EGMO Solutions

Kempu33334

July 2025

Contents

1 Fundementals 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 $ab = \gcd(a, b)\text{lcm}(a, b) = \text{lcm}(a, b) \mid c$. $\square$

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

$$\gcd(120, 500) = \gcd(120, 20) = \boxed{20}.$$

$\square$

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. $\square$

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 $\mathrm{lcm}(a, b) = \mathrm{lcm}(r, b)$?

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

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

which cannot be true. $\square$

1.8 Bézout's Theorem

No problems.

1.9 Base Systems

Problem 1.9.1

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

The former is 122_5, and the latter is 1000101_2. $\square$

Problem 1.9.2

Show that any power of 2 is of the form $100\ldots0_2$.

This is clear, since 2^n will be expressed as $1\underbrace{00\ldots0}_{n \text{ times}}$.

Problem 1.9.3

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

Clearly, since $a_k \ge 1$, we have that $\ell^k \le n$. 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 ℓ.

Note that since

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

we know that n has at least $k+1$ digits in base ℓ. 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. □

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. □

1.11 Example Problems

No problems.

1.12 Practice Problems

Problem 1.12.1

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

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

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. □

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. □

Problem 1.12.4

Define the nth 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. □

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, $m^{m^m}+1$, … is divisible by n.

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

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

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

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

as required. □

Problem 1.12.6 (Romanian Mathematical Olympiad)

Let a, b be positive integers such that there exists a prime p with the property $\operatorname{lcm}(a, a+p) = \operatorname{lcm}(b, b+p)$. 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 $n = \boxed{1}$.