

## Math 342 Tutorial

May 21, 2025

**Question 1.** Prove every integer  $n$  with  $|n| > 1$  is either prime or can be factored into a product of prime numbers [Hint: use the principle of strong mathematical induction].

We use induction, and we note it suffices to show the result for  $n > 0$ . Certainly, the result is true for  $n = 2$ . Next let  $n > 2$ . If  $n$  is prime, we're done. If  $n$  is composite, then there exists  $a, b \neq 1$  such that  $n = ab$ . But  $1 < a, b < n$  so that  $a$  and  $b$  are either prime or a product of prime numbers. But then  $n = ab$  is a product of prime numbers. By the principle of strong mathematical induction, the result follows.

**Question 2.** Use Question 1 to show there are infinitely many prime numbers [Hint. use contradiction and consider the number  $N = 1 + p_1 \cdots p_n$  where  $p_1, \dots, p_n$  are the assumed finite number of primes].

Towards a contradiction, assume there are only a finite number of primes, say  $p_1, \dots, p_n$ . Define  $N = 1 + p_1 \cdots p_n$ . From Question 1, either  $N$  is a prime or a product of primes. But  $N > p_i$  for all  $i \in \{1, \dots, n\}$ , hence  $N$  cannot be prime. Therefore,  $N$  is a product of the primes  $p_1, \dots, p_n$ . Observe, however, that no prime  $p_1, \dots, p_n$  can divide  $N$  for if some  $p_i \mid N$ , then  $p_i \mid 1$  which cannot be. So  $N$  cannot be a product of the primes  $p_1, \dots, p_n$ , a contradiction. This establishes the result.

**Question 3.** The gcd of a multiset  $\{a_1, \dots, a_n\}$  of integers is defined inductively by  $(a_1, a_2, \dots, a_n) = (a_1, (a_2, \dots, a_n))$ . Show (a) the gcd of  $\{a_1, \dots, a_n\}$  is independent of the ordering chosen for the elements of the set, and (b) there exists integers  $x_1, \dots, x_n$  such that  $(a_1, a_2, \dots, a_n) = x_1 a_1 + \cdots + x_n a_n$ .

(a) We show the following by induction:

- (1)  $(a_1, \dots, a_n) \mid a_i$  for each  $1 \leq i \leq n$ , and
- (2) if any  $d \mid a_i$  for each  $1 \leq i \leq n$ , we have  $d \mid (a_1, \dots, a_n)$ .

In particular, we start by showing that  $(a_1, \dots, a_n)$  is the largest common divisor of  $a_1, \dots, a_n$ . The base case ( $n = 2$ ) was shown in class. Let  $n > 2$ , and assume the result for  $n - 1$ , that is, the result holds for every multisubset of  $\mathbf{Z}$  of cardinality  $n - 1$ . Let  $\{b_1, \dots, b_n\}$  be an arbitrary multisubset of  $\mathbf{Z}$ . Since

$$(b_1, \dots, b_n) = (b_1, (b_2, \dots, b_n)),$$

we have that  $(b_1, \dots, b_n)$  divides both  $b_1$  and  $(b_2, \dots, b_n)$ . Since  $(b_2, \dots, b_n)$  divides each of  $b_2, \dots, b_n$ , so does  $(b_1, \dots, b_n)$ . This shows (1) holds for  $\{b_1, \dots, b_n\}$ . Next, let  $d$  be such that  $d \mid a_i$  for each  $1 \leq i \leq n$ . Since then  $d \mid b_i$  for  $i \geq 2$ , we have that  $d \mid (b_2, \dots, b_n)$  by the inductive hypothesis. Since  $d \mid b_1$  and  $d \mid (b_2, \dots, b_n)$ , we have that  $d \mid (b_1, (b_2, \dots, b_n)) = (b_1, \dots, b_n)$ . This shows that (2) holds for  $\{b_1, \dots, b_n\}$ . Since  $\{b_1, \dots, b_n\}$  was an arbitrary multisubset of  $\mathbf{Z}$  of cardinality  $n$ , it holds for every multisubset of cardinality  $n$ . It now follows that (1) and (2) hold for every multisubset of  $\mathbf{Z}$  of finite order by induction.

