Math 220 Fall 2021, Lecture 18: Number theory I

1. Mathematical induction (cont'd)

1.1. Binomial coefficients (cont'd)

Recall:

$$\binom{n}{k} := \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} \qquad \text{for all } n \in \mathbb{R} \text{ and } k \in \mathbb{N}.$$

Also, $\binom{n}{k} := 0$ whenever $k \notin \mathbb{N}$.

The binomial coefficients $\binom{n}{k}$ with $n, k \in \mathbb{N}$ form what is known as **Pascal's triangle**:

$$\begin{array}{rc|ccccccccccccccccc}
 & & &&&&&&&&& \overset{k=0}{\swarrow} \\
n=0 & \rightarrow & &&&&&&&& 1 && \overset{k=1}{\swarrow} \\
n=1 & \rightarrow & &&&&&&& 1 && 1 && \overset{k=2}{\swarrow} \\
n=2 & \rightarrow & &&&&&& 1 && 2 && 1 && \overset{k=3}{\swarrow} \\
n=3 & \rightarrow & &&&&& 1 && 3 && 3 && 1 && \overset{k=4}{\swarrow} \\
n=4 & \rightarrow & &&&& 1 && 4 && 6 && 4 && 1 && \overset{k=5}{\swarrow} \\
n=5 & \rightarrow & &&& 1 && 5 && 10 && 10 && 5 && 1 && \overset{k=6}{\swarrow} \\
n=6 & \rightarrow & && 1 && 6 && 15 && 20 && 15 && 6 && 1 && \overset{k=7}{\swarrow} \\
n=7 & \rightarrow & & 1 && 7 && 21 && 35 && 35 && 21 && 7 && 1 \\
n=8 & \rightarrow & 1 && 8 && 28 && 56 && 70 && 56 && 28 && 8 && 1
\end{array}$$

However, this triangle only covers the nonnegative integers n. What about negative n ? Let us add them to the table too:

											k=0 ↙		k=1 ↙		k=2 ↙		k=3 ↙
$n = -3$ →										1		-3		6		-10	
$n = -2$ →									1		-2		3		-4		
$n = -1$ →								1		-1		1		-1		1	
$n = 0$ →							1		0		0		0		0		
$n = 1$ →						1		1		0		0		0		0	
$n = 2$ →					1		2		1		0		0		0		
$n = 3$ →				1		3		3		1		0		0		0	
$n = 4$ →			1		4		6		4		1		0		0		
$n = 5$ →		1		5		10		10		5		1		0		0	
$n = 6$ →	1		6		15		20		15		6		1		0		

The $n = -1$ row consists of 1s and -1s (alternating between each other); this is simply saying that

$$\binom{-1}{k} = (-1)^k \qquad \text{for all } k \in \mathbb{N}$$

(which we have already checked). As for the $n = -2$ row, its entries are $1, -2, 3, -4, \ldots$, because

$$\begin{aligned} \binom{-2}{k} &= \frac{(-2)(-3)\cdots(-k-1)}{k!} = (-1)^k \cdot \frac{2 \cdot 3 \cdot \cdots \cdot (k+1)}{k!} \\ &= (-1)^k (k+1) \qquad \text{for all } k \in \mathbb{N}. \end{aligned}$$

But a closer look at the $n = -3$ row reveals a much more general pattern: The "negative part" of Pascal's triangle (i.e., the entries $\binom{n}{k}$ with negative n) is a rotated copy of the "nonnegative part" (i.e., the $\binom{n}{k}$ with $n \geq 0$) with some minus signs thrown in! To be precise, we have the following:

Theorem 1.1.1 (upper negation formula)**.** For any numbers n and $k \in \mathbb{Z}$, we have

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}.$$

Proof. If $k \notin \mathbb{N}$, then this is clear because both binomial coefficients are 0 by definition.

So we only need to prove the theorem in the case when $k \in \mathbb{N}$.

