University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Homework 1

Darij Grinberg

May 15, 2019

1 Exercise 1: Mutual divisibility is rare

1.1 Problem

Let a and b be two integers such that $a \mid b$ and $b \mid a$. Prove that $|a| = |b|$.

1.2 Solution

See the class notes, where this is Exercise 2.2.2. (The numbering may shift; it is one of the exercises in the "Divisibility" section.)

---

2 Exercise 2: Congruence means equal remainders

2.1 Problem

Let n be a positive integer. Let u and v be two integers. Prove that $u \equiv v \mod n$ if and only if $u\%n = v\%n$.

2.2 Solution

See the class notes, where this is Exercise 2.6.1. (The numbering may shift; it is one of the exercises in the "Division with remainder" section.)

---

3 Exercise 3: Even and odd

3.1 Problem

Let u be an integer.

(a) Prove that u is even if and only if $u\%2 = 0$.

(b) Prove that u is odd if and only if $u\%2 = 1$.

(c) Prove that u is even if and only if $u \equiv 0 \mod 2$.

(d) Prove that u is odd if and only if $u \equiv 1 \mod 2$.

(e) Prove that u is odd if and only if $u + 1$ is even.

(f) Prove that exactly one of the two numbers u and $u + 1$ is even.

(g) Prove that $u(u + 1) \equiv 0 \mod 2$.

(h) Prove that $u^2 \equiv -u \equiv u \mod 2$.

3.2 Solution

See the class notes, where this is Exercise 2.7.1 parts **(a)** to **(h)**. (The numbering may shift; it is one of the exercises in the "Even and odd numbers" section.)

---

4 Exercise 4: Factorials 102

4.1 Problem

(a) Prove that

$$\frac{1! \cdot 2! \cdot \cdots \cdot (2n)!}{n!} = 2^n \cdot \prod_{i=1}^{n} ((2i-1)!)^2 \qquad \text{for each } n \in \mathbb{N}.$$

(b) Prove that

$$\sum_{k=0}^{n} \frac{1}{k! \cdot (k+2)} = 1 - \frac{1}{(n+2)!} \qquad \text{for each } n \in \mathbb{N}.$$

4.2 Solution

We first recall that

$$n! = n \cdot (n-1)! \qquad \text{for each positive integer } n. \tag{1}$$

(This was the claim of Exercise 2 **(a)** on homework set #0.)

(a) This is precisely [Grinbe19, Exercise 3.5 **(c)**], with only a superficial difference (namely, I write "$\left(\prod_{i=1}^{n} ((2i-1)!)\right)^2$" instead of "$\prod_{i=1}^{n} ((2i-1)!)^2$" in [Grinbe19, Exercise 3.5 **(c)**], but these two expressions are clearly equivalent). I give two solutions in [Grinbe19, solution to Exercise 3.5 **(c)**]: one by manipulation and one by induction. Here I will only show the solution by manipulation:

Let $n \in \mathbb{N}$. Then, we can group the factors of the product $1! \cdot 2! \cdot \cdots \cdot (2n)!$ into pairs of successive factors. We thus obtain[1]

$$\begin{aligned}
&1! \cdot 2! \cdot \cdots \cdot (2n)! \\
&= (1! \cdot 2!) \cdot (3! \cdot 4!) \cdot \cdots \cdot ((2n-1)! \cdot (2n)!) = \prod_{i=1}^{n} \left((2i-1)! \cdot \underbrace{(2i)!}_{\substack{=(2i)\cdot(2i-1)! \\ (\text{by (1)})}} \right) \\
&= \prod_{i=1}^{n} \underbrace{((2i-1)! \cdot (2i) \cdot (2i-1)!)}_{=(2i)\cdot((2i-1)!)^2} = \prod_{i=1}^{n} \left((2i) \cdot ((2i-1)!)^2\right) \\
&= \underbrace{\left(\prod_{i=1}^{n} (2i)\right)}_{=2^n \prod_{i=1}^{n} i} \cdot \prod_{i=1}^{n} ((2i-1)!)^2 = 2^n \underbrace{\left(\prod_{i=1}^{n} i\right)}_{=1\cdot 2\cdot\cdots\cdot n = n!} \cdot \prod_{i=1}^{n} ((2i-1)!)^2 = 2^n n! \cdot \prod_{i=1}^{n} ((2i-1)!)^2 .
\end{aligned}$$

Dividing both sides of this equality by $n!$, we find

$$\frac{1! \cdot 2! \cdot \cdots \cdot (2n)!}{n!} = 2^n \cdot \prod_{i=1}^{n} ((2i-1)!)^2 .$$

This solves part **(a)** of the exercise.