Let  $\{a_1, \dots, a_n\}$  be an arbitrary multisubset of  $\mathbf{Z}$ , and let  $\sigma$  be an arbitrary permutation of  $\{a_1, \dots, a_n\}$ . From (1) and (2) above, we have that both  $(a_1, \dots, a_n) \mid (\sigma(a_1), \dots, \sigma(a_n))$  and  $(\sigma(a_1), \dots, \sigma(a_n)) \mid (a_1, \dots, a_n)$ . Therefore,  $(a_1, \dots, a_n) = (\sigma(a_1), \dots, \sigma(a_n))$  as these are both positive values by assumption. Since  $\{a_1, \dots, a_n\}$  and  $\sigma$  were arbitrary, the result follows.

(b) Note the logical form of the proposition we are required to prove. We must show for all  $n > 1$ , the result holds for every multisubset of  $\mathbf{Z}$  of cardinality  $n$ . We have shown the base case—that is,  $n = 2$ —in class already. Let  $n > 2$ , and suppose the result holds for  $n - 1$ ; namely, for every multisubset  $\{a_1, \dots, a_{n-1}\}$  of  $\mathbf{Z}$  of cardinality  $n - 1$ , there exists integers  $x_1, \dots, x_{n-1}$  such that

$a_1x_1 + \cdots + a_{n-1}x_{n-1} = (a_1, \dots, a_{n-1})$ . Let  $\{b_1, \dots, b_n\}$  be an arbitrary multisubset of  $\mathbf{Z}$  of cardinality  $n$ . From the base case, there exists integers  $y_1, y_2$  such that

$$(b_1, \dots, b_n) = (b_1, (b_2, \dots, b_n)) = y_1b_1 + y_2(b_2, \dots, b_n).$$

From the inductive hypothesis, there exists integers  $z_2, \dots, z_n$  such that

$$(b_2, \dots, b_n) = z_2b_2 + \cdots + z_nb_n.$$

Putting things together, we have

$$\begin{aligned} (b_1, \dots, b_n) &= (b_1, (b_2, \dots, b_n)) \\ &= y_1b_1 + y_2(b_2, \dots, b_n) \\ &= y_1b_1 + y_2z_2b_2 + \cdots + y_2z_nb_n. \end{aligned}$$

Since  $\{b_1, \dots, b_n\}$  was chosen arbitrarily, the result holds for every multisubset of cardinality  $n$  as well. The result now follows from the principle of mathematical induction.

**Question 4.** Let  $p$  be a prime. Show that if  $p \mid ab$  then  $p \mid a$  or  $p \mid b$ .

Suppose that  $p$  divides neither  $a$  nor  $b$  but  $p \mid ab$ . In particular,  $(a, p) = (b, p) = 1$ . Hence, there exists integers  $w, x, y$ , and  $z$  such that

$$1 = wp + xa = yp + zb.$$

Then

$$1 = (wp + xa)(yp + zb) = wyp^2 + (wzb + xay)p + xzab.$$

Since  $p \mid ab$  by assumption, we have that  $p \mid wyp^2 + (wzb + xay)p + xzab = 1$ , a contradiction. Therefore,  $p$  does not divide  $ab$ .

**Question 5.** If  $(a, b) = 1$ , then  $(a + b, a - b) = 1$  or  $2$ .

Let  $d = (a + b, a - b)$ . We have that  $d \mid a + b$  and  $d \mid a - b$ . Therefore,  $d \mid (a + b) + (a - b) = 2a$  and  $d \mid (a + b) - (a - b) = 2b$ . By assumption, there exists integers  $x, y$  such that  $ax + by = 1$  so that  $2ax + 2by = 2$ . Since  $d \mid 2a, 2b$ , it must be that  $d \mid 2ax + 2by = 2$ . Therefore,  $d = 1$  or  $2$  (up to negation).