In this case, we have

$$\begin{aligned}\binom{-n}{k} &= \frac{(-n)(-n-1)(-n-2)\cdots(-n-k+1)}{k!} \\ &= (-1)^k \cdot \frac{n(n+1)(n+2)\cdots(n+k-1)}{k!} \qquad \text{and} \\ \binom{n+k-1}{k} &= \frac{(n+k-1)(n+k-2)(n+k-3)\cdots n}{k!} \\ &= \frac{n(n+1)(n+2)\cdots(n+k-1)}{k!}.\end{aligned}$$

Comparing these equalities, we find $\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}$. This proves the upper negation formula. □

Corollary 1.1.2. We have $\binom{n}{k} \in \mathbb{Z}$ when $n, k \in \mathbb{Z}$.

Proof. If $n \geq 0$, then this has already been proved last time.

If $k < 0$, then this is clear because $\binom{n}{k} = 0$.

In the remaining case, use the upper negation formula. Details are LTTR. □

For us, probably the most important property of binomial coefficients is the following:

Theorem 1.1.3 (binomial formula, aka binomial theorem)**.** Let a and b be any numbers, and let $n \in \mathbb{N}$. Then,

$$\begin{aligned}(a+b)^n &= a^n + na^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + nab^{n-1} + b^n \\ &= \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}a^1 b^{n-1} + \binom{n}{n}a^0 b^n \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}.\end{aligned}$$

Proof. We shall prove the formula in its last version:

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}. \tag{1}$$

We shall prove this by induction on n:

Base case: For $n = 0$, the equality (1) is true, since

$$(a+b)^0 = 1 \qquad \text{and} \qquad \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^{0-0} = 1 \cdot 1 \cdot 1 = 1.$$

Induction step: Let $n \in \mathbb{N}$. Assume that (1) holds for n. We must show that (1) holds for $n+1$ instead of n.

In other words, we assume (as the IH) that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

We must show that

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

Indeed, we have

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n \cdot (a+b) = \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) \cdot (a+b) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) \cdot a + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) \cdot b \\
&= \sum_{k=0}^{n} \binom{n}{k} \underbrace{a^k b^{n-k} a}_{=a^{k+1} b^{n-k}} + \sum_{k=0}^{n} \binom{n}{k} a^k \underbrace{b^{n-k} b}_{=b^{n-k+1}} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}.
\end{aligned}$$

On the other hand, we know that for each k, we have

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

(Indeed, this is simply the formula $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ that we proved last time – Pascal's identity –, except that we apply it to $n+1$ instead of n.) Hence,

$$\begin{aligned}
&\sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k} \\
&= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} \qquad \left(\text{since } \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \right) \\
&= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} a^k b^{n+1-k} + \binom{n}{k} a^k b^{n+1-k} \right) \\
&= \sum_{k=0}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k}
\end{aligned}$$

$$\left(\begin{array}{c} \text{here, we are using the following rule for summations:} \\ \sum\limits_{k=u}^{v} (c_k + d_k) = \sum\limits_{k=u}^{v} c_k + \sum\limits_{k=u}^{v} d_k \text{ for any } u \text{ and } v \text{ and } c_k \text{ and } d_k \\ \text{(for example, this is saying that} \\ (c_0+d_0)+(c_1+d_1)+(c_2+d_2) = (c_0+c_1+c_2)+(d_0+d_1+d_2)\,) \end{array} \right)$$

$$\begin{aligned}
&= \left(\sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \underbrace{\binom{n}{0-1}}_{=\binom{n}{-1}=0} a^0 b^{n+1-0} \right) \\
&\qquad + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} + \underbrace{\binom{n}{n+1}}_{\substack{=0 \\ \text{(since } n+1>n)}} a^{n+1} b^{n+1-(n+1)} \right) \\
&= \left(\sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \underbrace{0a^0 b^{n+1-0}}_{=0} \right) + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} + \underbrace{0a^{n+1} b^{n+1-(n+1)}}_{=0} \right) \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}.
\end{aligned}$$

Let us compare this with

$$(a+b)^{n+1} = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}.$$

Our goal is to prove that the left hand sides of these two equalities are equal. Clearly, it suffices to prove that the right hand sides are equal. So we want to show that

$$\sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}$$
$$= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}.$$