(b) Again, the exercise can be proven by induction or by the telescope principle. Let me show the latter solution. First, I quote the telescope principle:

Proposition 4.1. *Let $m \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_m$ be $m+1$ real numbers. Then,*

$$\sum_{i=1}^{m} (a_i - a_{i-1}) = a_m - a_0.$$

Now, let me solve the exercise. Let $n \in \mathbb{N}$. For each $i \in \{0, 1, \ldots, n\}$, we set $a_i = \dfrac{-1}{(i+2)!}$. Thus, $a_0, a_1, \ldots, a_n$ are $n+1$ real numbers. We state the following:

[1] Strictly speaking, we are tacitly using the fact that each integer between 1 and $2n$ (inclusive) can be written either in the form $2i$ or in the form $2i-1$ for some $i \in \{1, 2, \ldots, n\}$, and that this i is unique. The proof of this fact relies on division with remainder.

Claim 1: For each $i \in \{0, 1, \ldots, n\}$, we have

$$a_i - a_{i-1} = \frac{1}{i! \cdot (i+2)}.$$

[*Proof of Claim 1:* Let $i \in \{0, 1, \ldots, n\}$. Then, (1) (applied to $i+1$ instead of n) yields $(i+1)! = (i+1) \cdot i!$. Also, (1) (applied to $i+2$ instead of n) yields $(i+2)! = (i+2) \cdot (i+1)!$.

The definition of a_i yields

$$a_i = \frac{-1}{(i+2)!} = \frac{-1}{(i+2) \cdot (i+1)!} \qquad (\text{since } (i+2)! = (i+2) \cdot (i+1)!) .$$

The definition of a_{i-1} yields

$$a_{i-1} = \frac{-1}{((i-1)+2)!} = \frac{-1}{(i+1)!} \qquad (\text{since } (i-1)+2 = i+1) .$$

Subtracting this equality from the previous one, we obtain

$$\begin{aligned} a_i - a_{i-1} &= \frac{-1}{(i+2) \cdot (i+1)!} - \frac{-1}{(i+1)!} = \frac{1}{(i+1)!} - \frac{1}{(i+2) \cdot (i+1)!} = \frac{(i+2)-1}{(i+2) \cdot (i+1)!} \\ &= \frac{i+1}{(i+2) \cdot (i+1)!} = \frac{i+1}{(i+2) \cdot (i+1) \cdot i!} \qquad (\text{since } (i+1)! = (i+1) \cdot i!) \\ &= \frac{1}{(i+2) \cdot i!} = \frac{1}{i! \cdot (i+2)}. \end{aligned}$$

This proves Claim 1.]

Now, Proposition 4.1 (applied to $m = n$) yields

$$\begin{aligned} \sum_{i=1}^{n} (a_i - a_{i-1}) &= \underbrace{a_n}_{\substack{= \frac{-1}{(n+2)!} \\ \text{(by the definition of } a_n)}} - \underbrace{a_0}_{\substack{= \frac{-1}{(0+2)!} \\ \text{(by the definition of } a_0)}} \\ &= \frac{-1}{(n+2)!} - \frac{-1}{(0+2)!} = \underbrace{\frac{1}{(0+2)!}}_{= \frac{1}{2!} = \frac{1}{2}} - \frac{1}{(n+2)!} = \frac{1}{2} - \frac{1}{(n+2)!}. \end{aligned}$$

Comparing this with

$$\sum_{i=1}^{n} \underbrace{(a_i - a_{i-1})}_{\substack{= \frac{1}{i! \cdot (i+2)} \\ \text{(by Claim 1)}}} = \sum_{i=1}^{n} \frac{1}{i! \cdot (i+2)},$$

we obtain

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

But

$$\sum_{k=0}^{n} \frac{1}{k! \cdot (k+2)} = \sum_{i=0}^{n} \frac{1}{i! \cdot (i+2)} \qquad \text{(here, we have renamed the summation index } k \text{ as } i\text{)}$$
$$= \underbrace{\frac{1}{0! \cdot (0+2)}}_{= \frac{1}{1 \cdot 2} = \frac{1}{2}} + \underbrace{\sum_{i=1}^{n} \frac{1}{i! \cdot (i+2)}}_{\substack{= \frac{1}{2} - \frac{1}{(n+2)!} \\ \text{(by (2))}}} = \underbrace{\frac{1}{2} + \frac{1}{2}}_{=1} - \frac{1}{(n+2)!} = 1 - \frac{1}{(n+2)!}.$$

This solves part **(b)** of the exercise.

