4. Math 235 Fall 2021, Worksheet 4: Algebraic tricks

This worksheet is devoted to some ways in which skilled algebraic manipulations (in the sense of high-school algebra: combining terms, expanding products, etc.) can help solve problems.

As before, $\mathbb{N}$ means the set $\{0, 1, 2, \ldots\}$.

4.1. Example problems

We begin with a fairly classical inequality:

Exercise 4.1.1. Let a, b, c be three real numbers. Prove the inequality

$$a^2 + b^2 + c^2 \geq bc + ca + ab.$$

Solution idea. There is a one-paragraph solution:

First solution to Exercise 4.1.1. Recall that $x^2 \geq 0$ for each real number x. Hence, we have $(b-c)^2 \geq 0$ and $(c-a)^2 \geq 0$ and $(a-b)^2 \geq 0$. However, by a straightforward computation, we can verify that

$$\begin{aligned}\left(a^2 + b^2 + c^2\right) - (bc + ca + ab) &= \frac{1}{2}\left(\underbrace{(b-c)^2}_{\geq 0} + \underbrace{(c-a)^2}_{\geq 0} + \underbrace{(a-b)^2}_{\geq 0}\right) \\ &\geq \frac{1}{2}(0 + 0 + 0) = 0.\end{aligned}$$

Thus, $a^2 + b^2 + c^2 \geq bc + ca + ab$, so that the exercise is solved. □

Clearly, the trick in this solution was to rewrite $\left(a^2 + b^2 + c^2\right) - (bc + ca + ab)$ as $\frac{1}{2}\left((b-c)^2 + (c-a)^2 + (a-b)^2\right)$. This can indeed be verified by a straightforward computation (just expand both sides), but how could this be discovered? Confronted with the expression $\left(a^2 + b^2 + c^2\right) - (bc + ca + ab)$, how would you know to rewrite it as $\frac{1}{2}\left((b-c)^2 + (c-a)^2 + (a-b)^2\right)$?

There are several other solutions that are easier to find:

Second solution to Exercise 4.1.1. The numbers a, b, c play symmetric roles in the exercise. Thus, we can permute them without changing the claim of the exercise. (For instance, we can swap a with b, or cyclically rotate a, b, c.) By an appropriate such permutation, we can achieve a situation in which c is the largest of the three numbers a, b, c. So let us WLOG assume that we are in this situation. Then, $c \geq a$ and

$c \geq b$, so that $c - a \geq 0$ and $c - b \geq 0$ and therefore $(c-a)(c-b) \geq 0$. (By the way, the same conclusion could be obtained if c was the smallest of a, b, c.) However,

$$\begin{aligned}
\left(a^2+b^2+c^2\right) - (bc+ca+ab) &= \underbrace{a^2+b^2-ab}_{=(a-b)^2+ab} + c^2 - bc - ca \\
&= (a-b)^2 + \underbrace{ab + c^2 - bc - ca}_{=(c-a)(c-b)} \\
&= \underbrace{(a-b)^2}_{\geq 0} + \underbrace{(c-a)(c-b)}_{\geq 0} \geq 0 + 0 = 0.
\end{aligned}$$

That is, $a^2 + b^2 + c^2 \geq bc + ca + ab$. Exercise 4.1.1 is solved again. □

Third solution to Exercise 4.1.1. The expression $\left(a^2+b^2+c^2\right) - (bc+ca+ab)$ (viewed as a polynomial in any of a, b, c) is quadratic, so we use the time-tested method of "completing the square" (the same method used, e.g., to rewrite $a^2 + 7a + 2$ as $\left(a + \frac{7}{2}\right)^2 - \frac{41}{4}$). We treat a as the variable and b and c as constants. We obtain

$$\begin{aligned}
\left(a^2+b^2+c^2\right) - (bc+ca+ab) &= \left(a - \frac{b+c}{2}\right)^2 + \frac{3}{4} \underbrace{\left(b^2 - 2bc + c^2\right)}_{=(b-c)^2} \\
&= \underbrace{\left(a - \frac{b+c}{2}\right)^2}_{\geq 0} + \frac{3}{4} \underbrace{(b-c)^2}_{\geq 0} \geq 0 + \frac{3}{4} 0 = 0.
\end{aligned}$$

In other words, $a^2 + b^2 + c^2 \geq bc + ca + ab$. Exercise 4.1.1 is solved again. □

There are many other solutions. The first solution is arguably the most elegant, not last because it can be used to prove the following generalization:

Proposition 4.1.1. For any n reals $a_1, a_2, \ldots, a_n$, we have

$$a_1^2 + a_2^2 + \cdots + a_n^2 \geq a_1 a_2 + a_2 a_3 + a_3 a_4 + \cdots + a_{n-1} a_n + a_n a_1.$$

Proof. Adapt the above first solution to Exercise 4.1.1. (Exercise!) □

□

Let us now return to the topic of divisibility.

Exercise 4.1.2. Let $P(x)$ be a polynomial in a single variable x with integer coefficients. Let a and b be two integers. Prove that $a - b \mid P(a) - P(b)$.

Solution idea. This is particularly easy using the substitution principle for congruences (from worksheet 3): Indeed, set $n = a - b$. Then, $a \equiv b \mod n$ (why?), so that $P(a) \equiv P(b) \mod n$ (by the substitution principle). However, this means that $n \mid P(a) - P(b)$. In view of $n = a - b$, this becomes $a - b \mid P(a) - P(b)$, and we are done.