It is clear that the second sum in this equality equals the fourth sum (since $n+1-k = n-k+1$ for each k). It remains to show that the first sum equals the third sum. In other words, it remains to show that

$$\sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k}.$$

But this is easy: These are one and the same sum, written differently. Indeed, this is similar to

$$\underbrace{\sum_{k=1}^{n} (k-1)^2}_{=0^2+1^2+\cdots+(n-1)^2} = \underbrace{\sum_{k=0}^{n-1} k^2}_{=0^2+1^2+\cdots+(n-1)^2} \qquad \text{and} \qquad \int_u^v f(t)\,dt = \int_{u-1}^{v-1} f(t+1)\,dt.$$

We say that the sum $\sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k}$ is obtained by **substituting** $k-1$ **for** k in the sum $\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k}$. The two sums have the exact same addends; they are just indexed differently. So they are equal. So we conclude that

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

This completes the induction step, and thus the binomial formula is proved. □

(For example, for $n=3$, we have obtained

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

from

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

by multiplying both sides by $a+b$ and expanding the right hand side.)

Here are two corollaries from the binomial formula:

Corollary 1.1.4. Let $n \in \mathbb{N}$. We have

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Proof. Apply the binomial formula to $a = 1$ and $b = 1$. This results in

$$(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \underbrace{1^k 1^{n-k}}_{=1} = \sum_{k=0}^{n} \binom{n}{k}.$$

However, $1 + 1 = 2$. So we get the claim. □

Corollary 1.1.5. Let $n \in \mathbb{N}$. We have

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \begin{cases} 0, & \text{if } n > 0; \\ 1, & \text{if } n = 0. \end{cases}$$

(This was an exercise on homework set #3.)

Proof. Apply the binomial formula to $a = -1$ and $b = 1$. This results in

$$(-1+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \underbrace{1^{n-k}}_{=1} = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

However, $(-1+1)^n = 0^n$ is 0 whenever $n > 0$, but is 1 when $n = 0$. □

For more about binomial coefficients, see any course on enumerative combinatorics (e.g., Math 222).

2. Number theory I

2.1. Divisibility

2.1.1. Definition

Definition 2.1.1. Let a and b be two integers.

We say that $a \mid b$ (or "a **divides** b", or "b is **divisible by** a", or "b is a **multiple** of a", or "a is a **divisor** of b") if there exists an integer c such that $b = ac$.

We furthermore write $a \nmid b$ if a does not divide b.

Example 2.1.2. **(a)** We have $4 \mid 12$, since there exists an integer c such that $12 = 4 \cdot c$ (namely, $c = 3$).

(b) We have $4 \nmid 11$, since there exists no integer c such that $11 = 4 \cdot c$.

(c) We have $1 \mid b$ for every integer b (since $b = 1 \cdot b$).

(d) We have $a \mid a$ for every integer a (since $a = a \cdot 1$). In particular, $0 \mid 0$. This is slightly controversial.

(e) We have $0 \mid b$ if and only if $b = 0$.

Definition 2.1.3. **(a)** An integer n is said to be **even** if $2 \mid n$.

(b) An integer n is said to be **odd** if $2 \nmid n$.

2.1.2. Basic properties

Here are some fundamental properties of divisibility:

Proposition 2.1.4. Let a and b be two integers.

(a) We have $a \mid b$ if and only if $|a| \mid |b|$ (this means "$|a|$ divides $|b|$").

(b) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

(c) If $a \mid b$ and $b \mid a$, then $|a| = |b|$.

(d) Assume that $a \neq 0$. Then, $a \mid b$ if and only if $\dfrac{b}{a} \in \mathbb{Z}$.

Proof. **(a)** This is an "if and only if" statement. In other words, we must prove the two implications

$$(a \mid b) \Longrightarrow (|a| \mid |b|) \qquad \text{and} \qquad (|a| \mid |b|) \Longrightarrow (a \mid b)\,.$$

Proof of $(a \mid b) \Longrightarrow (|a| \mid |b|)$*:* We assume that $a \mid b$. We must prove that $|a| \mid |b|$.

By the definition of divisibility, $a \mid b$ means that there exists some integer c such that $b = ac$. Consider this c. Now, $|b| = \pm b$ (this is shorthand for "$|b|$ is either b or $-b$"), so

$$|b| = \pm \underbrace{b}_{=ac} = \pm ac.$$

However, $a = \pm |a|$ (since $|a| = \pm a$). Note that the two $\pm$ signs can be different. In either case, we get

$$|b| = \pm \underbrace{a}_{=\pm|a|} c = \pm (\pm |a|)\, c = \pm |a|\, c = |a| \cdot \underbrace{(\pm c)}_{\text{an integer}}\,.$$

Thus, $|a| \mid |b|$. This proves the implication.

