1, 2, \ldots, p-1\}$ are relatively prime to p, $\phi(p) = p - 1$. QED

13.1.3 Problem 13.6

Prove that $\phi(n)$ is the number of invertible elements in $\mathbb{Z}_n$.

Proof. By definition, an element $x \in \mathbb{Z}_n$ is invertible iff $\gcd(x, n) = 1$, (they are relatively prime). Conveniently, the totient function at n, $\phi(n)$, counts how many numbers smaller than n are relatively prime to n. Therefore $\phi(n)$ is the number of invertible elements in $\mathbb{Z}_n$. QED

14 Applications to RSA

14.1 Practice Problems

14.1.1 Problem 14.1

(i) Produce a pair of keys and a message (a number n).

  (a) $p = 17$, $q = 53$. $N = pq = 901$.

  (b) $\phi(N) = 16 \cdot 52 = 832$.

  (c) Let $e = 3$, check $\gcd(e, p-1) = 1$, and $\gcd(e, q-1) = 1$. Therefore $\gcd(e, \phi(N)) = 1$.

  (d) Find d s.t. $ed \equiv 1 \mod \phi(N)$. $d = 555$.
  $ed = 555 \cdot 3 = 1665 \equiv 1 \mod 832$.

  (e) Public key$=(N, e) = (901, 3)$.
  Private key$=(N, d) = (901, 555)$.

  (f) Message: $n = 99$.

(ii) Encrypt the message.
$c \equiv n^e \mod N$.
$c \equiv 99^3 = 970299 \equiv 823 \mod 901$. Cyphertext: $c = 823$.

(iii) Decrypt the message.
$c^d \equiv n \mod N$.

$$c^d = 823^{555} = 99^{1665} = 99^{k(16)(52)+1}$$

In this case, $k = 2$ because $2 \cdot (16) \cdot (52) = 1664$. According to Euler's Theorem,

$$n^{\phi(N)} \equiv 1 \mod N$$

Also, in step (b) of part (i), we found

$$\phi(N) = 16 \cdot 52 = 832$$

So,

$$n^{(2 \cdot 16 \cdot 52)+1} = \underbrace{(n^{1664})}_{\equiv 1 \mod N} \cdot (n^1) \mod N = n = 99$$

15 Exams

15.1 Exam 1

15.1.1 Problem 1

Prove by induction: $7^{n+1} + 8^{2n-1} \vdots 57$ for all $n \in \mathbb{N}$.

Proof. Basis: Check for $n = 1$: $7^2 + 8 \vdots 57 = 57 \vdots 57$.
Inductive step: Assume that the formula holds for $n = k$. We must show it holds for $n = k + 1$. So, by assumption: $7^{k+1} + 8^{2k-1} \vdots 57$. We must show:

$$7^{k+2} + 8^{2k+1} \vdots 57$$

Simplifying:

$$= 7 \cdot 7^{k+1} + 64 \cdot 8^{2k-1}$$

Rearranging:

$$= 7 \cdot 7^{k+1} + 7 \cdot 8^{2k-1} + 57 \cdot 8^{2k-1} = 7(7^{k+1} + 8^{2k-1}) + 57 \cdot 8^{2k-1}$$

By our assumption:

$$7^{k+1} + 8^{2k-1} \vdots 57 \Longrightarrow 7(7^{k+1} + 8^{2k-1}) \vdots 57$$

and by definition:

$$57 \cdot 8^{2k-1} \vdots 57$$

Finally:

$$7(7^{k+1} + 8^{2k-1}) \vdots 57 \text{ and } 57 \cdot 8^{2k-1} \vdots 57$$
$$\Longrightarrow 7^{k+2} + 8^{2k+1} \vdots 57$$

As required. QED

15.1.2 Problem 2

Prove by induction: if $a \geq -1$, then, $(1 + a)^n \geq 1 + na$ for all $n \geq 0$.

Proof. Basis: Check for $n = 1$: $1 + a \geq 1 + a$.
Inductive step:
Assume the formula holds for $n = k$, so $(1+a)^k \geq (1+ka), a \geq -1$ We must show it holds for $n = k + 1$, that is:

$$(1 + a)^{k+1} \geq (1 + (k + 1)a)$$

Simplifying:

$$(1+a)\cdot(1+a)^k \geq (1+ka+a)$$

QED

15.1.3 Problem 3

Prove if $a \vdots c$ and $b \vdots c$, then for any x and y, $ax+by \vdots c$.

Proof. We must show that $ax+by=cl$, for some $l \in \mathbb{Z}$. $a \vdots c$, by definition means $a=cn, n \in \mathbb{Z}$, similarly, $b \vdots c$ by definition means $b=cm, m \in \mathbb{Z}$. Then for any x, y, $x \cdot cn + y \cdot cm \vdots c$, since we can factor out a c: $ax+by=c(xn+ym)$ let $l=xn+ym$, then we have: $ax+by=cl, l \in \mathbb{Z}$, which, by definition, means $ax+by \vdots c$. QED

15.1.4 Problem 4

Prove that $12 \not\vdots 5$.