However, let us give a more direct proof, as it is instructive in its own way. It relies on the following identity, which is one of the most important identities in mathematics:

Theorem 4.1.2 (generalized geometric series formula)**.** Let a and b be any two numbers (not necessarily integers), and let $m \in \mathbb{N}$. Then,

$$a^m - b^m = (a-b) \underbrace{\left(a^{m-1} + a^{m-2}b + a^{m-3}b^2 + \cdots + ab^{m-2} + b^{m-1}\right)}_{= \sum_{k=0}^{m-1} a^k b^{m-1-k}}.$$

For example, for $m = 4$, this is saying that

$$a^4 - b^4 = (a-b)\left(a^3 + a^2b + ab^2 + b^3\right).$$

For $m = 3$, this is saying that

$$a^3 - b^3 = (a-b)\left(a^2 + ab + b^2\right).$$

The $m = 2$ case, of course, should be particularly familiar:

$$a^2 - b^2 = (a-b)(a+b).$$

Why am I calling Theorem 4.1.2 the "generalized geometric series formula"? Because setting $b = 1$ in Theorem 4.1.2 yields

$$a^m - 1 = (a-1)\left(a^{m-1} + a^{m-2} + a^{m-3} + \cdots + a + 1\right),$$

whence

$$a^{m-1} + a^{m-2} + a^{m-3} + \cdots + a + 1 = \frac{a^m - 1}{a - 1} \qquad (\text{if } a \neq 1),$$

which is a well-known formula for the sum of a (finite) geometric series. (The infinite version follows by letting $m \to \infty$.)

Theorem 4.1.2 is not hard to prove by induction on m (see, e.g., [Grinbe19, solution to Exercise 1]), but it is more instructive to prove it directly using a string of cancellations:

Proof of Theorem 4.1.2. By the law of distributivity, we have

$$\begin{aligned}
&(a-b)\left(a^{m-1}+a^{m-2}b+a^{m-3}b^2+\cdots+ab^{m-2}+b^{m-1}\right)\\
&=\underbrace{(a-b)\,a^{m-1}}_{=a^m-a^{m-1}b}+\underbrace{(a-b)\,a^{m-2}b}_{=a^{m-1}b-a^{m-2}b^2}+\underbrace{(a-b)\,a^{m-3}b^2}_{=a^{m-2}b^2-a^{m-3}b^3}+\cdots+\underbrace{(a-b)\,ab^{m-2}}_{=a^2b^{m-2}-ab^{m-1}}+\underbrace{(a-b)\,b^{m-1}}_{=ab^{m-1}-b^m}\\
&=\left(a^m-a^{m-1}b\right)+\left(a^{m-1}b-a^{m-2}b^2\right)+\left(a^{m-2}b^2-a^{m-3}b^3\right)\\
&\qquad+\cdots+\left(a^2b^{m-2}-ab^{m-1}\right)+\left(ab^{m-1}-b^m\right). \qquad (1)
\end{aligned}$$

A close look at the right hand side reveals that almost all of its terms cancel each other: To wit, each term other than the "bookend terms" a^m and b^m has the form $a^{m-i}b^i$ for some $i \in \{1,2,\ldots,m-1\}$, and appears once with a $+$ sign and once with a $-$ sign (which, of course, means that its two appearances cancel out). Thus, the right hand side equals $a^m - b^m$. Thus, (1) simplifies to

$$(a-b)\left(a^{m-1}+a^{m-2}b+a^{m-3}b^2+\cdots+ab^{m-2}+b^{m-1}\right)=a^m-b^m.$$

This proves Theorem 4.1.2. (A pedantic reader will observe that our "cancellation" argument does not work for $m = 0$, in which case there are no terms on the right hand side to begin with. But this case can be safely left aside as obvious.) □

We can now finish our second, direct solution to Exercise 4.1.2: Write the polynomial $P(x)$ in the form $P(x) = \sum_{m=0}^{d} p_m x^m$, where $p_0, p_1, \ldots, p_d$ are integers (the coefficients of $P(x)$). Then, $P(a) = \sum_{m=0}^{d} p_m a^m$ and $P(b) = \sum_{m=0}^{d} p_m b^m$, so that

$$\begin{aligned}
P(a)-P(b) &= \sum_{m=0}^{d} p_m a^m - \sum_{m=0}^{d} p_m b^m\\
&= \sum_{m=0}^{d} p_m \underbrace{\left(a^m-b^m\right)}_{\substack{=(a-b)\left(a^{m-1}+a^{m-2}b+a^{m-3}b^2+\cdots+ab^{m-2}+b^{m-1}\right)\\ \text{(by Theorem 4.1.2)}}}\\
&= \sum_{m=0}^{d} p_m (a-b)\left(a^{m-1}+a^{m-2}b+a^{m-3}b^2+\cdots+ab^{m-2}+b^{m-1}\right)\\
&= (a-b)\cdot \underbrace{\sum_{m=0}^{d} p_m \left(a^{m-1}+a^{m-2}b+a^{m-3}b^2+\cdots+ab^{m-2}+b^{m-1}\right)}_{\text{This is obviously an integer!}}.
\end{aligned}$$

This immediately yields $a-b \mid P(a) - P(b)$. Thus, Exercise 4.1.2 is solved again. □

Some more comments are worth making here. First, Theorem 4.1.2 has an analogue for $a^m + b^m$ instead of $a + b$, which however requires m to be odd:

Theorem 4.1.3. Let a and b be any two numbers (not necessarily integers), and let $m \in \mathbb{N}$ be odd. Then,

$$a^m + b^m = (a+b) \underbrace{\left(a^{m-1} - a^{m-2}b + a^{m-3}b^2 \pm \cdots - ab^{m-2} + b^{m-1}\right)}_{= \sum\limits_{k=0}^{m-1} (-1)^{m-1-k} a^k b^{m-1-k}}.$$

Proof. Apply Theorem 4.1.2 to $-b$ instead of b, and use the fact that $(-b)^m = -b^m$ (which is a consequence of m being odd). □

For example, for $m = 3$, Theorem 4.1.3 is saying that

$$a^3 + b^3 = (a+b)\left(a^2 - ab + b^2\right) \tag{2}$$

for any numbers a and b.

