

# EGMO Solutions

Kempu33334

July 2025

## Contents

<b>1 Fundamentals of Number Theory</b>	<b>2</b>
1.1 Divisibility . . . . .	2
1.2 Divisibility Properties . . . . .	2
1.3 Euclid's Division Lemma . . . . .	2
1.4 Primes . . . . .	2
1.5 Looking at Numbers as Multisets . . . . .	3
1.6 GCD and LCM . . . . .	3
1.7 Euclid's Division Algorithm . . . . .	4
1.8 Bézout's Theorem . . . . .	4
1.9 Base Systems . . . . .	5
1.10 Extra Results as Problems . . . . .	6
1.11 Example Problems . . . . .	6
1.12 Practice Problems . . . . .	6

# 1 Fundamentals of Number Theory

## 1.1 Divisibility

*No problems.*

## 1.2 Divisibility Properties

### Problem 1.2.1

Show that if  $n > 1$  is an integer,  $n \nmid 2n^2 + 3n + 1$ .

Assume there exists such an  $n$ . Then, subtracting  $n(2n+3)$  from the RHS of the condition, we find that  $n \nmid 1$ , so  $n = 1$  or  $-1$ , which is a contradiction.  $\square$

### Problem 1.2.2

Let  $a > b$  be natural numbers. Show that  $a \nmid 2a + b$ .

Assume for the sake of contradiction there exists  $a > b$  where  $a \mid 2a + b$ . Then,  $a \mid b$ , implying that  $a \leq b$ , which is a contradiction.  $\square$

### Problem 1.2.3

For 2 fixed integers  $x, y$ , prove that

$$x - y \mid x^n - y^n$$

for any non-negative integer  $n$ .

Clearly, the statement is equivalent to  $x^n - y^n \pmod{x-y} \equiv 0$ . However, we can write that

$$x^n - y^n \equiv (x - (x-y))^n - y^n \equiv 0 \pmod{x-y}$$

as required.  $\square$

## 1.3 Euclid's Division Lemma

*No problems.*

## 1.4 Primes

### Problem 1.4.1

Find all positive integers  $n$  for which  $3n - 4$ ,  $4n - 5$ , and  $5n - 3$  are all prime numbers.

In order for  $5n - 3$  to be prime, we must have  $n$  even or  $n = 1$ . Hence, make the transformation  $n = 2n'$ . Then,  $3n - 4 \mapsto 6n' - 4$ , which can never be prime other than when  $n = 2$ . Trying both  $n = 1$  and  $n = 2$ , we find that only  $n = \boxed{2}$  works.  $\square$

**Problem 1.4.2**

If  $p < q$  are two consecutive odd prime numbers, show that  $p + q$  has at least 3 prime factors (not necessarily distinct).

Clearly, it cannot have zero or one prime factor. If it has two prime factors, then we can express

$$p + q = rs$$

for some primes  $r$  and  $s$ . However, we know that one of these has to be 2, hence WLOG assume it is  $r$ . Then,

$$\frac{p+q}{2} = s$$

which implies that there exists a prime between  $p$  and  $q$ , which contradicts the fact that they are consecutive, as required.  $\square$

## 1.5 Looking at Numbers as Multisets

*No problems.*

## 1.6 GCD and LCM

**Problem 1.6.1**

Prove that  $\gcd(a, b) = a$  if and only if  $a \mid b$ .

We start with the if direction. Clearly, if  $a = 2^{a_1}3^{a_2}\dots$  and  $b = 2^{b_1}3^{b_2}\dots$ , then the divisibility condition implies  $a_i \leq b_i$  for all  $i \geq 1$ . Hence,

$$\min(a_i, b - i) = a_i$$

which proves the claim.

For the only if direction, we know that  $\min(a_i, b_i) = a_i$  for any  $i \geq 1$ , implying that  $a_i \leq b_i$ , which proves the desired result.  $\square$

**Problem 1.6.2**

If  $p$  is a prime, prove that  $\gcd(a, p) \in \{1, p\}$ .