Proof. Assume 12 *is* divisible by 5. Then 12=5c, for some **integer** c. This means that $c=\frac{12}{5}$, which is not an integer, thus we have a contradiction, so $12 \not\vdots 5$. QED

15.1.5 Problem 5

Let $a, b, c \in \mathbb{N}$ and suppose $a > c$ and $b > c$. True or false: if $ab \vdots c$, then $a \vdots c$ or $b \vdots c$. Prove.

Proof. This is true, since $ab \vdots c$, by definition, means $ab=cn$, for some $n \in \mathbb{N}$. QED

15.2 Exam 2

15.2.1 Problem 1

Find $\gcd(2322, 654)$ using Euclid's Algorithm.

$$2322 = 654 \cdot 3 + 360$$

$$654 = 360 \cdot 1 + 294$$

$$360 = 294 \cdot 1 + 66$$

$$294 = 66 \cdot 4 + 30$$

$$66 = 30 \cdot +6$$

$$30 = 6 \cdot 5 + 0$$

Therefore $\gcd(2322, 654) = 6$.

15.2.2 Problem 2

Prove that for any $n \geq 2$, the numbers $n! + 2, n! + 3, ..., n! + n$ are composite.

Proof.

Remark. *Any number $n! \in \mathbb{N}$ can be written as $n! = 2 * 3 * 4 * ... * n$.*

Remark. *Any number $n!$ where $n \geq 2$ is even, since it will always be something times 2.*

For any number $n \geq 2$, we may write $n! = 2 * 3 * 4 * ... * n$. n is either even or odd.

1. $\forall n$, $n! + x$, where $x \in \{2, 4, ..., n\}$, is always even, and therefore composite, since $n!$ is even, by the remark above, so you are always able to factor out a 2 from $n! + x$, thus $n! + x$ is composite.

2. $\forall n$, $n! + y$, where $y \in \{3, 5, ..., n-1\}$, is always composite, because if you rearrange $n!$, and factor out y, you get $n! = y(z)$. Where $z = \frac{n!}{y} \in \mathbb{N}$. and we can factor out y from y, of course. Thus, we are able to rewrite $n! + y = y(z + 1)$. For example if $n = 4$, then $n! + 3 = 3(8 + 1)$ is composite. Therefore y is a factor, so $n! + y$ is composite.

Since n plus any even or odd number up to n is composite, then the statement is true. QED

15.2.3 Problem 3

Prove by strong induction that for any $n \in \mathbb{N}$, $n > 1$, there exists a prime factorization of n.

Proof. Basis: $n = 2$, the prime factorization is $2 = 2^1$.
Inductive step: Assume it is true for all $n > k$.
N2S: It is true for $n = k$. There are 2 cases:

1. If $n = k$ is prime, then the prime factorization is trivial, $k = k \cdot 1$.
2. If $n = k$ is composite, then $\exists m, n \in \mathbb{N}$, s.t. $k = m \cdot n$, and $1 < m, n \leq (k-1)$. By our inductive assumption, m, n both have prime factorizations, so we may write them as $m = 2^{m_2} * 3^{m_3} * 5^{m_5} * ... * p^{m_p}$, and $n = 2^{n_2} * 3^{n_3} * 5^{n_5} * ... * p^{n_p}$. Then k must have a prime factorization, namely $k = 2^{m_2+n_2} * 3^{m_3+n_3} * 5^{m_5+n_5} * ... * p^{m_p+n_p}$.

Therefore, by strong induction, for any $n \in \mathbb{N}$, $n > 1$, there exists a prime factorization of n. QED

15.2.4 Problem 4

Find a solution to the equation $5x + 8y = 1$.
Since this is a Linear Diophantine equation, it can be solved via the reverse Euclidean Algorithm.

$$8 = 5 \cdot 1 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

In reverse:

$$\begin{aligned} 1 &= (1 \cdot 3) + (-1 \cdot 2) \\ &= (-1 \cdot 5) + (2 \cdot 3) \\ &= (2 \cdot 8) + (-3 \cdot 5) \end{aligned}$$

Therefore $x = -3, y = 2$ is a solution to this equation.

15.2.5 Problem 5

Let $f(x) = x^2$. For each pair of sets X and Y below, determine if f defines a function from $X \rightarrow Y$, and if yes, whether this function is injective and/or surjective.

1. $X = \mathbb{N}$, $Y = \mathbb{N}$. Yes, f defines an injective function.

Proof. f is injective because $\forall x_1 \neq x_2 \in \mathbb{N}$, their mapping is $f(x_1) = x_1^2$, and $f(x_2) = x_2^2$. If $f(x_1) = f(x_2)$, then $x_1^2 = x_2^2 \implies (x_1 - x_2)^2 = 0$, and since the natural numbers have no nontrivial zero divisors, x_1 must equal x_2. Since this is true, the contrapositive, (if $f(x_1) \neq f(x_2)$, then $x_1 \neq x_2$) must be true. Therefore f is injective.
f is not surjective because any number $y \in \mathbb{N}$ which is not a perfect square, is not hit. QED

2. $X = \mathbb{Z}$, $Y = \mathbb{Z}$. Yes, f defines a function, however it is neither injective nor surjective.

