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. □

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. □

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. □

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. □

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 $a_i \le b_i$ for all $i \ge 1$. 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 $i \ge 1$, implying that $a_i \le b_i$, 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

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

as required. $\square$

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 $0 \le r < b$. Then our lemma states that

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

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

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

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. $\square$

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_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 $\ell^k \leq n < \ell^{k+1}$ 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 ℓ.

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 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. $\square$

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. □

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. □

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. $\square$

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 $m + 1$, $m^m + 1$, $m^{m^m} + 1$, $\ldots$ 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. $\square$

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 $n = \boxed{1}$.

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,

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

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 $a \le b \le c$. 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 $\operatorname{lcm}(a, b, c) \le \frac{ab}{2}$. Then, substituting gives that

$$ab = bc + ac$$

which cannot work. Hence, we have the required conclusion. □

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. □

Problem 1.12.11 (Iran MO 2017 Round 2/1)

Prove the following:

1. There doesn't exist a sequence $a_1, a_2, a_3, \ldots$ 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 $a_1, a_2, a_3, \ldots$ 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 $\gcd(a_i + j, a_j + 1) = \gcd((a_i + i) + (a_j + j), a_j + 1)$. 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

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

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

Problem 1.12.12 (Russia 2017 Grade 10 Day 1/5)

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

We find that we must have

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

and as a result,

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

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 $n = \boxed{4, 8}$, as required. $\square$

Problem 1.12.13 (IMO 2002/4)

Let $n \geq 2$ be a positive integer, with divisors $1 = d_1 < d_2 < \cdots < d_k = n$. Prove that $d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$ 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

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

which is clear by telescoping.

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

Claim

In order for $d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k \mid n^2$, 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

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

so it cannot work, as required. □

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. □

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.

We claim the answer is $n = p^k$ for all odd primes p and positive integers k, which clearly works. We begin with a claim.

Claim

We claim n cannot have more than one prime factor.

Proof. Assume there exists, for the sake of contradiction, satisfactory n which contains more than one prime factor. Then, we write $n = p^k m$, where $p \nmid m$ and $m \neq 1$. In that case, notice that $p + m - 1$ must divide n. Now, since all the prime factors of m are greater than p, we know that $\gcd(p - 1, m) = 1$, so

$$p + m - 1 = p^\ell$$

for some non-negative integer ℓ. In addition, we know that $p^\ell + m - 1 = 2p^\ell - p$ must divide n and as a result, we know that $2p^{\ell-1} - 1$ must divide m. As a result,

$$2p^{\ell-1} - 1 \mid p^\ell - p + 1 \implies \gcd(2p^{\ell-1} - 1, p^\ell - p + 1) = \gcd(2p^{\ell-1} - 1, p^{\ell-1} - (p-1)/2) = 2p^{\ell-1} - 1.$$

However, we must have that

$$p^{\ell-1} + (p - 1)/2 \leq 1$$

which is clearly impossible. □

As a result, we take $n = p^k$, which clearly works. □

Problem 1.12.15 (INMO 2019/3)

Let m, n be distinct positive integers. Prove that

$$\gcd(m,n)+\gcd(m+1,n+1)+\gcd(m+2,n+2)\le 2|m-n|+1.$$

Further, determine when equality holds.

WLOG let $m\ge n$, and notice that

$$\gcd(m,n)+\gcd(m+1,n+1)+\gcd(m+2,n+2)=\gcd(m-n,n)+\gcd(m-n,n+1)+\gcd(m-n,n+2).$$

Then, we know that at most one of $\gcd(m-n,n)$, $\gcd(m-n,n+1)$, and $\gcd(m-n,n+2)$ can be exactly $m-n$, while the others must be less than or equal to $\frac{m-n}{2}$ (as long as $m-n>1$). As a result, we find that

$$\gcd(m-n,n)+\gcd(m-n,n+1)+\gcd(m-n,n+2)\le m-n+\frac{m-n}{2}+\frac{m-n}{2}=2(m-n)<2(m-n)+1$$

which is good. On the other hand, we have equality if and only if $m-n=1$ or $m-n=2$ with even n. $\square$