When m is even, there is no such formula as Theorem 4.1.3, and indeed $a^m + b^m$ is not usually divisible by $a + b$ in this case (for example, $a = 1$ and $b = 2$ and $m = 2$).

Let us also state the "cancellation" argument that we used to simplify the right hand side of (1) explicitly as a theorem:

Theorem 4.1.4. Let u and v be two integers such that $u - 1 \leq v$. Let a_s be a number for each $s \in \{u, u+1, \ldots, v+1\}$. Then,

$$\sum_{s=u}^{v} (a_s - a_{s+1}) = a_u - a_{v+1}.$$

Proof. We have

$$\sum_{s=u}^{v} (a_s - a_{s+1}) = (a_u - a_{u+1}) + (a_{u+1} - a_{u+2}) + (a_{u+2} - a_{u+3}) + \cdots + (a_v - a_{v+1}).$$

If $v \geq u$, then all terms on the right hand side cancel out except for the two "bookend terms" a_u and a_{v+1}; thus we are left with the difference $a_u - a_{v+1}$. Thus, Theorem 4.1.4 holds if $v \geq u$. The case $v = u - 1$ is even more obvious (as the theorem is just saying that $0 = 0$ in that case).

Alternatively, Theorem 4.1.4 can also be proved by a completely straightforward induction on v. □

Theorem 4.1.4 is called the *telescope principle for sums* since the cancelling terms in the proof make the sum "fold like a telescope". Here is an alternative version of the principle (with "backward" instead of "forward" differences):

Theorem 4.1.5 (telescope principle for sums)**.** Let u and v be two integers such that $u-1 \leq v$. Let a_s be a number for each $s \in \{u-1, u, \ldots, v\}$. Then,

$$\sum_{s=u}^{v} (a_s - a_{s-1}) = a_v - a_{u-1}.$$

Proof. The same cancellation argument as in Theorem 4.1.4 works here, except that the cancelling terms are slightly further from each other. Alternatively, this can easily be derived from Theorem 4.1.4 as follows: Set

$$b_i := -a_{i-1} \qquad \text{for each } i \in \{u, u+1, \ldots, v+1\}.$$

Then, for each $s \in \{u, u+1, \ldots, v\}$, we have

$$\underbrace{b_s}_{=-a_{s-1}} - \underbrace{b_{s+1}}_{=-a_{(s+1)-1}=-a_s} = (-a_{s-1}) - (-a_s) = a_s - a_{s-1}.$$

Hence,

$$\sum_{s=u}^{v} \underbrace{(b_s - b_{s+1})}_{=a_s - a_{s-1}} = \sum_{s=u}^{v} (a_s - a_{s-1}).$$

Comparing this with

$$\sum_{s=u}^{v} (b_s - b_{s+1}) = \underbrace{b_u}_{=-a_{u-1}} - \underbrace{b_{v+1}}_{\substack{=-a_{(v+1)-1} \\ =-a_v}} \qquad \text{(by Theorem 4.1.4, applied to } b_i \text{ instead of } a_i\text{)}$$
$$= (-a_{u-1}) - (-a_v) = a_v - a_{u-1},$$

we obtain $\sum\limits_{s=u}^{v} (a_s - a_{s-1}) = a_v - a_{u-1}$. This proves Theorem 4.1.5. □

The telescope principle is often useful in computing or simplifying sums. When one applies Theorem 4.1.4 to simplify a sum of the form $\sum\limits_{s=u}^{v} (a_s - a_{s+1})$ (or Theorem 4.1.5 to simplify a sum of the form $\sum\limits_{s=u}^{v} (a_s - a_{s-1})$), one says that the sum *telescopes* to $a_u - a_{v+1}$ (or $a_v - a_{u-1}$, respectively). Here is one less trivial example of a sum that telescopes:

Exercise 4.1.3. Let $n \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{n} (-1)^k k! (n-k)! = \begin{cases} \dfrac{2(n+1)!}{n+2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

Solution idea. We want to make the sum telescope. That is, we want to write the addend $(-1)^k k! (n-k)!$ in the form $a_k - a_{k+1}$ for some numbers $a_0, a_1, \ldots, a_{n+1}$. What are these numbers $a_0, a_1, \ldots, a_{n+1}$? (They are not determined uniquely, but we hope that we can find some good choice.)

Let us get the $(-1)^k$ out of the way first. To have $(-1)^k k! (n-k)! = a_k - a_{k+1}$ is tantamount to having $k! (n-k)! = (-1)^k (a_k - a_{k+1})$. If we set

$$b_i := (-1)^i a_i \qquad \text{for each } i \in \{0, 1, \ldots, n+1\},$$

then the latter equation rewrites as $k! (n-k)! = b_k + b_{k+1}$, because we have

$$\underbrace{b_k}_{=(-1)^k a_k} + \underbrace{b_{k+1}}_{\substack{=(-1)^{k+1} a_{k+1} \\ =-(-1)^k a_{k+1}}} = (-1)^k a_k - (-1)^k a_{k+1} = (-1)^k (a_k - a_{k+1}).$$

Thus, we want to find $n+2$ numbers $b_0, b_1, \ldots, b_{n+1}$ such that $k! (n-k)! = b_k + b_{k+1}$ for all $k \in \{0, 1, \ldots, n\}$.