---

5 Exercise 5: Binomial coefficients 102

5.1 Problem

Prove that

$$\frac{(ab)!}{a! \, (b!)^a} = \prod_{k=1}^{a} \binom{kb-1}{b-1}$$

for all $a \in \mathbb{N}$ and all positive integers b.

5.2 Solution

First, let us state an analogue of the telescope principle (Proposition 4.1) for products instead of sums:

Proposition 5.1. *Let $m \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_m$ be $m+1$ nonzero real numbers. Then,*

$$\prod_{i=1}^{m} \frac{a_i}{a_{i-1}} = \frac{a_m}{a_0}.$$

Proof of Proposition 5.1. Take your favorite proof of Proposition 4.1, and replace addition by multiplication, subtraction by division and sums by products. This will yield a proof of Proposition 5.1. □

Furthermore, recall the following facts:

Proposition 5.2. *If $n \in \mathbb{N}$ and $k \in \mathbb{N}$ are such that $n \geq k$, then*

$$\binom{n}{k} = \frac{n!}{k! \, (n-k)!}.$$

Proposition 5.2 is Exercise 3 **(a)** on homework set #0.

Proposition 5.3. *Any $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$ satisfy*

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

Proposition 5.3 is Exercise 3 **(f)** on homework set #0.

Now, let $a \in \mathbb{N}$, and let b be a positive integer. Thus, $b \neq 0$ (since b is positive).

Claim 1: We have

$$\binom{kb-1}{b-1} = \frac{1}{k} \cdot \frac{1}{b!} \cdot \frac{(kb)!}{((k-1)\,b)!}$$

for each positive integer k.

[*Proof of Claim 1:* Let k be a positive integer. Then, Proposition 5.3 (applied to kb and b instead of n and k) yields

$$b\binom{kb}{b} = kb\binom{kb-1}{k-1}.$$

We can cancel b from this equality (since b is nonzero), and thus obtain

$$\binom{kb}{b} = k\binom{kb-1}{k-1}.$$

On the other hand, $k \geq 1$ (since k is a positive integer). We can multiply this inequality by b (since b is positive) and thus obtain $kb \geq 1b = b$. Hence, Proposition 5.2 (applied to kb and b instead of n and k) yields $\binom{kb}{b} = \frac{(kb)!}{b!\,(kb-b)!} = \frac{(kb)!}{b!\,((k-1)\,b)!}$ (since $kb - b = (k-1)\,b$). Comparing this equality with $\binom{kb}{b} = k\binom{kb-1}{k-1}$, we obtain

$$k\binom{kb-1}{k-1} = \frac{(kb)!}{b!\,((k-1)\,b)!}.$$

We can divide both sides of this equality by k (since k is positive and thus nonzero); thus we obtain

$$\binom{kb-1}{b-1} = \frac{1}{k} \cdot \frac{(kb)!}{b!\,((k-1)\,b)!} = \frac{1}{k} \cdot \frac{1}{b!} \cdot \frac{(kb)!}{((k-1)\,b)!}.$$

This proves Claim 1.]

Now,

$$\prod_{k=1}^{a} \underbrace{\dbinom{kb-1}{b-1}}_{\substack{=\frac{1}{k}\cdot\frac{1}{b!}\cdot\frac{(kb)!}{((k-1)b)!} \\ \text{(by Claim 1)}}}$$

$$= \prod_{k=1}^{a} \left(\frac{1}{k} \cdot \frac{1}{b!} \cdot \frac{(kb)!}{((k-1)b)!}\right) = \underbrace{\left(\prod_{k=1}^{a} \frac{1}{k}\right)}_{\substack{=\frac{1}{\prod_{k=1}^{a} k}=\frac{1}{a!} \\ \text{(since } \prod_{k=1}^{a} k=a!)}} \cdot \underbrace{\left(\prod_{k=1}^{a} \frac{1}{b!}\right)}_{=\left(\frac{1}{b!}\right)^a=\frac{1}{(b!)^a}} \cdot \underbrace{\left(\prod_{k=1}^{a} \frac{(kb)!}{((k-1)b)!}\right)}_{\substack{=\prod_{i=1}^{a} \frac{(ib)!}{((i-1)b)!} \\ \text{(here, we have renamed the} \\ \text{index } k \text{ as } i \text{ in the product)}}}$$

$$= \frac{1}{a!} \cdot \frac{1}{(b!)^a} \cdot \underbrace{\prod_{i=1}^{a} \frac{(ib)!}{((i-1)b)!}}_{\substack{=\frac{(ab)!}{(0b)!} \\ \text{(by Proposition 5.1,} \\ \text{applied to } m=a \text{ and } a_i=(ib)!)}} = \frac{1}{a!} \cdot \frac{1}{(b!)^a} \cdot \underbrace{\frac{(ab)!}{(0b)!}}_{\substack{=\frac{(ab)!}{1} \\ \text{(since } (0b)!=0!=1)}}$$

$$= \frac{1}{a!} \cdot \frac{1}{(b!)^a} \cdot \frac{(ab)!}{1} = \frac{1}{a!} \cdot \frac{1}{(b!)^a} \cdot (ab)! = \frac{(ab)!}{a!\,(b!)^a}.$$

