

DISCRETE MATHEMATICS
HOMEWORK 6 SOLUTIONS

1. Suppose on the contrary that $\sqrt[3]{4}$ is rational. Then we can write $\sqrt[3]{4} = a/b$, where a and b are integers, and $\gcd(a, b) = 1$. A bit of algebra gives

$$\begin{aligned} 4 &= \frac{a^3}{b^3} \\ 4b^3 &= a^3. \end{aligned} \tag{1}$$

Since $2b^3 \in \mathbb{Z}$, this means that $2 \mid a^3$, which implies that $2 \mid a$. Why? Well, one argument uses unique factorization. If a factors into primes as

$$a = p_1 p_2 \cdots p_k,$$

then a^3 must factor as

$$a^3 = p_1^3 p_2^3 \cdots p_k^3.$$

In other words, a and a^3 contain exactly the same primes in their prime factorizations. Since $2 \mid a^3$, 2 must be one of the primes in the factorization of a^3 ; so 2 is one of the primes in the factorization of a ; in other words, $2 \mid a$.

We can therefore write $a = 2z$ for some integer z . Plugging this into equation (1) gives

$$\begin{aligned} 4b^3 &= (2z)^3 \\ 4b^3 &= 8z^3 \\ b^3 &= 2z^3. \end{aligned}$$

Now we reason just like we did above: This means that $2 \mid b^3$, which implies that $2 \mid b$.

This is a contradiction, though, since we started by assuming that $\gcd(a, b) = 1$, and we have now just shown that a and b have a common divisor of 2 . The initial hypothesis must therefore be incorrect, and $\sqrt[3]{4}$ must be irrational.

There are many small variants of this proof, most notably one using our alternative analysis of why $2 \mid a^3 \implies 2 \mid a$ without using unique factorization.

2. One could use Euclid's algorithm to solve most of these. One could also just mess around and discover that $2 \cdot 311 = 622 = 1$, so that $\frac{1}{2} = 311$; and that $4 \cdot 466 = 1864 = 1$, so that $\frac{1}{4} = 466$; and that $5 \cdot 497 = 2485 = 1$, so that $\frac{1}{5} = 497$. (An easy way to do the last 2 in your head is to observe that $4 \cdot 155 = 620 = -1$, which means that $1 = 4(-155) = 4 \cdot 466$; and that $5 \cdot 124 = -1$, which means that $5(-124) = 5 \cdot 497 = 1$.)

The fraction $\frac{1}{3}$ does not exist in \mathbb{Z}_{621} . Why? Well, if $x = \frac{1}{3}$ in \mathbb{Z}_{621} , then $3x = 1$ in \mathbb{Z}_{621} , which means that $3x = 1 + 621y$ in \mathbb{Z} for some $y \in \mathbb{Z}$, which means that for some $y \in \mathbb{Z}$,

$$\begin{aligned} 3x - 621y &= 1 \\ 3(x - 207y) &= 1. \end{aligned}$$

Since $3 \mid 3(x - 207y)$ but $3 \nmid 1$, it follows that $3(x - 207y) \neq 1$. Thus, $\frac{1}{3}$ does not exist

3. The first and third claims were correct; the second was nonsense.
 (a) If $a \mid b$, then there is an integer x such that

$$b = ax.$$

Multiplying by c then gives

$$bc = (ax)c = (ac)x.$$

Thus, $ac \mid bc$.

- (b) If $a \mid c$ and $b \mid c$, then it is not in general the case that $ab \mid c$. For instance, let $a = 6$, $b = 4$, and $c = 12$.
 (c) If $a \mid (b + c)$ and $a \mid (b - c)$, then there are integers x and y such that

$$\begin{aligned} ax &= b + c \\ ay &= b - c. \end{aligned}$$

Adding these equations gives $a(x + y) = 2b$. Since the integers are closed under addition, $x + y \in \mathbb{Z}$. Thus, $a \mid 2b$. It is not necessarily the case that $a \mid b$. For instance, let $a = 4$, $b = 2$, and $c = 6$.

4. The first of these had a solution; the second did not.
 (a) To solve the equation $79x - 250y = 1$, we begin by doing Euclid's algorithm in order to be sure a solution will exist. The calculation looks like this:

$$\begin{aligned} 250 &= 79(3) + 13 \\ 79 &= 13(6) + 1 \\ 13 &= 1(13) + 0. \end{aligned}$$

The gcd is therefore 1; so there should be a solution. To find it, we rewrite the equations from Euclid's algorithm for the remainders:

$$\begin{aligned} 13 &= 250 - 79(3) \\ 1 &= 79 - 13(6). \end{aligned}$$

We then use the first equation as a substitution in the second to get

$$1 = 79 - [250 - 79(3)](6) = 79(19) - 250(6).$$

One solution to the equation is thus $x = 19$, $y = 6$.