We fix $k \in \{0, 1, \ldots, n\}$ and start playing around with $k! (n-k)!$. On the one hand, from $(k+1)! = (k+1) \cdot k!$, we obtain $k! = \dfrac{(k+1)!}{k+1}$, so that

$$\begin{aligned} k! (n-k)! &= \frac{(k+1)!}{k+1} \cdot (n-k)! \\ &= \frac{(k+1)! (n-k)!}{k+1}. \end{aligned} \tag{3}$$

On the other hand, from $(n-k+1)! = (n-k+1) \cdot (n-k)!$, we obtain $(n-k)! = \dfrac{(n-k+1)!}{n-k+1}$, so that

$$\begin{aligned} k! (n-k)! &= k! \cdot \frac{(n-k+1)!}{n-k+1} \\ &= \frac{k! (n-k+1)!}{n-k+1}. \end{aligned} \tag{4}$$

A ray of hope shines through: The numerator in (3) is the same as the numerator in (4) with k replaced by $k+1$. That is, if the numerator in (4) was b_k, then the numerator in (3) would be b_{k+1}. In order to obtain $b_k + b_{k+1}$, we thus somehow need to add the numerators and hope the result is still $k!\,(n-k)!$. And we would also want the denominators to disappear, or at least to become independent of k.

This is a lot to wish for, but it does indeed come true! The helpful fairy here is the following lemma:

Lemma 4.1.6 (equal fractions lemma)**.** Let a, b, c, d, x be five real numbers such that $b \neq 0$ and $d \neq 0$ and $b + d \neq 0$ and

$$x = \frac{a}{b} = \frac{c}{d}.$$

Then,

$$x = \frac{a+c}{b+d}.$$

In other words, this lemma is saying that if two fractions are equal, then the fraction obtained by adding their numerators and adding their denominators is also equal to them (as long as the denominator is nonzero). The proof is so easy that one might question whether the lemma deserves a name; but my view is that it does for its usefulness.

Now, recall the equalities (3) and (4). Thanks to these two equalities, we can apply Lemma 4.1.6 to $x = k!\,(n-k)!$ and $a = (k+1)!\,(n-k)!$ and $b = k+1$ and $c = k!\,(n-k+1)!$ and $d = n-k+1$. We thus obtain

$$\begin{aligned}
&k!\,(n-k)! \\
&= \frac{(k+1)!\,(n-k)! + k!\,(n-k+1)!}{(k+1)+(n-k+1)} \\
&= \frac{(k+1)!\,(n-k)! + k!\,(n-k+1)!}{n+2} \qquad \left(\text{since } (k+1)+(n-k+1) = n+2\right) \\
&= \frac{(k+1)!\,(n-k)!}{n+2} + \frac{k!\,(n-k+1)!}{n+2} \\
&= \frac{k!\,(n-k+1)!}{n+2} + \frac{(k+1)!\,(n-k)!}{n+2}.
\end{aligned} \tag{5}$$

Now it is clear what to do: We set

$$b_i := \frac{i!\,(n-i+1)!}{n+2} \qquad \text{for each } i \in \{0, 1, \ldots, n+1\}. \tag{6}$$

Then, (5) rewrites as

$$k!\,(n-k)! = b_k + b_{k+1}. \tag{7}$$

If we furthermore set

$$a_i := (-1)^i\, b_i \qquad \text{for each } i \in \{0, 1, \ldots, n+1\} \tag{8}$$

(so that we have $b_i = (-1)^i a_i$, as intended above), then we have

$$(-1)^k \underbrace{k!\,(n-k)!}_{\substack{=b_k+b_{k+1} \\ \text{(by (7))}}} = (-1)^k (b_k + b_{k+1}) = (-1)^k b_k + \underbrace{(-1)^k}_{=-(-1)^{k+1}} b_{k+1}$$

$$= \underbrace{(-1)^k b_k}_{\substack{=a_k \\ \text{(by (8))}}} - \underbrace{(-1)^{k+1} b_{k+1}}_{\substack{=a_{k+1} \\ \text{(by (8))}}} = a_k - a_{k+1}.$$

Forget that we fixed k. We thus have proved that $(-1)^k k!\,(n-k)! = a_k - a_{k+1}$ for all $k \in \{0,1,\ldots,n\}$ (where the b_i are defined by (6), and the a_i are defined by (8)). Thus,

$$\sum_{k=0}^{n} \underbrace{(-1)^k k!\,(n-k)!}_{=a_k - a_{k+1}} = \sum_{k=0}^{n} (a_k - a_{k+1}) = a_0 - a_{n+1}$$

(by the telescope principle[1]). In view of

$$a_0 = \underbrace{(-1)^0}_{=1} b_0 \qquad \text{(by (8))}$$
$$= b_0 = \frac{0!\,(n-0+1)!}{n+2} \qquad \text{(by (6))}$$
$$= \frac{(n+1)!}{n+2}$$

and

$$a_{n+1} = (-1)^{n+1} \frac{(n+1)!}{n+2} \qquad \text{(by a similar computation)},$$

we can rewrite this as

$$\sum_{k=0}^{n} (-1)^k k!\,(n-k)! = \frac{(n+1)!}{n+2} - (-1)^{n+1} \frac{(n+1)!}{n+2}$$
$$= \underbrace{\left(1 - (-1)^{n+1}\right)}_{=\begin{cases} 2, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}} \frac{(n+1)!}{n+2}$$
$$= \begin{cases} 2, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases} \cdot \frac{(n+1)!}{n+2} = \begin{cases} \dfrac{2\,(n+1)!}{n+2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

This solves Exercise 4.1.3. □

[1] or, to be specific, by Theorem 4.1.4, applied to $u = 0$ and $v = n$

Many other examples of the use of the telescope principle are found in [Grinbe20, §4.1.4].

Let us go back to some number theory:

Exercise 4.1.4. Let n be a positive integer. Let u be the number of pairs (j,k) of positive integers satisfying $\dfrac{1}{j} - \dfrac{1}{k} = \dfrac{1}{n}$.