Clearly, the only divisors of  $p$  are 1 and  $p$ .  $\square$

**Problem 1.6.3**

Let  $a, b$  be relatively prime. Show that if  $a \mid c, b \mid c$ , then  $ab \mid c$ .

This is clear since  $ab = \gcd(a, b) \operatorname{lcm}(a, b) = \operatorname{lcm}(a, b) \mid c$ .  $\square$

**Problem 1.6.4**

Prove that if  $p$  is a prime with  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .

Clearly, if  $p \nmid a$  and  $p \nmid b$ , then  $p \nmid ab$ , which is a contradiction.  $\square$

## 1.7 Euclid's Division Algorithm

### Problem 1.7.1

Find  $\gcd(120, 500)$  using the algorithm.

We have that

$$\gcd(120, 500) = \gcd(120, 20) = [20].$$

□

### Problem 1.7.2

Show that  $\gcd(4n + 3, 2n) \in \{1, 3\}$ .

We note that

$$\gcd(4n + 3, 2n) = \gcd(3, 2n)$$

which implies the conclusion. □

### Problem 1.7.3

Let  $a, b$  be integers. We can write  $a = bq + r$  for integers  $q, r$  where  $0 \leq r < b$ . Then our lemma states that

$$\gcd(a, b) = \gcd(r, b).$$

However, is  $\text{lcm}(a, b) = \text{lcm}(r, b)$ ?

No. If so, then multiplying the two, we have that

$$ab = rb \implies a = r$$

which cannot be true. □

## 1.8 Bézout's Theorem

### Problem 1.8.1

Let  $a, b, x, y, n$  be integers such that

$$ax + by = n.$$

Prove that  $\gcd(a, b)$  divides  $n$ .

Clearly, since  $\gcd(a, b)$  divides the LHS, it must also divide the RHS, as required. □

### Problem 1.8.2

Let  $(a, b) = (8, 12)$ . Find  $x, y \in \mathbb{Z}$  such that

$$ax + by = \gcd(a, b).$$

It suffices to find  $x$  and  $y$  satisfying

$$2x + 3y = 1$$

and clearly,  $(x, y) = \boxed{(2, -1)}$  works.  $\square$

### Problem 1.8.3

Let  $(a, b) = (7, 12)$ . Find  $x, y \in \mathbb{Z}$  such that

$$ax + by = \gcd(a, b).$$

We must find  $x$  and  $y$  where

$$7x + 12y = 1$$

but clearly  $(x, y) = (7, -4)$  works, so we are done.  $\square$

## 1.9 Base Systems

### Problem 1.9.1

Find 37 in base 5. Find 69 in base 2.

The former is 122<sub>5</sub>, and the latter is 1000101<sub>2</sub>.  $\square$

### Problem 1.9.2

Show that any power of 2 is of the form 100...0<sub>2</sub>.

This is clear, since  $2^n$  will be expressed as 1  $\underbrace{00\dots0}_{n \text{ times}}$ .

### Problem 1.9.3

Prove in general that if  $n = a_0 \times \ell^0 + \dots + a_k \times \ell^k$ , then  $k$  is such that  $\ell^k \leq n < \ell^{k+1}$  and  $a_k$  is such that  $a_k \ell^k \leq n < (a_k + 1) \ell^k$ .

Clearly, since  $a_k \geq 1$ , we have that  $\ell^k \leq n$ . In addition, since  $a_{k+1} = 0$ , we have the other bound. Now, for the latter statement, the lower bound is obvious. The upper bound can be shown by considering that  $a_i < \ell$  for all  $i$  and using the geometric series formula.

### Problem 1.9.4

Let  $k = \lfloor \log_\ell(n) \rfloor$ . Show that  $n$  has exactly  $k + 1$  digits in base  $\ell$ .