**Question 6.** If  $(a, b) = 1$ , then  $(a + b, a^2 - ab + b^2) = 1$  or  $3$ .

Let  $d = (a + b, a^2 - ab + b^2)$ , and note that  $d = (a + b, a^2 - ab + b^2) = (a + b, (a + b)^2 - 3ab) = (a + b, 3ab)$ . Suppose that  $d > 1$  and  $p$  is a prime divisor of  $d$ . Then  $p \mid a + b$ , and either  $p \mid 3$  or  $p \mid a$  or  $p \mid b$ . If  $p \mid a$ , then  $p \mid (a + b) - a = b$  contradicting the fact that  $a$  and  $b$  are coprime. Thus,  $p$  does not divide  $a$ . Similarly,  $p$  does not divide  $b$ . Hence,  $p$  divides  $3$ . But  $3$  is prime so that  $p = 3$ . We have, therefore, that  $d = 1$  or  $3^k$  for some  $k > 0$ . Suppose next that  $k > 1$ . The single prime divisor  $3$  of  $d = 3^k$  must divide  $3ab$ . But we have already seen that  $3$  cannot divide  $a$  or  $b$ , so it must (trivially) divide the remaining factor  $3$ . Inductively,  $d = 3^k \mid 3$ , contradicting the the assumption that  $k > 1$ . We finally have that  $d = 1$  or  $3$ .

**Question 7.** If  $(a, b) = 1$ , then  $(a^n, b^k) = 1$  for all  $n, k \geq 1$ .

Recall that  $(a, b) = 1$  if and only if  $a$  and  $b$  have no common factors that are not  $1$ . Let  $n, k > 1$  be given, and suppose that  $(a^n, b^k) = d$  with  $d > 1$ . Let  $p$  be a prime divisor of  $d$ . Then  $p \mid a^n, b^k$ ; in

particular,  $p \mid a, b$ , a contradiction. Therefore,  $d = 1$ .

**Question 8.** If  $2^n - 1$  is a prime, then  $n$  is a prime.

Towards a contradiction, suppose that  $n$  is composite, say  $n = xy$  with  $1 < x, y < n$ . Then

$$2^{xy} - 1 = (2^x - 1)(2^{x(y-1)} + 2^{x(y-2)} + \dots + 2^x + 1).$$

However,  $2^x - 1 > 1$  since  $x > 1$ , hence  $2^x - 1$  is a nontrivial divisor of  $2^n - 1$ . This contradicts the assumption that  $2^n - 1$  is prime; thus, it must be that  $n$  is prime.

**Question 9.** If  $2^n + 1$  is a prime, then  $n$  is a power of 2.

Towards a contradiction, suppose that  $n = 2^k m$  with  $m > 1$  odd. Then

$$2^{2^k m} + 1 = (2^{2^k})^m + 1 = (2^{2^k} + 1)(2^{2^k(m-1)} - 2^{2^k(m-2)} + \dots - 2^{2^k} + 1).$$

But  $2^{2^k} + 1 \geq 2$ . Since  $m > 1$ , we have that  $2^{2^k m} + 1 > 2^{2^k} + 1$  and  $2^{2^k(m-1)} - 2^{2^k(m-2)} + \dots - 2^{2^k} + 1 > 1$ . We have exhibited factorization of  $2^n + 1$  into a product of two nontrivial divisors contradicting the assumption that  $2^n + 1$  is prime. Therefore,  $m = 1$  and  $n$  is a power of 2.

**Question 10.** (a) Suppose that  $(a, b) = (c, d) = 1$  and  $\frac{a}{b} + \frac{c}{d} = n$  is an integer. Show  $|b| = |d|$ .  
(b) Prove the sum  $\sum_{k=1}^n \frac{1}{k}$  is not an integer for  $n > 1$  [Hint. show the sum can be written as  $\frac{a}{b}$  with  $a$  and  $b$  of opposite parity].

(a) We have that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = n.$$

In particular, we have that  $bd \mid ad + bc \Rightarrow b \mid ad + bc \Rightarrow b \mid ad$ . Since  $(a, b) = 1$ , it follows that  $b \mid d$ . Similarly,  $d \mid b$ . Thus,  $|b| = |d|$ .