Prove that u is the number of all integers $i \in \{1, 2, \ldots, n-1\}$ satisfying $i \mid n^2$.

Solution idea. (See [Grinbe20, §A.11.5] for details.) The core of the solution is the following chain of equivalences (which holds for any three nonzero numbers j, k, n, not just for integers):

$$\begin{aligned}
& \left(\frac{1}{j} - \frac{1}{k} = \frac{1}{n}\right) \\
\iff & (nk - nj = jk) \qquad \text{(here, we multiplied both sides by } njk\text{)} \\
\iff & (nk - nj - jk = 0) \\
\iff & \left(nk - nj - jk + n^2 = n^2\right) \qquad \left(\begin{array}{c}\text{here, we added } n^2 \text{ to both sides} \\ \text{for no visible reason}\end{array}\right) \\
\iff & \left((n-j)(n+k) = n^2\right) \qquad \left(\text{since } nk - nj - jk + n^2 = (n-j)(n+k)\right).
\end{aligned}$$

This transformation is known as *Simon's favorite factoring trick* (a moniker it has gotten on the early 2000's webforums; its discovery, I am sure, predates whatever Simon it is referring to). In a way, it is similar to "completing the square": a quadratic expression (in our case, $nk - nj - jk$) is made to factor by adding a new addend to it.

The trick gives the exercise away. Indeed, replacing the condition $\dfrac{1}{j} - \dfrac{1}{k} = \dfrac{1}{n}$ in the exercise by the equivalent relation $(n-j)(n+k) = n^2$, we see immediately what these pairs (j,k) have to do with divisors of n^2. Namely, if (j,k) is a pair of positive integers satisfying $\dfrac{1}{j} - \dfrac{1}{k} = \dfrac{1}{n}$, then $n - j$ is an integer $i \in \{1, 2, \ldots, n-1\}$ satisfying $i \mid n^2$ (indeed, $(n-j)(n+k) = n^2$ yields that $n - j \mid n^2$, and furthermore it shows that $n - j$ is positive (why?); but $n - j$ is also $\leq n - 1$ (since $j \geq 1$)). Thus, we have found a map

$$\begin{aligned}
&\text{from the set } \left\{\text{pairs } (j,k) \text{ of positive integers satisfying } \frac{1}{j} - \frac{1}{k} = \frac{1}{n}\right\} \\
&\text{to the set } \left\{\text{integers } i \in \{1, 2, \ldots, n-1\} \text{ satisfying } i \mid n^2\right\}
\end{aligned}$$

which sends a pair (j,k) to $n - j$. Let us denote this map by f.

Conversely, we can define a map g

$$\text{from the set } \left\{\text{integers } i \in \{1,2,\ldots,n-1\} \text{ satisfying } i \mid n^2\right\}$$
$$\text{to the set } \left\{\text{pairs } (j,k) \text{ of positive integers satisfying } \frac{1}{j}-\frac{1}{k}=\frac{1}{n}\right\}$$

which sends each i in the former set to the pair $\left(n-i,\ \dfrac{n^2}{i}-n\right)$. It is straightforward to check that this map g is well-defined and inverse to f. (Indeed, the definition of g was obtained by solving for the pair (j,k) satisfying $\dfrac{1}{j}-\dfrac{1}{k}=\dfrac{1}{n}$ and $n-j=i$.)

Now, the map f is invertible (since g is inverse to f), thus a bijection[2]. Hence, we have found a bijection

$$\text{from the set } \left\{\text{integers } i \in \{1,2,\ldots,n-1\} \text{ satisfying } i \mid n^2\right\}$$
$$\text{to the set } \left\{\text{pairs } (j,k) \text{ of positive integers satisfying } \frac{1}{j}-\frac{1}{k}=\frac{1}{n}\right\}$$

(namely, f). This shows that these two sets have the same size. In other words, the number of all integers $i \in \{1,2,\ldots,n-1\}$ satisfying $i \mid n^2$ equals the number of all pairs (j,k) of positive integers satisfying $\dfrac{1}{j}-\dfrac{1}{k}=\dfrac{1}{n}$. Since the latter number is u, we have thus solved Exercise 4.1.4. □

We now come back to inequalities:

Exercise 4.1.5. Let a,b,c be three nonnegative reals. Prove the inequality

$$a^3+b^3+c^3 \geq 3abc.$$

Solution idea. This is similar to Exercise 4.1.1, in that there is again a magical one-paragraph solution:

First solution to Exercise 4.1.5. Expanding the product $(a+b+c)\left(a^2+b^2+c^2-bc-ca-ab\right)$, we obtain

$$\begin{aligned}&(a+b+c)\left(a^2+b^2+c^2-bc-ca-ab\right)\\&=a^3+b^3+c^3-3abc.\end{aligned} \tag{9}$$

[2]Reminder: "Bijection" means "bijective map" (also known as "one-to-one correspondence").

Hence,

$$a^3 + b^3 + c^3 - 3abc = \underbrace{(a+b+c)}_{\geq 0} \underbrace{\left(a^2 + b^2 + c^2 - bc - ca - ab\right)}_{\substack{\geq 0 \\ \text{(since Exercise 4.1.1} \\ \text{says that } a^2+b^2+c^2 \geq bc+ca+ab)}} \geq 0.$$

In other words, $a^3 + b^3 + c^3 \geq 3abc$. This solves Exercise 4.1.5. □

This is nice, but again completely unmotivated: How would one find the identity (9) if one didn't already know its left hand side?

There are, in fact, several ways. One is to treat a, b, c as indeterminates and try to factor the polynomial $a^3 + b^3 + c^3 - 3abc$. Factoring a multivariate polynomial is not trivial, but there are algorithms that do it mechanically (see, e.g., `https://math.stackexchange.com/q/3127648` for an outline of such an algorithm). Sadly, these algorithms are too slow to be useful on an exam, particularly when one is not sure whether a nontrivial factorization actually exists (very often, it does not, so one would just waste time looking for one!) and whether it will be helpful to solving the problem.