   Proof. It is not injective because $x_1 = 2, x_2 = -2$ both map to 4. It is not surjective because any negative number, as well as any number that is not a perfect square, is not hit. QED

3. $X = \mathbb{Z}$, $Y = \mathbb{N}$. Yes, f defines a function, however it is neither injective nor surjective.

   Proof. It is not injective because again, both $x_1 = 2, x_2 = -2$ map to 4. It is not surjective because any number that is not a perfect square is not hit. QED

4. $X = \mathbb{N}$, $Y = \mathbb{Z}$. Yes, f defines an injective function.

   Proof. Similarly to the first part, f is injective because $\forall x_1 \neq x_2 \in \mathbb{N}$, their mapping is $f(x_1) = x_1^2$, and $f(x_2) = x_2^2$. If $f(x_1) = f(x_2)$, then, by the first part of this problem, $x_1 = x_2$. Therefore the contrapositive is true, so f is an injection.
   f is not surjective because any negative integer, or integer that is not a perfect square, is not hit. QED

5. $X = \{0, 1\}$, $Y = \{0, 1\}$. Yes, f defines a bijective function.

   Proof. f is injective because we can check all $x \in X$, to see if we get different values of $y \in Y$. $f(0) = 0^2 = 0 \in Y$, and $f(1) = 1^2 = 1 \in Y$. We also just checked that every $y \in Y$ has a unique $x \in X$, so the function is both injective and surjective. QED

15.3 Exam 3

15.3.1 Problem 1

Give an example of a relation that is reflexive and transitive, but not symmetric.

Proof. Consider the set $X = \{1, 2, 3\}$ and the relation $R = \{(1, 1), (2, 2), (3, 3)$ $(1, 2), (2, 3), (1, 3)\}$. This is reflexive because all of $(1, 1), (2, 2), (3, 3)$ are in the relation. It is transitive because $1R2, 2R3 \implies 1R3$ is true. However it is not symmetric because $(1, 3)$ is in the relation, but $(3, 1)$ is not. In other words, you can start at 1 and get to 3, but you can't start at 3 and get to 1. QED

15.3.2 Problem 2

Fix $n \in \mathbb{N}$, prove that if $a \equiv b \mod n$, and $c \equiv d \mod n$, then $ac \equiv bd \mod n$.

Proof. By definition, if $a \equiv b \mod n$, then

$$b = a + nk$$

, for some $k \in \mathbb{Z}$ and similarly,

$$d = c + nl$$

for some $l \in \mathbb{Z}$.
N2S: $bd = ac + nq$, since this shows $bd \equiv ac \mod n$. So

$$bd = (a + nk)(c + nl) = ac + anl + cnk + n^2kl$$

Thus,

$$bd = ac + n(al + ck + nkl)$$

Let $q = (al + ck + nkl)$. This shows that $bd = ac + nq$, for some $q \in \mathbb{Z}$, therefore $bd \equiv ac \mod n$. QED

15.3.3 Problem 3

Determine if $x \mod n$ is invertible, and if yes, find its inverse for the following pairs:

1. $x = 15, n = 42$. By problem 10.1, an element $x \mod n$ is invertible iff $\gcd(x, n) = 1$. In this case, $\gcd(15, 42) = 3$, therefore x is a zero divisor, and therefore has no inverse.

2. $x = 22, n = 13$. $x \equiv 9 \mod 13$, and by the same argument, $\gcd(9, 13) = 1$, so x has an inverse, $x' = 3$, since $9 \cdot 3 = 27 \equiv 1 \mod 13$.

15.3.4 Problem 4

Let $n \in \mathbb{N}$ and $y \in \mathbb{Z}_n$. Suppose that the left multiplication map $L_y : \mathbb{Z}_n \to \mathbb{Z}_n$ is bijective. Prove that y is invertible.

Proof. N2S: $\exists y' \in \mathbb{Z}_n$ such that $y'y \equiv 1 \mod n$.
If the left multiplication map $L_y : \mathbb{Z}_n \to \mathbb{Z}_n$ is bijective, then it is injective and surjective. By the definition of surjectivity, this means every number $x \in \{1, 2, ..., n-1\}$ is mapped to. This means there must be some mapping L_y from y to 1, and therefore y has an inverse (is invertible). QED

15.3.5 Problem 5

Find $1120^{1012} \mod 11$.
Note $1120 \equiv 9 \mod 11$, and by FlT, since 11 is prime, $a^{10} \equiv 1 \mod 11$.

$$9^{1012} = 9^{10 \cdot 101 + 2} = (9^{10})^{42}(9^2) = 1 \cdot 9^2 = 81 \equiv 4 \mod 11$$