Note that since

$$\ell^k = \ell^{\lfloor \log_\ell(n) \rfloor} \leq n$$

we know that  $n$  has at least  $k + 1$  digits in base  $\ell$ . In addition,

$$\ell^{k+1} = \ell^{\lfloor \log_\ell(\ell n) \rfloor} > \ell^{\log_\ell(\ell n) - 1} = n$$

which shows that there are at most  $k + 1$  digits, as required.  $\square$

## 1.10 Extra Results as Problems

### Problem 1.10.1

Prove that if  $ab = cd$ , then  $a + b + c + d$  is not a prime number.

Substitute  $a = pq$ ,  $b = rs$ ,  $c = pr$ , and  $d = qs$ . Then,

$$a + b + c + d = pq + pr + qs + rs = (q + r)(p + s)$$

so we are done.  $\square$

## 1.11 Example Problems

*No problems.*

## 1.12 Practice Problems

### Problem 1.12.1

Show that any composite number  $n$  has a prime factor  $\leq \sqrt{n}$ .

Assume not. Then, since  $n$  has at least two prime factors, consider any two of them, say  $p$  and  $q$ . Since  $pq \leq n$ , we know that  $p$  and  $q$  cannot both be greater than  $\sqrt{n}$ , so at least one of them is  $\leq \sqrt{n}$ , contradiction.  $\square$

### Problem 1.12.2 (IMO 1959/1)

Prove that for any natural number  $n$ , the fraction

$$\frac{21n+4}{14n+3}$$

is irreducible.

We have that

$$\gcd(21n+4, 14n+3) = \gcd(7n+1, 14n+3) = \gcd(7n+1, 1) = 1$$

so they are relatively prime, as required.  $\square$

### Problem 1.12.3

Let  $x, y, a, b, c$  be integers.

1. Prove that  $2x + 3y$  is divisible by 17 if and only if  $9x + 5y$  is divisible by 17.
2. If  $4a + 5b - 3c$  is divisible by 19, prove that  $6a - 2b + 5c$  is also divisible by 19.

We start with the first statement and the if direction. We have that  $9x + 5y \pmod{17} \equiv 0$ . Multiplying by 4, we have that  $36x + 20y \pmod{17} \equiv 2x + 3y \equiv 0$  as required. For the only if direction, we can multiply  $2x + 3y \pmod{17} \equiv 0$  by 13.

For the second part, we have that  $4a + 5b - 3c \pmod{19} \equiv 0$ , and multiplying by 11 gives the desired result.  $\square$

**Problem 1.12.4**

Define the  $n$ th Fermat number  $F_n$  by  $F_n = 2^{2^n} + 1$ . Show that  $\gcd(F_m, F_n) = 1$  for any  $m \neq n$ .

Assume for the sake of contradiction there exist  $m \neq n$  such that  $\gcd(F_m, F_n) \neq 1$ . Then, let  $p$  be some prime dividing  $F_m$ . Then,

$$2^{2^m} + 1 \equiv 0 \pmod{p} \implies 2^{2^{m+1}} \equiv 1 \pmod{p}.$$

Hence the order of  $2 \pmod{p}$  is  $2^{m+1}$ . Similarly, if  $p$  divides  $F_n$ , then we find that the order of  $2 \pmod{p}$  is  $2^{n+1}$ . However, these two quantities can only be equal if  $m = n$ , which is a contradiction of the original statement.  $\square$

**Problem 1.12.5**

Prove that for each positive integer  $n$ , there is a positive integer  $m$  such that each term of the infinite sequence  $m + 1, m^m + 1, m^{m^m} + 1, \dots$  is divisible by  $n$ .

If  $n$  is even, then take  $m = n - 1$ . This clearly works since

$$(n-1)^{(n-1)(n-1)\dots} \equiv (-1)^{(n-1)(n-1)\dots} \equiv -1 \pmod{n}.$$

If  $n$  is odd, then take  $m = 2n - 1$ . Then, we have that

$$(2n-1)^{(2n-1)(2n-1)\dots} \equiv (-1)^{(2n-1)(2n-1)\dots} \equiv -1 \pmod{n}$$

as required.  $\square$

**Problem 1.12.6 (Romanian Mathematical Olympiad)**

Let  $a, b$  be positive integers such that there exists a prime  $p$  with the property  $\text{lcm}(a, a+p) = \text{lcm}(b, b+p)$ . Prove that  $a = b$ .