But when general methods fail, tricks can save the day. One trick is to reduce the polynomial to a univariate one by fixing two of a, b, c. For example, if $b = 1$ and $c = 1$, then the polynomial $a^3 + b^3 + c^3 - 3abc$ becomes $a^3 + 1^3 + 1^3 - 3a \cdot 1 \cdot 1 = a^3 - 3a + 2$, which can be easily factored by finding rational roots (see the Wikipedia page for "rational root theorem" for how this works). Thus one obtains the factorization $a^3 - 3a + 2 = (a+2)(a-1)^2$. Likewise, setting $b = 2$ and $c = 1$, one obtains the factorization $(a+3)\left(a^2 - 3a + 3\right)$. Of course, one should not forget simple cases like $b = 0$ and $c = 0$, in which case the factorization a^3 comes out, or $b = 0$ and $c = 1$, in which case it is $(a+1)\left(a^2 - a + 1\right)$. Based on these examples, one might suspect that $a + b + c$ is always a factor in the factorization; that is, there should be some polynomial P in a, b, c such that

$$a^3 + b^3 + c^3 - 3abc = (a+b+c) \cdot P(a,b,c).$$

This polynomial P should be quadratic (for degree reasons), and it can be found by polynomial division (dividing $a^3 + b^3 + c^3 - 3abc$ by $a + b + c$), again treating b and c as constants (but not specifying their values). Thus one is led to (9).

Yet another way to discover (9) (using less work but more insight) is the following:

$$\begin{aligned}
& a^3+b^3+c^3-3abc \\
&= a^3+b^3-\underbrace{(a+b)^3}_{=a^3+3a^2b+3ab^2+b^3}+(a+b)^3+c^3-3abc \\
&= \underbrace{a^3+b^3-\left(a^3+3a^2b+3ab^2+b^3\right)}_{\substack{=-3a^2b-3ab^2 \\ =-3ab(a+b)}}+\underbrace{(a+b)^3+c^3}_{\substack{=((a+b)+c)\left((a+b)^2-(a+b)c+c^2\right) \\ \text{(by (2), applied to } a+b \text{ and } c \\ \text{instead of } a \text{ and } b)}}-3abc \\
&= -3ab\left(a+b\right)+\left(\left(a+b\right)+c\right)\left(\left(a+b\right)^2-\left(a+b\right)c+c^2\right)-3abc \\
&= \underbrace{-3ab\left(a+b\right)-3abc}_{=-3ab(a+b+c)}+\underbrace{\left(\left(a+b\right)+c\right)}_{=a+b+c}\left(\left(a+b\right)^2-\left(a+b\right)c+c^2\right) \\
&= -3ab\left(a+b+c\right)+\left(a+b+c\right)\left(\left(a+b\right)^2-\left(a+b\right)c+c^2\right) \\
&= \left(a+b+c\right)\underbrace{\left(-3ab+\left(\left(a+b\right)^2-\left(a+b\right)c+c^2\right)\right)}_{\substack{=a^2+b^2+c^2-bc-ca-ab \\ \text{(by expanding the squares and products)}}} \\
&= \left(a+b+c\right)\left(a^2+b^2+c^2-bc-ca-ab\right).
\end{aligned}$$

However, discovering (9) is not the only way to solve Exercise 4.1.5. There are several other approaches. Here is one that is particularly dear to my heart.

We recall our Third solution to Exercise 4.1.1 above. In that solution, we have "completed a square", which was possible because the polynomial in question was quadratic. Unfortunately, our polynomial $a^3+b^3+c^3-3abc$ is cubic in each of its variables, so this does not work. However, we can do something ludicrous: We introduce another variable in which the polynomial will have a lower degree!

For brevity, we set $F\left(a,b,c\right) := a^3+b^3+c^3-3abc$ (so that the claim of Exercise 4.1.5 can be rewritten as $F\left(a,b,c\right) \geq 0$), and we consider the polynomial $F\left(a+d,b+d,c+d\right)$, where d is a new indeterminate. (That is, we shift each of a,b,c by the same indeterminate amount d.) It is easy to see that this new polynomial $F\left(a+d,b+d,c+d\right)$ will have degree at most 2 in d, since the d^3-terms all cancel out:

$$F\left(a+d,b+d,c+d\right) = \underbrace{\left(a+d\right)^3+\left(b+d\right)^3+\left(c+d\right)^3}_{=3d^3+\text{(lower powers of } d)} - 3\underbrace{\left(a+d\right)\left(b+d\right)\left(c+d\right)}_{=d^3+\text{(lower powers of } d)}$$

(where we treat a,b,c as constants). This makes $F\left(a+d,b+d,c+d\right)$ a good candidate for "completing the square".

Actually computing this polynomial $F\left(a+d,b+d,c+d\right)$ reveals that it is not quadratic but linear in d:

$$F\left(a+d,b+d,c+d\right) = \left(a^3+b^3+c^3-3abc\right)+3d\left(a^2+b^2+c^2-bc-ca-ab\right).$$

This is not quite what we wanted (there is no square to complete), but it is just as useful, as it points us in a new direction: For any $d \geq 0$ and any $a, b, c \in \mathbb{R}$, we have

$$\begin{aligned} F(a+d, b+d, c+d) &= \underbrace{\left(a^3+b^3+c^3-3abc\right)}_{=F(a,b,c)} + 3d \underbrace{\left(a^2+b^2+c^2-bc-ca-ab\right)}_{\substack{\geq 0 \\ \text{(by Exercise 4.1.1)}}} \\ &\geq F(a,b,c) + 3d \cdot 0 = F(a,b,c). \end{aligned} \tag{10}$$

In other words, if we shift each of a, b, c to the right[3] by one and the same nonnegative amount d, then the value $F(a,b,c)$ can only increase. Thus, conversely, if we shift each of a, b, c to the left by one and the same nonnegative amount d, then the value $F(a,b,c)$ can only decrease. However, by this kind of left-shift, we can always achieve a case in which one of a, b, c is 0 (we just keep shifting until the smallest of a, b, c reaches 0; in other words, we shift to the left by $\min\{a,b,c\}$). Thus, if we can show that $F(a,b,c) \geq 0$ in this simple case, then we will be able to conclude that $F(a,b,c) \geq 0$ always holds (i.e., holds for all nonnegative reals a, b, c) – because shifting a, b, c back can only increase $F(a,b,c)$.