To get more solutions, do what we did in class: let $x = 19 + 250k$ and $y = 6 + 79k$ for any integer k . This always produces solutions, since

$$\begin{aligned}79(19 + 250k) - 250(6 + 79k) &= 79(19) + 79(250k) - 250(6) - 250(79k) \\ &= 79(19) - 250(6) = 1.\end{aligned}$$

To show that every solution has this form, let (x, y) be any solution whatever. Then

$$79x - 250y = 1 = 79(19) - 250(6),$$

so

$$79(x - 19) = 250(y - 6). \tag{1}$$

This means that $250 \mid 79(x-19)$. Since we have just shown that $\gcd(250, 79) = 1$, the Fundamental Theorem of Arithmetic tells us that $250 \mid (x - 19)$, i.e., that for some $k \in \mathbb{Z}$, $x - 19 = 250k$, i.e., that $x = 19 + 250k$, as desired. Finally, plugging this into equation (1) gives $79(250k) = 250(y - 6)$, so that $79k = y - 6$ and $y = 6 + 79k$. Every solution therefore has the form we claimed.

- (b) The equation $52x - 143y = 1$ has no solutions, since the left hand side is a multiple of $13 = \gcd(52, 143)$, and the right hand side is not.
- (c) What do these problems have to do with the problems of finding $1/79$ in \mathbb{Z}_{250} and $1/52$ in \mathbb{Z}_{143} ? Well, $1/79$ exists in \mathbb{Z}_{250} iff there is a solution to the equation $79x = 1$ in \mathbb{Z}_{250} (and the solution x is the value of $1/79$). This happens iff there is a solution in \mathbb{Z} to $79x = 1 + 250y$, i.e., a solution to $79x - 250y = 1$. In other words, the value of $1/79$ is exactly the x -value of the solution in part (b). In \mathbb{Z}_{250} , $1/79 = 19$.

The same analysis shows that $1/55$ exists in \mathbb{Z}_{143} if and only if the equation $52x - 143y = 1$ has solutions in \mathbb{Z} , which it doesn't.

5. Most of these weren't too bad, but there may have been exceptions.

- (a) $-13 = 65$ in \mathbb{Z}_{78} because $13 + 65 = 0$ in \mathbb{Z}_{78} .
- (b) There are a couple of approaches to this one. You could just start multiplying and discover by trial and error that $5 \times 8 = 40 = 3$ in \mathbb{Z}_{37} , which means that $3/5 = 8$ in \mathbb{Z}_{37} . You could also discover (either by trial and error or using the methods of the previous problem) that $5 \times 15 = 75 = 1$, which means that $1/5 = 15$, so that $3/5 = 3(1/5) = 3(15) = 45 = 8$.
- (c) $\sqrt{-1} = \pm 5 = 5$ or 8 in \mathbb{Z}_{13} , since $5^2 = 8^2 = 12 = -1$ in \mathbb{Z}_{13} .
- (d) This one contained a slight surprise: $\sqrt{4}$ has 4 distinct values in \mathbb{Z}_{21} : any of 2, 5, 16, or 19 square to give 4 in \mathbb{Z}_{21} .
- (e) $\gcd(1234567890, 99)$ could be worked out either by factoring 99 as $3^2 \cdot 11$, and looking for which of these factors divided 1234567890, or by using Euclid's algorithm. Either approach would have given a gcd of 9.
- (f) To work out $\gcd(39495952, 12472429)$ probably requires Euclid's algorithm. I'll spare you the arithmetic, but the answer turns out to be 439.

6. First, let me give a fairly naïve solution, close to what I did in class.

Here's Euclid's algorithm applied to compute $\gcd(493, 403)$:

$$494 = 403 \cdot 1 + 91 \tag{1}$$

$$403 = 91 \cdot 4 + 39 \tag{2}$$

$$91 = 39 \cdot 2 + 13 \tag{3}$$

$$39 = 13 \cdot 3 \tag{4}$$

Euclid therefore claims that $\gcd(494, 403) = 13$.

To show this, I want to show two things:

- (a) $13 \mid 403$ and $13 \mid 494$. This establishes that 13 is a common divisor of 403 and 494.
- (b) If c is any other common divisor of 494 and 403, then $c \mid 13$. This will imply that $c \leq 13$, so that 13 is the greatest of the common divisors.

