# Problem Set 5,6 Solutions

Questions? Corrections? email jjudge@uchicago.edu (John)

edited by Subhadip Chowdhury

*The University of Chicago, CAAP 2018: Proof-Based Methods in Calculus (Chowdhury)*

July 13, 2018

## Exercise 1: Divisibility Properties

**Problem 1.1.** *For each of the following statements, either prove it is true or provide an example that shows it is not true. Be brief about the proof, don't worry about the format too much; make sure that the mathematical reasoning is correct.*

*(a) If $a|c$ and $b|c$, then $ab|c$.*
*(b) If $2a|4b$, then $a|b$.*
*(c) If $a|b$, then $a^2|b^3$*
*(d) If $a|b$, then $(a+2)|(b+2)$.*
*(e) If $a|b$ and $c|d$, then $ac|bd$.*
*(f) If $ab|c$, then $a|c/b$*

(a) False

*Proof.* Take $a = 3$, $b = 3$, and $c = 3$. Then $3|3$, but 9 does not divide 3. □

(b) False.

*Proof.* Take $a = 6$ and $b = 3$. Then $12|12$, but 6 does not divide 4. □

(c) True

*Proof.* If $a|b$, then there is an integer $n$ such that $an = b$. Cubing both sides, we get $a^3n^3 = b^3$, or $a^2(an^3) = b^3$. As $an^3$ is an integer, $a^2|b^3$.

□

(d) False

*Proof.* Take $a = 2$, $b = 4$. Then $2|4$, but 4 does not divide 6. □

(e) True

*Proof.* If $a|b$ and $c|d$, then there exists integers $m$, $n$ such that $an = b$ and $cm = d$. If both right sides are multiplied together and both left sides are multiplied together, then the two equated, we have that $an \times cm = bd$. Since $nm$ is an integer (integers are closed under multiplication), we find that $ac|bd$. □

(f) True

*Proof.* If $ab|c$, then there is an integer $n$ such that $abn = c$. We can divide both sides of $abn = c$ by $b$, which must be non-zero by the problem statement. Then[1] $an = \frac{c}{b}$, and $n$ is an integer. Hence $a|\frac{c}{b}$. □

## Exercise 2: Divisibility and GCD Properties

**Problem 2.1.** *For each of the following statements, either prove it is true or provide an example that shows it is not true.*

*(a) If* $(a, b) = 1$ *and* $(b, c) = 1$*, then* $(a, c) = 1$.
*(b) If* $n|(a, b)$*, then* $n|a$ *and* $n|b$.

(a) False.

*Proof.* Consider $a = c = 3$ and $b = 7$. Then $(3, 7) = 1$ and $(7, 3) = 1$. But $(3, 3) = 3 \neq 1$. □

(b) True.

*Proof.* We have that $n|(a, b)$. We also have that $(a, b)|a$, which is required by the definition of GCD. By the transitive property of divisibility[2], we find that we have $n|a$. By similar reasoning, we find $n|b$. □

## Exercise 3: GCD Addition

**Problem 3.1.** *For any integers a, b, and c, show that* $(a + bc, b) = (a, b)$.

I will present two proofs of this theorem. The first is modeled after the proof of Theorem 3.7.2 in Hermann & Sally. The second is by contradiction, and makes a good example of using the extremal principle.

*Proof.* Suppose the set $S_1$ is the set of common divisors of $a$ and $b$, and the set $S_2$ is the set of common divisors of $a + bc$ and $b$. If we can show that $S_1 = S_2$, then we can conclude that both sets have the same greatest element. We will do this by showing that every element of $S_2$ is in $S_1$, and that every element of $S_1$ is in $S_2$.

Now, for every $f \in S_2$, $f|b$, so $f|(-cb)$ by the fourth property listed in the Assignment 5 notes. We can use the additive property of divisibility to find that, since $f|(a + cb)$ and $f|(-cb)$, we know $f|(a + cb) + (-cb)$, or $f|a$. Hence $f \in S_1$. So every element of $S_2$ is an element of $S_1$.

Now, for every $f \in S_1$, we similarly have $f|cb$. Moreover, again using the the additive property, since $f|a$ and $f|cb$, we know $f|(a + cb)$. Hence $f \in S_2$. So every element of $S_1$ is an element of $S_2$. □

1. You are not required to show $\frac{c}{b}$ is an integer. But it is, since $an$ is an integer.
2. Transitive Property of Divisibility was proved in class.

*Proof.* Suppose $d = (a, b)$, then $\exists n, m \in \mathbb{Z}$ such that $dn = a$ and $dm = b$, where $d$ is the greatest such integer.Then consider $a + bc = dn + dmc = d(n + mc)$. So $d$ is a common factor of $a + bc$ and $b$. Now it remains to show that no greater common factor exists.