We have that

$$\frac{a^2 + ap}{\gcd(a, p)} = \frac{b^2 + bp}{\gcd(b, p)} \implies \frac{\gcd(b, p)}{\gcd(a, p)} = \frac{b^2 + bp}{a^2 + ap}.$$

We now case on the  $v_p$  of the two variables.

If  $v_p(a) = v_p(b) = 0$  or  $v_p(a), v_p(b) \geq 1$ , then we have that

$$a^2 + ap = b^2 + bp \implies (a-b)(a+b+p) = 0.$$

Hence, either  $a = b$ , or one of  $a$  or  $b$  is negative, which we cannot have. Hence, this case is done.

Now, if  $v_p(a) = 0$  and  $v_p(b) \geq 1$ , then we have that

$$p(a^2 + ap) = b^2 + bp \implies a^2p + ap^2 - b^2 - bp = 0$$

however this means that  $p \mid b$ , so substituting  $b = kp$ , we have that

$$a^2 + ap - k^2p - kp = 0$$

which implies the same thing as the case above, so  $a = k$  implying that  $b = ap$ . However, this means that

$$p = \frac{b^2 + bp}{a^2 + ap} = \frac{a^2p^2 + ap^2}{a^2 + ap} \implies a^2 + ap = a^2p + ap$$

so  $p = 1$ , which doesn't work.

The case where  $v_p(a) \geq 1$  and  $v_p(b) = 0$  is similar.

Hence, exhausted all cases, we are done.  $\square$

**Problem 1.12.7** (St. Petersburg 1996)

Find all positive integers  $n$  such that

$$3^{n-1} + 5^{n-1} \mid 3^n + 5^n.$$

We have that

$$3^{n-1} + 5^{n-1} \mid 3 \cdot 3^{n-1} + 5 \cdot 5^{n-1} \implies 5^{n-1} - 3^{n-1} \pmod{5^{n-1} + 3^{n-1}} \equiv 0.$$

Hence, we must have that  $5^{n-1} = 3^{n-1}$  so  $n = \boxed{1}$ .

**Problem 1.12.8** ((Russia 2001 Grade 11 Day 2/2))

Let  $a, b$  be naturals such that  $ab(a+b)$  is divisible by  $a^2 + ab + b^2$ . Show that  $|a - b| > \sqrt[3]{ab}$ .

Let  $\gcd(a, b) = d$ , so that  $a = dm$  and  $b = dn$ . Then,

$$m^2 + mn + n^2 \mid dm(m+n)$$

and  $\gcd(m, n) = 1$ . In addition, we make a claim.

**Claim**

If  $\gcd(m, n) = 1$ , then  $\gcd(m^2 + mn + n^2, mn(m+n)) = 1$ .

*Proof.* Let  $p$  be a prime dividing  $m$ . Then, notice that it also divides  $mn(m+n)$ . Now, in order for  $p$  to divide  $m^2 + mn + n^2$ , it would have to divide  $n^2$ , but  $m$  and  $n$  don't share a common prime factor. Hence, we have the required conclusion.  $\square$

As a result, we know that  $m^2 + mn + n^2 \mid d$ , so  $m^2 + mn + n^2 \leq d$ . Hence,

$$|a - b|^3 \geq d^2 \cdot d|m - n|^3 \geq d^2(m^2 + mn + n^2) = a^2 + ab + b^2 > ab$$

so we are done.  $\square$

**Problem 1.12.9** (Germany)

Let  $m$  and  $n$  be two positive integers where  $\gcd(m, n) = 1$ . Prove that for every positive integer  $k$ ,  $n+m$  is a divisor of  $n^2 + km^2$  if and only if  $n+m$  is a divisor of  $k+1$ .

We start with the only if direction. Since

$$n^2 + km^2 \equiv m^2 + km^2 \equiv (k+1)m^2 \equiv 0 \pmod{m+n}$$

and as  $\gcd(m, m+n) = 1$ , we know that  $m+n$  divides  $k+1$ .