(b) We claim the sum always evaluates to a fraction  $\frac{a}{b}$  with  $a$  odd and  $b$  even. The proof is by induction on  $n$ . For  $n = 2$ , we have  $1 + \frac{1}{2} = \frac{3}{2}$ , so the base case holds. Let  $n > 2$  be given, and suppose the result holds for all  $m$  with  $m < n$  and  $m > 2$ . Partitioning the sum  $\sum_{k=1}^n \frac{1}{k}$  into whether the denominator is even or odd, we find that

$$\sum_{k=1}^n \frac{1}{k} = 1 + \dots + \frac{1}{k} = \sum_{k=2}^{\lfloor n/2 \rfloor} \frac{1}{2k-1} + \frac{1}{2} \sum_{k=1}^{\lfloor n/2 \rfloor} \frac{1}{k}.$$

By our inductive hypothesis, we can write  $\frac{1}{2} \sum_{k=1}^{\lfloor n/2 \rfloor} \frac{1}{k}$  as  $\frac{a}{b}$  with  $a$  odd and  $b$  even. Next, observe that  $\sum_{k=2}^{\lfloor n/2 \rfloor} \frac{1}{2k-1} = \frac{f(k)}{(2k-1)!!}$  where  $f(k)$  is a polynomial in  $k$ . Since  $(2k-1)!!$  is odd, it follows that  $\sum_{k=2}^{\lfloor n/2 \rfloor} \frac{1}{2k-1} = \frac{f(k)}{(2k-1)!!}$  can be written as  $\frac{c}{d}$  with  $d$  odd. Then

$$\sum_{k=1}^n \frac{1}{k} = \frac{c}{d} + \frac{a}{b} = \frac{cb + ad}{db}.$$

Since  $a$  and  $d$  are odd,  $ad$  is odd. Also,  $cb$  is even as  $b$  is even. Therefore,  $cb + ad$  is odd. Finally,  $db$  is even as  $b$  is even. Thus, the result holds for  $n$  as well and the proposition follows by the strong principle of mathematical induction.

**Question 11.** Prove: **(a)** For every integer  $k$  the numbers  $2k + 1$  and  $9k + 4$  are relatively prime. **(b)** For every integer  $k$ , express the gcd of  $2k - 1$  and  $9k + 4$  as a function of  $k$ .

**(a)** We solve  $x(2k + 1) + y(9k + 4) = 1$ . This leads to the system  $2x + 9y = 0$ ,  $x + 4y = 1$  of linear equations. This system has the unique solution  $x = 9$  and  $y = -2$ . Therefore  $9(2k + 1) - 2(9k + 4) = 1$ , which shows  $(2k + 1, 9k + 4) = 1$ .

**(b)** We have

$$(2k-1, 9k+4) = (2k-1, 4(2k-1)+(k+8)) = (k+8, 2k-1) = (k+8, 2(2k-1)-17) = (k+8, 17).$$

So  $(2k - 1, 9k + 4) = 1$  or  $17$ . But  $(2k - 1, 9k + 4) = 17$  if and only if  $k = 17m + 9$  for some integer  $m$ . In all other cases,  $(2k - 1, 9k + 4) = 1$ .

**Question 12.** Prove that for positive integers  $m$  and  $a$  we have

$$\left( \frac{a^m - 1}{a - 1}, a - 1 \right) = (a - 1, m).$$

Let  $d = \left( \frac{a^m - 1}{a - 1}, a - 1 \right)$ , and observe

$$\begin{aligned} \frac{a^m - 1}{a - 1} &= a^{m-1} + a^{m-2} + \cdots + a + 1 \\ &= (a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1) + m. \end{aligned}$$

Since  $a - 1 \mid a^k - 1$  for  $k \geq 0$ , we have that  $d \mid m$  whereupon  $d \mid (a - 1, m)$ . Conversely, since  $(a, m) \mid a - 1, m$ , it follows that  $(a, m) \mid \frac{a^m - 1}{a - 1}$  and hence  $(a, m) \mid \left( \frac{a^m - 1}{a - 1}, a - 1 \right) = d$ . Thus  $d = (a - 1, m)$ .