The simple case deserves its name. To wit, if one of a, b, c is 0, then $3abc = 0$, so that $F(a,b,c) = a^3 + b^3 + c^3 \geq 0$ obviously. Thus, we have again solved Exercise 4.1.5, but this time without factoring $F(a,b,c)$. Again, this solution can be written up pretty neatly:

Second solution to Exercise 4.1.5. Let $m := \min\{a,b,c\}$. Thus, we have $m \leq a$ and $m \leq b$ and $m \leq c$, but m is one of the three numbers a, b, c. The latter fact yields $m \geq 0$.

Next, let $\alpha := a - m$ and $\beta := b - m$ and $\gamma := c - m$. Then, α, β, γ are nonnegative reals (since $m \leq a$ and $m \leq b$ and $m \leq c$), and at least one of them is 0 (since m is one of the three numbers a, b, c). Hence, $\alpha\beta\gamma = 0$. However, from $\alpha = a - m$, we obtain $a = \alpha + m$ and similarly $b = \beta + m$ and $c = \gamma + m$. Thus,

$$\begin{aligned} & a^3+b^3+c^3-3abc \\ &= (\alpha+m)^3 + (\beta+m)^3 + (\gamma+m)^3 - 3(\alpha+m)(\beta+m)(\gamma+m) \\ &= \underbrace{\alpha^3+\beta^3+\gamma^3}_{\substack{\geq 0 \\ \text{(since } \alpha,\beta,\gamma \text{ are nonnegative)}}} - 3\underbrace{\alpha\beta\gamma}_{=0} + 3m \underbrace{\left(\alpha^2+\beta^2+\gamma^2-\beta\gamma-\gamma\alpha-\alpha\beta\right)}_{\substack{\geq 0 \\ \text{(by Exercise 4.1.1, applied to } \alpha,\beta,\gamma \text{ instead of } a,b,c)}} \\ & \qquad \text{(this can be checked by straightforward computation)} \\ &\geq 0 - 3 \cdot 0 + 3m \cdot 0 = 0. \end{aligned}$$

In other words, $a^3 + b^3 + c^3 \geq 3abc$. This solves Exercise 4.1.5 again.

(Note that we have implicitly used $m \geq 0$. Do you see where?) □

[3] on the real axis

□

One more factorization problem (this time explicitly stated as one):

Exercise 4.1.6. Factor the polynomial

$$x(y-z)^3 + y(z-x)^3 + z(x-y)^3.$$

Solution idea. As already discussed in the solution to Exercise 4.1.5, this sort of exercise can be solved mechanically by a computer: There are algorithms for factoring a polynomial with integer coefficients. On an exam, however, tricks are more useful.

One trick that helps here is *identifying factors*: We just try to find the factors of the factorization one after the other, by asking ourselves what these factors can be. The more factors we find, the easier it becomes to find the rest, because we can divide our known factors out[4] and get a polynomial of smaller degree. Our polynomial

$$P(x,y,z) := x(y-z)^3 + y(z-x)^3 + z(x-y)^3$$

has degree 4; thus, if we can find two linear factors, then the quotient by them will have degree 2, which sounds rather manageable.

How do we find factors? If $Q(x,y,z)$ is a factor of $P(x,y,z)$, then $P(x,y,z)$ will always be 0 whenever $Q(x,y,z)$ is 0. Thus, if we know a large set on which $P(x,y,z)$ is 0, then a factor of $P(x,y,z)$ is not far away. (I am not explaining what "large" means, so this should not be taken too literally.)

We are in luck: Our polynomial $P(x,y,z)$ is 0 whenever $x=y$. Indeed, if $x=y$, then

$$\begin{aligned} P(x,y,z) &= \underbrace{x}_{=y}(y-z)^3 + y\left(z - \underbrace{x}_{=y}\right)^3 + z\underbrace{(x-y)^3}_{\substack{=0 \\ \text{(since } x=y\text{)}}} \\ &= y(y-z)^3 + y\underbrace{(z-y)^3}_{=-(y-z)^3} = y(y-z)^3 - y(y-z)^3 = 0. \end{aligned}$$

In other words, our polynomial $P(x,y,z)$ is 0 whenever the linear polynomial $x-y$ is 0. This suggests that $x-y$ should be a factor of $P(x,y,z)$. For analogous reasons, $y-z$ and $z-x$ should be factors of $P(x,y,z)$ as well. Thus, we try to successively divide $P(x,y,z)$ by $x-y$, $y-z$ and $z-x$, and see what comes out.

This works indeed, and what comes out is $x+y+z$. Thus, we obtain

$$P(x,y,z) = (x-y)(y-z)(z-x)(x+y+z).$$

Our factorization is therefore

$$x(y-z)^3 + y(z-x)^3 + z(x-y)^3 = (x-y)(y-z)(z-x)(x+y+z).$$

[4]using polynomial division (e.g., treating x as a variable and y and z as constants)

Of course, once this factorization has been found, verifying it is a matter of just expanding both sides; thus, you don't need to write up the above thinking process on an exam.