We proceed with the if direction. Since

$$0 \equiv k+1 \equiv (k+1)m^2 \equiv m^2 + km^2 \equiv n^2 + km^2 \pmod{m+n}$$

as required.  $\square$

**Problem 1.12.10** (Japan 2020 Junior Finals P3)

Find all tuples of positive integers  $(a, b, c)$  such that

$$4 \operatorname{lcm}(a, b, c) = ab + bc + ca.$$

WLOG let  $a \leq b \leq c$ . Then, we know that  $a \mid bc$ ,  $b \mid ac$ , and  $c \mid ab$ . Now, since  $\operatorname{lcm}(a, b, c) \mid ab$ , we may make the following claim.

**Claim**

We claim that  $\operatorname{lcm}(a, b, c) = ab$ .

*Proof.* Clearly, if it is not equal to  $ab$ , then  $\operatorname{lcm}(a, b, c) \leq \frac{ab}{2}$ . Then, substituting gives that

$$ab = bc + ac$$

which cannot work. Hence, we have the required conclusion.  $\square$

Hence, substituting  $\operatorname{lcm}(a, b, c) = ab$ , we find that

$$3ab = bc + ac$$

and from the claim above,  $\gcd(a, b) = 1$ . Hence, we find that either  $c \mid 3$ ,  $c \mid a$ , or  $c \mid b$ . We now case.

- If  $c \mid 3$ , then either  $c = 3$  or  $c = 1$ . If it is the latter, then we must have  $a = b = c = 1$ , which clearly does not work. If it is the former, then we wish to find solutions to  $ab = a + b$  which factors as  $(a - 1)(b - 1) = 1$ , so we must have  $a = b = 2$ . Trying this, we see that this does not work.
- If  $c \mid a$ , then we know that  $a = b = c$ , so trying this,

$$4a = 3a^2 \implies a = \frac{4}{3}$$

which does not work.

- If  $c \mid b$ , then we know that  $b = c$ , so the equation reduces to

$$4 \operatorname{lcm}(a, b) = 2ab + b^2.$$

Now, if  $\operatorname{lcm}(a, b) = ab$ , then we know that  $2ab = b^2$  so  $2a = b$ , but then we must have  $b = c = 2$ , so  $a = 1$ . Trying this, we see that this is indeed a solution. Else, we know that  $\operatorname{lcm}(a, b) = \frac{ab}{2}$ , but this cannot lead to solutions.

Hence, the only solution is  $\boxed{(1, 2, 2)}$  and permutations.  $\square$

**Problem 1.12.11** (Iran MO 2017 Round 2/1)

Prove the following:

1. There doesn't exist a sequence  $a_1, a_2, a_3, \dots$  of positive integers such that for all  $i < j$ , we have  $\gcd(a_i + j, a_j + i) = 1$ .
2. Let  $p$  be an odd prime number. Prove that there exists a sequence  $a_1, a_2, a_3, \dots$  of positive integers such that for all  $i < j$ ,  $p \nmid \gcd(a_i + j, a_j + i)$ .

We start with the first part. Notice that by selecting  $i = 2m$  and  $j = 2n$ , we find that any even indexed term must be odd. Then, by taking  $i = 2m$  and  $j = 2n - 1$ , we find that all odd indexed terms must be odd also. However, selecting  $i = 2m - 1$  and  $j = 2n - 1$  then gives a contradiction since 2 must divide it.

We finish with the second part. Notice that  $\gcd(a_i + j, a_j + i) = \gcd((a_i + i) + (a_j + j), a_j + i)$ . Hence, it suffices to find a sequence  $\{a\}$  where

$$p \nmid (a_i + i) + (a_j + j).$$

However, we can just select the sequence where  $a_i = (i - 1)p + 2 - i$ , so that

$$\{a\} = 1, p, 2p - 1, 3p - 2, \dots$$

Then, notice that the sum of any two terms must be  $4 \pmod{p}$ , as required.  $\square$

**Problem 1.12.12** (All Russian Olympiad 2017 Day 1 Grade 10 P5)

Suppose  $n$  is a composite positive integer. Let  $1 < a_1 < a_2 < \dots < a_k < n$  be all the divisors of  $n$ . It is known, that  $a_1 + 1, \dots, a_k + 1$  are all divisors for some  $m$  (except 1,  $m$ ). Find all such  $n$ .