Problem 1.12.16 (USAMO 2007/1)

Let n be a positive integer. Define a sequence by setting $a_1=n$ and for each $k>1$, letting a_k to be the unique integer in the range $0\le a_k\le k-1$ for which $a_1+a_2+\cdots+a_k$ is divisible by k. For instance, when $n=9$, the obtained sequence is 9, 1, 2, 0, 3, 3, 3, ... Prove that for any n, the sequence $\{a\}$ eventually becomes constant.

Notice that if there exists k,

$$\frac{a_1+a_2+\cdots+a_k}{k}<k$$

then the sequence will become constant for obvious reasons (simply selecting $\frac{a_1+a_2+\cdots+a_k}{k}$ for all successive elements suffices). Hence, assume that this does not happen. Then, we know that

$$\begin{aligned} a_1&\ge 1\\ a_1+a_2&\ge 4\\ &\vdots \end{aligned}$$

However, the sequence $\{a\}$ is bounded by $a_i\le i-1$, and since $n^2-\frac{n(n+1)}{2}$ is monotonically increasing, this cannot hold. Hence, we have the required conclusion. $\square$

Problem 1.12.17 (USAMO 2007/5)

Prove that for every nonnegative integer n, the number $7^{7^n}+1$ is the product of at least $2n+3$ (not necessarily distinct) primes.

We induct on n. For the base case, it is clearly true for $n=0$. Now, assume it is true for some n, so that $m=7^{7^n}$ is the product of at least $2n+3$ primes. Then,

$$7^{7^{n+1}}+1=m^7+1=(m+1)(m^6-m^5+m^4-m^3+m^2-m+1).$$

We may write that

$$m^6-m^5+m^4-m^3+m^2-m+1=(m+1)^6-7m(m^2+m+1)^2$$

which is a difference of squares. Hence, the total number of prime divisors is at least $2n+3+2 = 2n+5$, so we have the requireed conclusion.

Problem 1.12.18 (ELMO 2017/1)
Let $a_1, a_2, \ldots, a_n$ be positive integers with product P, where n is an odd positive integer. Prove that
$$\gcd(a_1^n + P, a_2^n + P, \ldots, a_n^n + P) \le 2 \cdot \gcd(a_1, a_2, \ldots, a_n)^n.$$

Since the equation is homogeneous, assume that $\gcd(a_1, a_2, \ldots, a_n) = 1$. Then, we wish to show that
$$g = \gcd(a_1^n + P, a_2^n + P, \ldots, a_n^n + P) \le 2.$$
Now, let $p \mid g$ be a prime. If there exists i such that $p \mid a_i$, then we reach a contradiction with the condition on the gcd of all the a. Hence, $\gcd(g, P) = 1$. Now, since
$$g \mid a_i^n + P$$
over all i, we find that
$$a_i^n \equiv -P \pmod g$$
and a cyclic multiplication yields that
$$2P^g \equiv 0 \pmod g$$
so $g \mid 2$, as required. $\square$

Problem 1.12.19 (IMO 2001/6)
Let $a > b > c > d$ be positive integers and suppose that
$$ac + bd = (b + d + a - c)(b + d - a + c).$$
Prove that $ab + cd$ is not prime.

We know that $b + d + a - c \mid ac + bd$, so
$$\gcd(ac + bd, b + d + a - c) = \gcd((a + b)(a + d), b + d + a - c) = b + d + a - c$$
so
$$b + d + a - c \mid (a + b)(a + d).$$
Similarly, we know that $b + d - a + c \mid ac + bd$, so
$$\gcd(ac + bd, b + d - a + c) = \gcd((b + c)(c + d), b + d - a + c) = b + d - a + c$$
so
$$b + d - a + c \mid (b + c)(c + d).$$
Hence, we find that
$$ac + bd \mid (a + b)(a + d)(b + c)(c + d) = ((ac + bd) + (ad + bc))((ab + cd) + (ac + bd))$$
implying that
$$ac + bd \mid (ad + bc)(ab + cd).$$
We know that
$$ab + cd > ac + bc > ad + bc$$
by the Rearrangment Inequality. Hence, if $ab + cd$ were to be prime, then $ac + bd \mid ad + bc$ which isn't possible, so we have the required conclusion. $\square$

2 Modular Arithmetic Basics

2.1 Motivation

Problem 2.1.1

Show that $a + n \equiv a \pmod{n}$.