Here is another way to find this factorization: Let $f = y - z$ and $g = z - x$. Then, $f + g = (y - z) + (z - x) = y - x = -(x - y)$, so that $x - y = -(f + g)$. Thus, $(x - y)^3 = (-(f + g))^3 = -(f + g)^3$. Now,

$$\begin{aligned}
& x \left(\underbrace{y - z}_{=f} \right)^3 + y \left(\underbrace{z - x}_{=g} \right)^3 + z \underbrace{(x - y)^3}_{=-(f+g)^3} \\
&= xf^3 + yg^3 + z \left(-(f + g)^3 \right) \\
&= xf^3 + yg^3 - z \underbrace{(f + g)^3}_{=f^3+3f^2g+3fg^2+g^3} \\
&= xf^3 + yg^3 - z \left(f^3 + 3f^2g + 3fg^2 + g^3 \right) \\
&= \underbrace{\left(xf^3 - zf^3 \right)}_{=(x-z)f^3} + \underbrace{\left(yg^3 - zg^3 \right)}_{=(y-z)g^3} - \underbrace{\left(z \cdot 3f^2g + z \cdot 3fg^2 \right)}_{=3zfg(f+g)} \\
&= \underbrace{(x - z)}_{\substack{=-(z-x)=-g \\ (\text{since } z-x=g)}} f^3 + \underbrace{(y - z)}_{=f} g^3 - 3zfg(f + g) \\
&= \underbrace{(-g) f^3 + fg^3}_{=-fg(f^2-g^2)} - 3zfg(f + g) \\
&= -fg \underbrace{\left(f^2 - g^2 \right)}_{=(f-g)(f+g)} - 3zfg(f + g) \\
&= -fg(f - g)(f + g) - 3zfg(f + g) \\
&= \underbrace{f}_{=y-z} \underbrace{g}_{=z-x} \underbrace{(f + g)}_{=-(x-y)} \underbrace{(-(f - g) - 3z)}_{\substack{=-(x+y+z) \\ (\text{by easy computation})}} \\
&= (y - z)(z - x)(-(x - y))(-(x + y + z)) \\
&= (x - y)(y - z)(z - x)(x + y + z).
\end{aligned}$$

□

See also [Grinbe20, Exercise 1.1.7] for an exercise similar to Exercise 4.1.6.

4.2. Class problems

The following problems are to be discussed during class.

Exercise 4.2.1. Let $n \geq 2$ be an integer. Simplify the product $\prod_{k=2}^{n} \frac{k-1}{k+1}$.

[**Hint:** The telescope principle applies to products just as it does to sums.]

Exercise 4.2.2. Solve Exercise 1.3.1 from worksheet 1 again using the telescope principle.

(Here is the exercise: Let n be a positive integer. For each $k \in \{1, 2, \ldots, n-1\}$, we let

$$a_k := (n-k) \prod_{i=0}^{k-2} (n-i) = (n-k)(n-k+2)(n-k+3) \cdots n.$$

Prove that

$$\sum_{k=1}^{n-1} a_k = n! - 1.$$

)

Exercise 4.2.3. Let a and b be positive integers such that $(a, b) \neq (1, 1)$. Prove that $a^4 + 4b^4$ cannot be prime.

Exercise 4.2.4. Let $n \in \mathbb{N}$. Let $P(x)$ be an arbitrary polynomial of degree smaller than n in a single variable x. Prove that

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

Exercise 4.2.5. Let x, y, z be three positive reals such that $xyz = 1$. Simplify

$$\frac{1}{1+x+xy} + \frac{1}{1+y+yz} + \frac{1}{1+z+zx}.$$

4.3. Homework exercises

Solve 3 of the 6 exercises below and upload your solutions on gradescope by October 22.

Exercise 4.3.1. Let n be a positive integer. Let u be the number of pairs (j, k) of positive integers satisfying $\frac{1}{j} + \frac{1}{k} = \frac{1}{n}$.

Prove that u is the number of all positive divisors of n^2.

Exercise 4.3.2. Let $n \geq 2$ be an integer. Simplify the product $\prod_{k=2}^{n} \frac{k^3 - 1}{k^3 + 1}$.

Exercise 4.3.3. Prove that

$$a(a-b)(a-c) + b(b-c)(b-a) + c(c-a)(c-b) \geq 0$$

for any three nonnegative reals a, b, c.

[**Hint:** Don't look for a factorization! This polynomial does not have a nontrivial factorization.]

Exercise 4.3.4. Let a, b, c be three real numbers such that $(a+b+c)^3 = a^3 + b^3 + c^3$. Prove that $(a+b+c)^n = a^n + b^n + c^n$ for each odd positive integer n.

Exercise 4.3.5. Let $n > 1$ be an integer. Factor the polynomial

$$\left(1 + x + x^2 + \cdots + x^n\right)^2 - x^n$$

as a product of two non-constant polynomials.

Exercise 4.3.6. Let n be a positive integer. Let $g(x)$ denote the polynomial $-\left(x^1 + x^2 + \cdots + x^n\right)$. Let $h(x)$ denote the polynomial

$$\sum_{k=0}^{n} (g(x))^k = (g(x))^0 + (g(x))^1 + (g(x))^2 + \cdots + (g(x))^n.$$

Prove that the coefficients of the powers $x^2, x^3, \ldots, x^n$ in $h(x)$ are 0.

References

[Grinbe19] Darij Grinberg, *UMN Spring 2019 Math 4281 homework set #0 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/19s/hw0s.pdf`

[Grinbe20] Darij Grinberg, *Math 235: Mathematical Problem Solving*, 10 August 2021. `https://www.cip.ifi.lmu.de/~grinberg/t/20f/mps.pdf`