Suppose there exists a greater common factor $e = (a + bc, b)$, where $e > d$. Then $\exists n', m' \in \mathbb{Z}$ such that $en' = a + bc$ and $em' = b$. Subtraction of $bc$ to both sides of the prior equation, and substitution of the latter equation for $b$, gives $en' - cem' = a$, or $a = e(n' - cm')$. This means that $e$ divides $a$. Moreover, $e|b$, so $e$ is a common factor of $a$ and $b$, and $e > d$. But this is a contradiction, as $d$ was supposed to be the greatest common factor of $a$ and $b$.

□

## Exercise 4: GCD of Consecutive Integers

**Problem 4.1.** *Using Exercise* 3*, show that* $(n, n + 1) = 1$ *for any integer* $n$*.*

*Proof.* Suppose, for the sake of contradiction, that there exists $k \in \mathbb{N}$ such that $k|n$ and $k|(n + 1)$, and yet $k > 1$. Then, there are integers $a, b$ such that $n = ak$ and $(n + 1) = bk$. Then, consider

$$(n + 1) - n = bk - ak$$

The right side is $(b - a)k$, and $(b - a) \in \mathbb{Z}$ means that $k$ divides the expression on the left side. But the left side is just 1. But $k > 1$, so $k$ cannot divide 1. This contradiction completes the proof.[3] □

## Exercise 5: Triple Primes

**Problem 5.1.** *The set of primes* $3, 5, 7$ *is the only set of triple primes.*

As mentioned in class, for this problem you do not need to include proof that every third consecutive odd integer is divisible by three. But can you prove it by induction?

*Proof.* We observe that every third odd integer is divisible by three. In particular, we mean that between every two consecutive odd integers *that are divisible by* 3, there are exactly two consecutive odds that are *not* divisible by 3. Now, choose any three consecutive odd integers $a$, $b$, and $c$. Suppose by contradiction that none of them is divisible by 3. Thus, there are two possible locations for $a$, $b$, and $c$, between the preceding and following odds that are divisible by three. By Pigeonhole Principle, at least two of $a$, $b$, and $c$ are the same odd integer not divisible by three. But if they are the same integer, they are not consecutive. This is a contradiction.

Thus one of the triple primes must be divisible by 3, and hence it has to be 3 itself. So the only example is $\{3, 5, 7\}$. □

You did not need to use PHP or proof by contradiction in your solution. The following, shorter proof would have been fine:

*Proof.* We observe that every third odd integer is divisible by three. In particular, we mean that between every two consecutive odd integers *that are divisible by* 3, there are exactly two consecutive odds that are *not* divisible by 3. But we can only choose at most 2 consecutive odd integers not divisible by 3.

3. Alternately, we can plug in $a = 1, b = n$, and $c = 1$ in to exercise 3 to get $(n, n + 1) = (n, 1) = 1$.

Thus one of the triple primes must be divisible by 3, and hence it has to be 3 itself. So the only example is $\{3, 5, 7\}$.

□

## Exercise 6: Smallest Prime Factor

**Problem 6.1.** *Show that if $p$ is the smallest prime factor of $n \in \mathbb{N}$, and $p > \sqrt[3]{n}$, then $\frac{n}{p}$ is either a prime or equal to* 1.

*Proof.* Since $p|n$, there is an integer $x$ such that $xp = n$. For the sake of contradiction, suppose $x$ is composite. Then, multiplying both sides of the inequality in the hypothesis by $x$, we get

$$xp > x\sqrt[3]{n}$$

Substitute $xp = n$, and observe that the inequality holds when both sides are cubed:

$$n^3 > x^3 n \tag{1}$$

Since $n > 0$, we can say $n^2 > x^3$, and furthermore that $n^{2/3} > x$. Taking the square root of both sides, $\sqrt[3]{n} > \sqrt{x}$. Since the hypothesis requires $p > \sqrt[3]{n}$, we also have $p > \sqrt{x}$. Now, $x$ is composite, so it must have some prime factor $q$ which, as we proved in class, can be at most $\sqrt{x}$, i.e. $q \leq \sqrt{x}$ Combining this with previous inequalities, we find $q > p$. But since $x|n$, we must have that $q|n$ (transitive property of divisibility, from class). Then $q$ is a factor of $n$ and it is less than $p$, which was supposed to be the smallest prime factor of $n$. This is a contradiction.

□

Here is another proof that Professor Subhadip came up with.

*Proof.* Assume, for the sake of contradiction, that $\frac{n}{p}$ is neither a prime, nor equal to 1, i.e. $\frac{n}{p}$ is a composite integer. Then $\frac{n}{p}$ must have a prime factor, call it $q$.

Since $q \mid \frac{n}{p}$ and $\frac{n}{p} \mid n$ (since $n = \frac{n}{p} \times p$), by transitive property we get that $q \mid n$. But $p$ is the smallest prime factor of $n$, hence $q > p$.