Proof of $(|a| \mid |b|) \Longrightarrow (a \mid b)$*:* Analogous.

So part **(a)** is proved.

(b) Assume that $a \mid b$ and $b \neq 0$. We must prove $|a| \leq |b|$.

By the definition of divisibility, $a \mid b$ means that there exists some integer c such that $b = ac$. Consider this c. Now, $|b| = |ac| = |a| \cdot |c|$ (since it is well-known and easy to check that $|xy| = |x| \cdot |y|$ for any two real numbers x and y). However, $c \neq 0$ (because if we had $c = 0$, then we would have $b = a \underbrace{c}_{=0} = a \cdot 0 = 0$, which would contradict $b \neq 0$). Thus, $c \geq 1$ or $c \leq -1$ (because c is an integer). Hence, $|c| \geq 1$. Now,

$$\begin{aligned} |b| &= |a| \cdot \underbrace{|c|}_{\geq 1} \geq |a| \cdot 1 \qquad \text{(since } |a| \geq 0\text{)} \\ &= |a|, \end{aligned}$$

so that $|a| \leq |b|$. This proves part **(b)**.

(c) Assume that $a \mid b$ and $b \mid a$. We must prove that $|a| = |b|$.

If $a = 0$, then $a \mid b$ implies $b = 0$, so we are done.

If $b = 0$, then $b \mid a$ implies $a = 0$, so we are done.

Thus, we are done if any of a and b is 0.

Hence, we can now assume that $a \neq 0$ and $b \neq 0$.

From $a \mid b$ and $b \neq 0$, we conclude that $|a| \leq |b|$ (by part **(b)**).

From $b \mid a$ and $a \neq 0$, we conclude that $|b| \leq |a|$ (by part **(b)**, but applied to b and a instead of a and b).

Combining the two inequalities $|a| \leq |b|$ and $|b| \leq |a|$, we obtain $|a| = |b|$. This proves part **(c)**.

(d) We must prove that $a \mid b$ if and only if $\frac{b}{a} \in \mathbb{Z}$. In other words, we must prove the two implications

$$(a \mid b) \Longrightarrow \left(\frac{b}{a} \in \mathbb{Z}\right) \qquad \text{and} \qquad \left(\frac{b}{a} \in \mathbb{Z}\right) \Longrightarrow (a \mid b).$$

Both are easy: If $a \mid b$, then $b = ac$ for some integer c, and thus this c must be $\frac{b}{a}$, and therefore $\frac{b}{a} = c \in \mathbb{Z}$. Conversely, if $\frac{b}{a} \in \mathbb{Z}$, then $b = ac$ for the integer $c = \frac{b}{a}$, so we get $a \mid b$. Thus, part **(d)** is proved. □

> **Theorem 2.1.5** (rules for divisibilities)**.** **(a)** We have $a \mid a$ for every $a \in \mathbb{Z}$. (This is called **reflexivity of divisibility**.)
>
> **(b)** If $a, b, c \in \mathbb{Z}$ satisfy $a \mid b$ and $b \mid c$, then $a \mid c$. (This is called **transitivity of divisibility**.)
>
> **(c)** If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$, then $a_1a_2 \mid b_1b_2$.
>
> **(d)** If $d, a, b \in \mathbb{Z}$ satisfy $d \mid a$ and $d \mid b$, then $d \mid a + b$.

Proof. **(a)** Let $a \in \mathbb{Z}$. Then, $a = a \cdot 1$, so that $a \mid a$ (since 1 is an integer). This proves part **(a)**.

(b) Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid b$ and $b \mid c$. We must prove that $a \mid c$.

We have $a \mid b$. By the definition of divisibility, this yields that there exists some integer x such that $b = ax$. Consider this x.

We have $b \mid c$. By the definition of divisibility, this yields that there exists some integer y such that $c = by$. Consider this y.