This solves the exercise.

5.3 Remark

Proposition 2.17.12 in the class notes says that $\dbinom{n}{k}$ is an integer for all $n \in \mathbb{Z}$ and $k \in \mathbb{Q}$. In other words,

$$\dbinom{n}{k} \in \mathbb{Z} \qquad \text{for all } n \in \mathbb{Z} \text{ and } k \in \mathbb{Q}. \tag{3}$$

Using this fact and the above exercise, we can show the following:

Corollary 5.4. *Let $a \in \mathbb{N}$. Let b be a positive integer. Then, $a!\,(b!)^a \mid (ab)!$.*

Proof of Corollary 5.4. The exercise yields

$$\frac{(ab)!}{a!\,(b!)^a} = \prod_{k=1}^{a} \underbrace{\dbinom{kb-1}{b-1}}_{\substack{\in\mathbb{Z} \\ \text{(by (3), applied to } kb-1 \text{ and } b-1 \\ \text{instead of } n \text{ and } k)}} \in \mathbb{Z}.$$

In other words, $a!\,(b!)^a \mid (ab)!$. This proves Corollary 5.4. □

We refer to [GrKnPa94, Chapter 5] for further properties of binomial coefficients.

---

6 Exercise 6: Binomial coefficients and coprimality

6.1 Problem

It is well-known (see, e.g., [Grinbe19, Proposition 3.20]) that

$$\binom{n}{k} \in \mathbb{Z} \text{ for all } n \in \mathbb{Z} \text{ and } k \in \mathbb{N}. \tag{4}$$

(This is not at all clear from the definition of $\binom{n}{k}$; it is saying that the product of any k consecutive integers is divisible by $k!$. The case of $k = 2$ is the statement of Exercise 3 **(g)**.) Thus, we can study the divisibility of binomial coefficients by various integers. There are hundreds of theorems about this; this exercise is about one of them.

Let a and b be two coprime positive integers.

(a) Prove that $\dfrac{a}{a+b}\dbinom{a+b}{a} = \dbinom{a+b-1}{a-1}$ and $\dfrac{b}{a+b}\dbinom{a+b}{a} = \dbinom{a+b-1}{b-1}$.

(b) Prove that if $h \in \mathbb{Q}$ satisfies $ah \in \mathbb{Z}$ and $bh \in \mathbb{Z}$, then $h \in \mathbb{Z}$. (This is where the coprimality of a and b comes into play.)

(c) Prove that $a + b \mid \dbinom{a+b}{a}$.

(d) Find a counterexample to the claim of part **(c)** if a and b are allowed to not be coprime.

6.2 Solution

We recall *Bezout's theorem* (proven in the class notes):

Theorem 6.1. *Let a and b be two integers. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that*

$$\gcd(a, b) = xa + yb.$$

Both a and b are positive integers. Hence, the sum $a + b$ is a positive integer as well. Thus, in particular, $a + b$ is nonzero.

(a) We have $a + b \geq a$ (since b is positive and thus nonnegative). Hence, Proposition 5.2 (applied to $n = a + b$ and $k = a$) yields

$$\binom{a+b}{a} = \frac{(a+b)!}{a!\,((a+b)-a)!} = \frac{(a+b)!}{a!b!} \qquad (\text{since } (a+b)-a = b).$$

The same argument (but with the roles of a and b interchanged) yields

$$\binom{b+a}{b} = \frac{(b+a)!}{b!a!} = \frac{(b+a)!}{a!b!} = \frac{(a+b)!}{a!b!} \qquad (\text{since } b+a = a+b).$$