Now since $q \mid \frac{n}{p}$, we get that $r = \frac{n}{pq}$ is an integer. In fact, since $n = r \times (pq)$, we get that $r$ is a factor of $n$. Note that $r > 1$, since $\frac{n}{p}$ not a prime implies $\frac{n}{p} \neq q$. Now $r$ may or may not be prime, but in either case, $r > p$. This is because $p$ is the smallest factor of $n$, bigger than 1.

To conclude we have

$$n = p \times q \times r \geq p \times p \times p = p^3 \implies \sqrt[3]{n} > p$$

which is a contradiction.

□

## Exercise 7: Consecutive Composites

**Problem 7.1.** *Can you find* 3 *consecutive composite integers? How about four? Five? Can you find a formula that will produce n consecutive composite integers?*

**Solution 1.** *These are five consecutive composites:*

**Theorem 7.2.** *$\forall n \in \mathbb{N}$ s.t. $n \geq 3$, the following set contains n consecutive composite integers:*

$$\{(n+1)!+2, (n+1)!+3, (n+1)!+4, (n+1)!+5, ..., (n+1)!+n+1)\}$$

*Proof.* Express the elements in the above set as $S = \{(n+1)!+i \mid 2 \leq i \leq n+1\}$. Observe that any integer $i$, such that $2 \leq i < (n+1)$, is a factor of $(n+1)! = 1 \times 2 \times 3 \times ... \times (n+1)$. That is, we know $i|(n+1)!$ when $2 \leq i < (n+1)$. Moreover, since $(n+1) > 3$, by the additive property of divisibility, we know that $i|\{(n+1)!+i\}$. Therefore, the $i^{th}$ term in $S$ is divisible by $i$. Clearly cardinality of $S$ is $n$. Hence $S$ contains $n$ consecutive composites. □

# Exercise 8: Euclidean Algorithm

**Problem 8.1.** *Suppose c and d are positive integers such that $c = dq + r$ for some integers q and r. Then show that $(c, d) = (d, r)$.*

*Proof.* Note that $r = c - dq$. Then by the Theorem in Exercise 3, for any integers $c$, $d$, and $-q$,[4] we have that $(c + d(-q), d) = (c, d) \implies (c, r) = (c, d)$.

□

# Exercise 9: Factor Large Composites (Extra Credit)

**Problem 9.1.** *(a) Factor $a^4 + 4b^4$*
*(b) Show that $4^{545} + 545^4$ is not a prime number.*
*(c) Show that $n^4 + 4^n$ is not a prime number for any natural number n.*

*(a) The Sophie Germain identity states that*

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$$

*Proof.* Consider completing the square for $a^4 + 4b^4$, which gives:

$$\begin{aligned} a^4 + 4b^4 &= a^4 + 4b^4 + 4a^2b^2 - 4a^2b^2 \\ &= (a^4 + 4a^2b^2 + 4b^4) - 4a^2b^2 \\ &= (a^2 + 2b^2)^2 - (2ab)^2 \end{aligned}$$

The difference of squares can be then factored to get

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$$

□

*(b)*

$$\begin{aligned} &4^{545} + 545^4 \\ &= 545^4 + 4(4^{544}) \\ &= 545^4 + 4(4^{136})^4 \end{aligned}$$

4. i.e. we are plugging in $c$, $d$ and $-q$ in the places of $a$, $b$, and $c$, respectively.

*Applying the Sophie Germain identity for* $a = 545$ *and* $b = 4^{136}$*, the original expression becomes*

$$\left(\left(545^4\right)^2 + 2\left(4^{136}\right)^2 + 2\left(545^4\right)\left(4^{136}\right)\right) \times \left(\left(545^4\right)^2 + 2\left(4^{136}\right)^2 - 2\left(545^4\right)\left(4^{136}\right)\right)$$

*which is a product of two factors greater than* 1.
*(c)*

*Proof.* Consider $a = n$ and $b = 4^{\frac{n-1}{4}}$ (we have pulled out a factor of 4 and then lowered the exponent by a factor of 4, turning the second term from $4^n$ into $4(4^{n-1}$ and then into $4(4^{\frac{n-1}{4}})^4$, which looks like $4b^4$. If $n$ is odd, then $b$ is an integer, and we can apply the Sophie Germain identity to factor the expression $n^4 + 4^n$, and get

$$\left(n^2 + 2\left(4^{\frac{n-1}{4}}\right)^2 + 2n(4^{\frac{n-1}{4}})\right)\left(n^2 + 2\left(4^{\frac{n-1}{4}}\right)^2 - 2n(4^{\frac{n-1}{4}})\right)$$

which is a product of two integer factors greater than 1.
Now, if $n$ is even, then $n^4 + 4^n$ is also even (any even integer to a positive integer power is also even; moreover, a sum of even integers is also even), and therefore has 2 as a factor.

□