Now,

$$c = \underbrace{b}_{=ax} y = axy.$$

Thus, there exists some integer z such that $c = az$ (namely, $z = xy$). In other words, $a \mid c$. Thus, part **(b)** is proved.

(c) Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$. We must prove that $a_1 a_2 \mid b_1 b_2$.

We have $a_1 \mid b_1$. In other words, there exists some integer c_1 such that $b_1 = a_1 c_1$. Consider this c_1.

We have $a_2 \mid b_2$. In other words, there exists some integer c_2 such that $b_2 = a_2 c_2$. Consider this c_2.

Now, multiplying the two equalities $b_1 = a_1 c_1$ and $b_2 = a_2 c_2$, we obtain

$$b_1 b_2 = a_1 c_1 \cdot a_2 c_2 = (a_1 a_2) \underbrace{(c_1 c_2)}_{\text{an integer}}.$$

Therefore, $a_1 a_2 \mid b_1 b_2$. Hence, part **(c)** is proved.

(d) Let $d, a, b \in \mathbb{Z}$ satisfy $d \mid a$ and $d \mid b$. We must prove that $d \mid a + b$.

We have $d \mid a$. In other words, there exists some integer x such that $a = dx$. Consider this x.

We have $d \mid b$. In other words, there exists some integer y such that $b = dy$. Consider this y.

Adding the two equalities $a = dx$ and $b = dy$ together, we find $a + b = dx + dy = d \underbrace{(x + y)}_{\text{an integer}}$. Thus, $d \mid a + b$. This proves part **(d)**. □

Part **(b)** of the above theorem tells us that divisibilities can be chained together: If $a \mid b$ and $b \mid c$, then $a \mid c$. You will often see "$a \mid b$ and $b \mid c$" rewritten shortly as "$a \mid b \mid c$". More generally, the statement

$$\text{"}a_1 \mid a_2 \mid \cdots \mid a_k\text{"}$$

means that $a_1 \mid a_2$ and $a_2 \mid a_3$ and so on and $a_{k-1} \mid a_k$. By induction on k, you can easily see that such a chain of divisibilities automatically yields $a_1 \mid a_k$.

How can you spot divisibilities in real life? For small values of a, there are several known **divisibility criteria**, which give simple ways to check whether an integer b is divisible by a (without computing $\frac{b}{a}$). Here are some:

Theorem 2.1.6. Let $b \in \mathbb{N}$. Write b in decimal.

(a) We have $2 \mid b$ if and only if the last digit of b is 0, 2, 4, 6 or 8.

(b) We have $5 \mid b$ if and only if the last digit of b is 0 or 5.

(c) We have $10 \mid b$ if and only if the last digit of b is 0.

(d) We have $3 \mid b$ if and only if the sum of the digits of b is divisible by 3.

(e) We have $9 \mid b$ if and only if the sum of the digits of b is divisible by 9.

> **Example 2.1.7.** Let $b = 10835$. Then, $2 \nmid b$, since the last digit of b is not 0, 2, 4, 6 or 8. However, $5 \mid b$, since the last digit of b is 0 or 5. Do we have $3 \mid b$? The sum of the digits of b is $1 + 0 + 8 + 3 + 5 = 17$, which is not divisible by 3. Thus, b is not divisible by 3.

How do we prove the theorem? The easiest part is part **(c)**: If you multiply a number (written in decimal) by 10, you are just adding a new digit 0 at its end. So, if $10 \mid b$, then the last digit of b is 0. Conversely, if the last digit of b is 0, then $b = 10 \cdot b'$, where b' is b without its last digit. For example, $380 = 10 \cdot 38$.

Part **(a)** is easy to check. Indeed, if $2 \mid b$, then $b = 2c$ for some integer c, and therefore the last digit of b is 2 times the last digit of c, possibly minus 10 (because of the classical method for multiplying numbers). It is easy to check that the only options for this are 0, 2, 4, 6 and 8. The converse is also easy to check: If the last digit of b is 6 (for example), then $b = 10c + 6$ for some $c \in \mathbb{Z}$, and thus $b = 10c + 6 = 2\underbrace{(5c+3)}_{\text{an integer}}$, so $2 \mid b$.

Similarly, part **(b)** can be shown.

What about **(d)** and **(e)**? We will see this soon.