To show claim (a), we work upward through equations (1–4), keeping track of what numbers we encounter are multiples of 13.

Equation (4) tells us that $13 \mid 39$.

Since $13 \mid 39$, it follows from a previous homework problem ($a \mid b \implies a \mid bc$) that $13 \mid (39 \cdot 2)$. Both terms on the right hand side of (3) are therefore multiples of 13, so a previous homework problem ($a \mid b$ and $a \mid c \implies a \mid (b + c)$) implies that $13 \mid (39 \cdot 2 + 13)$, i.e., that $13 \mid 91$.

Now apply the same reasoning to equation (2). Both terms on the right hand side of (2) are already known to be multiples of 13, so the left hand side must be, as well: $13 \mid 403$.

Finally, do it again with equation (1). Both terms on the right hand side of (1) are already known to be multiples of 13; so the left hand side must also be a multiple of 13: $13 \mid 494$.

The previous two paragraphs have established claim (a), that 13 is a common divisor of 494 and 403.

To address claim (b), it helps if we first rewrite equations (1–3) like this:

$$494 - 403 \cdot 1 = 91 \tag{1'}$$

$$403 - 91 \cdot 4 = 39 \tag{2'}$$

$$91 - 39 \cdot 2 = 13. \tag{3'}$$

Now suppose c is any common divisor of 494 and 403. Then both terms on the left hand side of (1') are multiples of c ; so the right hand side must also be a multiple of c : $c \mid 91$.

We now know that both terms on the left hand side of (2') are multiples of c ; so the right hand side must also be a multiple of c : $c \mid 39$.

Finally, we now know that both terms on the left hand side of (3') are multiples of c ; so the right hand side must also be a multiple of c : $c \mid 13$. This establishes claim (b), and therefore that $13 = \gcd(494, 403)$.

Now, a properly suspicious reader would rightly observe that showing a result for a single example hardly constitutes a general proof. On the other hand, it seems to me

that if one understands an example like this, one can see that we didn't use anything special about 494 and 403, and that exactly the same argument would apply no matter what our starting numbers were. It is certainly possible to write a general proof with letters by following this template, and to do so is a good exercise for anyone aspiring to be a mathematician and feeling themselves up to the task. I won't do that here, but I'd be happy to work through it with anyone who is interested. Now that the test is no longer on, you could also read what Andrews has to say about the question.

There is a better approach, though, and several of you found it. It comes from thinking of Euclid's Algorithm recursively. That is, Euclid says that if $b = 0$, then $\gcd(a, b) = |a|$. (This is obvious.) If $b \neq 0$, then write $a = bq + r$, $0 \leq r < b$. Euclid says

$$\gcd(a, b) = \gcd(b, r). \tag{5}$$

If we can establish equation (5), then recursion takes care of the rest.

To prove equation (5), we prove that in fact the common divisors of a and b are the same as the common divisors of b and r . After all, if d is a common divisor of b and r , then $d \mid bq$ and $d \mid r$; so $d \mid (bq + r)$. In other words, $d \mid a$; so d is a common divisor of a and b .

Conversely, if d is a common divisor of a and b , then $d \mid bq$; so $d \mid (a - bq)$. In other words, $d \mid r$; so d is a common divisor of b and r . Therefore, the common divisors of a and b are the same as the common divisors of b and r , and equation (5) is true. Since $0 \leq r < b$, the recursion must terminate after a finite number of steps with $r = 0$.

7. I'd start out and do the problem for primes and prime powers. If p is a prime, then

$$\begin{aligned} \nu(p^0) &= 1 \\ \nu(p^1) &= 1 \\ \nu(p^2) &= 2 \\ \nu(p^3) &= 2 \\ \nu(p^4) &= 3 \\ &\vdots \\ \nu(p^\alpha) &= 1 + \lfloor \alpha/2 \rfloor. \end{aligned}$$

Now let's look at what happens to a product of 2 prime powers. If p and q are distinct primes, then the squares dividing $p^\alpha q^\beta$ are exactly the products of the squares dividing p^α and the squares dividing q^β . That is,

$$\nu(p^\alpha q^\beta) = \nu(p^\alpha) \nu(q^\beta) = (1 + \lfloor \alpha/2 \rfloor)(1 + \lfloor \beta/2 \rfloor).$$

The obvious conjecture one would draw at this point is that

$$\nu(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = (1 + \lfloor \alpha_1/2 \rfloor)(1 + \lfloor \alpha_2/2 \rfloor) \cdots (1 + \lfloor \alpha_k/2 \rfloor)$$

It's possible to give a good inductive argument for this claim, but I'd be OK with students only getting this far on the problem.