We find that we must have

$$(a_1 + 1)(a_k + 1) = (a_2 + 1)(a_{k-1} + 1) = \dots$$

and as a result,

$$a_1 + a_k = a_2 + a_{k-1} = \dots$$

Now, looking at the first equality, we must have that

$$a_1 + \frac{n}{a_1} = a_2 + \frac{n}{a_2} \implies a_1 - a_2 = n \left( \frac{1}{a_2} - \frac{1}{a_1} \right) = \frac{n(a_1 - a_2)}{a_1 a_2}.$$

Hence, either  $a_1 = a_2$  or  $a_1 a_2 = n$ . Clearly, we cannot have the latter, so  $\tau(n) \leq 4$ . We now case.

- If  $\tau(n) = 2$ , then it must be prime, which contradicts the problem statement.
- If  $\tau(n) = 3$ , then  $n = p^2$  for some prime  $p$ . Then, we require for  $p+1$  to be the all the divisors of some  $m$ , but  $2 \mid p+1$  unless  $p = 2$ , for which we find the solution  $n = 4$ .
- If  $\tau(n) = 4$ , then either  $n = p^3$  or  $n = pq$  for primes  $p, q$ . If it is the former, then there must exist  $m$  such that all the divisors of  $m$  are  $p+1$  and  $p^2+1$ . However, notice that unless  $p = 2$ , both are divisible by two, so this is impossible. If  $p = 2$ , then notice that  $m = 15$  works, so this is satisfactory. On the other hand, if  $n = pq$ , then WLOG  $p < q$ . In that case,  $p+1$  and  $q+1$  must be all the divisors of  $m$ , however this is impossible for the same reason as the previous case.

Hence, in the end, our only solutions are  $n = [4, 8]$ , as required.  $\square$

**Problem 1.12.13** (IMO 2002/4)

Let  $n \geq 2$  be a positive integer, with divisors  $1 = d_1 < d_2 < \dots < d_k = n$ . Prove that  $d_1d_2 + d_2d_3 + \dots + d_{k-1}d_k$  is always less than  $n^2$ , and determine when it is a divisor of  $n^2$ .

We first prove the first part. Notice that  $\max(d_i) = \frac{n}{k-i+1}$ . Hence, we wish to show that

$$\frac{n}{1} \cdot \frac{n}{2} + \frac{n}{2} \cdot \frac{n}{3} + \dots + \frac{n}{k-1} \cdot \frac{n}{k} < n^2$$

which is clear by telescoping.

We now show the second part. We start with a claim.

**Claim**

In order for  $d_1d_2 + d_2d_3 + \dots + d_{k-1}d_k \mid n^2$ ,  $n$  cannot be composite.

*Proof.* Suppose for the sake of contradiction that there exists composite  $n$  that works. Let  $p$  be the smallest prime dividing  $n$ . Then, notice that

$$d_1d_2 + d_2d_3 + \dots + d_{k-1}d_k > d_{k-1}d_k = \frac{n^2}{p}$$

so it cannot work, as required.  $\square$

Trying primes  $n = p$ , we find that we must have  $p + 1 \mid p^2$ , or

$$\gcd(p^2, p+1) = p+1.$$

Solving this, we require for  $1 = p+1$ , which has no solutions. Hence, there exist no solutions.  $\square$

**Problem 1.12.14** (Russia 2001 Grade 10 Day 2/4)

Find all odd positive integers  $n > 1$  such that if  $a$  and  $b$  are relatively prime divisors of  $n$ , then  $a+b-1$  divides  $n$ .