Comparing these two equalities, we obtain

$$\binom{b+a}{b} = \binom{a+b}{a}. \tag{5}$$

Proposition 5.3 (applied to $n = a+b$ and $k = a$) yields $a\dbinom{a+b}{a} = (a+b)\dbinom{a+b-1}{a-1}$. We can divide both sides of this equality by $a+b$ (since $a+b$ is nonzero). We thus obtain

$$\frac{a}{a+b}\dbinom{a+b}{a} = \dbinom{a+b-1}{a-1}. \tag{6}$$

The same argument (but with the roles of a and b interchanged) yields

$$\frac{b}{b+a}\dbinom{b+a}{b} = \dbinom{b+a-1}{b-1}.$$

In view of (5), this rewrites as

$$\frac{b}{b+a}\dbinom{a+b}{a} = \dbinom{b+a-1}{b-1}.$$

In view of $b+a = a+b$, this rewrites as

$$\frac{b}{a+b}\dbinom{a+b}{b} = \dbinom{a+b-1}{b-1}. \tag{7}$$

Having proven both (6) and (7), we have thus solved part **(a)** of the exercise.

(b) Let $h \in \mathbb{Q}$ satisfy $ah \in \mathbb{Z}$ and $bh \in \mathbb{Z}$. We must prove that $h \in \mathbb{Z}$.

Theorem 6.1 shows that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$. Consider these x and y.

But we know that a and b are coprime. In other words, $\gcd(a,b) = 1$. Hence, $1 = \gcd(a,b) = xa + yb$. Multiplying both sides of this equality by h, we find

$$h \cdot 1 = h(xa + yb) = x \cdot (ah) + y \cdot (bh).$$

All four numbers x, ah, y and bh on the right hand side of this equality are integers (since $x \in \mathbb{Z}$, $ah \in \mathbb{Z}$, $y \in \mathbb{Z}$ and $bh \in \mathbb{Z}$). Thus, the right hand side of this equality is an integer. Therefore, so is the left hand side. In other words, $h \cdot 1 \in \mathbb{Z}$. In other words, $h \in \mathbb{Z}$. This solves part **(b)** of the exercise.

(c) Recall that a is a positive integer; hence, $a \in \mathbb{N}$ and $a - 1 \in \mathbb{N}$. Also, $b - 1 \in \mathbb{N}$ (since b is a positive integer). Now, (4) yields $\dbinom{a+b}{a} \in \mathbb{Z}$ (since $a+b \in \mathbb{Z}$ and $a \in \mathbb{N}$) and $\dbinom{a+b-1}{a-1} \in \mathbb{Z}$ (since $a+b-1 \in \mathbb{Z}$ and $a-1 \in \mathbb{N}$) and $\dbinom{a+b-1}{b-1} \in \mathbb{Z}$ (since $a+b-1 \in \mathbb{Z}$ and $b-1 \in \mathbb{N}$).

Define $h \in \mathbb{Q}$ by $h = \dfrac{1}{a+b}\dbinom{a+b}{a}$. (This is well-defined, since $a+b$ is nonzero and $\dbinom{a+b}{a}$ belongs to $\mathbb{Z}$.)

From $h = \dfrac{1}{a+b}\dbinom{a+b}{a}$, we obtain

$$ah = a \cdot \frac{1}{a+b}\dbinom{a+b}{a} = \frac{a}{a+b}\dbinom{a+b}{a} = \dbinom{a+b-1}{a-1} \qquad \text{(by part (a) of this exercise)}$$
$$\in \mathbb{Z}.$$

From $h = \frac{1}{a+b}\binom{a+b}{a}$, we also obtain

$$bh = b \cdot \frac{1}{a+b}\binom{a+b}{a} = \frac{b}{a+b}\binom{a+b}{a} = \binom{a+b-1}{b-1} \qquad \text{(by part **(a)** of this exercise)}$$
$$\in \mathbb{Z}.$$

Thus, part **(b)** of this exercise yields $h \in \mathbb{Z}$. In view of $h = \frac{1}{a+b}\binom{a+b}{a} = \frac{\binom{a+b}{a}}{a+b}$, this rewrites as $\frac{\binom{a+b}{a}}{a+b} \in \mathbb{Z}$. In other words, $a+b \mid \binom{a+b}{a}$ (since $a+b$ is nonzero). This solves part **(c)** of the exercise.

(d) For example, setting $a = 2$ and $b = 2$ yields a counterexample, since $2+2 \nmid \binom{2+2}{2}$. (In fact, $2+2 = 4 \nmid 6 = \binom{4}{2} = \binom{2+2}{2}$.)

References

[GrKnPa94] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics, Second Edition*, Addison-Wesley 1994.
See `https://www-cs-faculty.stanford.edu/~knuth/gkp.html` for errata.

[Grinbe19] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
`http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf`
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see `https://github.com/darijgr/detnotes/releases/tag/2019-01-10` .