This is clear, since $n \equiv 0 \pmod{n}$. □

Problem 2.1.2

Let a, n be fixed integers. Show that the set of integers b such that $b \equiv a \pmod{n}$ form an arithmetic progression. What is the common difference?

Since they all leave the same remainder when divided by n, we know that they form an arithmetic progress with common difference n. □

Problem 2.1.3

Show that the set of integers a such that $a \equiv 0 \pmod{n}$ is the set of multiples of n.

Clearly, this is just all numbers which are divisible by n. □

2.2 Remainder Idea

No problems.

2.3 Residue Classes

Problem 2.3.1

Guess why the above classes are called "residue" classes.

Residue is just what is left behind. □

Problem 2.3.2

Show that the number of the classes modulo n is exactly n.

There is a clear bijection between the numbers $0, 1, \ldots, n-1$ and each residue class. □

2.4 Basic Properties

Problem 2.4.1

Show that ab has remainder $rs \mod n$ by writing $a = nx + r$ and $b = ny + s$ and evaluating ab.

We may write that

$$ab \equiv (nx + r)(ny + s) \equiv n(\cdots) + rs \equiv rs \pmod{n}$$

as required. $\square$

Problem 2.4.2

Find the remainder when 2^{10} is divided by 10.

We know $2^{10} = 1024$, so the answer is 4. $\square$

Problem 2.4.3

Find $1002 \times 560 \pmod 7$.

Since $7 \mid 560$, the answer is 0. $\square$

Problem 2.4.4

Show that if $a \equiv b \pmod n$, then $ka \equiv kb \pmod n$ for any integer k.

We are given that $a - b$ is a multiple of n, so $k(a-b)$ is too. $\square$

Problem 2.4.5

Show that $a - b \mid a^n - b^n$ for any integer n.

We write the following:

$$a^n - b^n \equiv b^n - b^n \equiv 0 \pmod{a-b}$$

as required. $\square$

Problem 2.4.6

If p is an odd prime, and a, b are coprime, show that

$$\gcd\left(\frac{a^p+b^p}{a+b}, a+b\right) \in \{1, p\}.$$

We may write that

$$\frac{a^p+b^p}{a+b} \equiv a^{p-1} - a^{p-2}b + \cdots + b^{p-1} \equiv pa^{p-1} \pmod{a+b}$$

and since $\gcd(a,b) = 1$, we clearly have the necessary conclusion. $\square$

Problem 2.4.7

Let f be a polynomial with integer coefficients. Show that $a - b | f(a) - f(b)$ for any integers a, b is the same as saying $f(a+d) \equiv f(a) \pmod d$.

Let $b = a - d$. Then, we find that

$$d \mid f(a) - f(a-d)$$

which is the required conclusion. $\square$

Problem 2.4.8

Show that $ka \equiv kb \pmod{n}$ implies $a \equiv b \pmod{n}$ if and only if $\gcd(k, n) = 1$.

Clearly, an inverse k^{-1} with respect to modulo n exists if and only if $\gcd(k, n) = 1$, so both directions are trivial. $\square$

2.5 Two Special Equal Sets

No problems.

2.6 Fermat's Little Theorem

Problem 2.6.1

Show that $a^p \equiv a \pmod{p}$ holds in the case when $\gcd(a, p) \neq 1$.

Notice that by simply multiplying $a^{p-1} \equiv 1 \pmod{p}$ by a, we take care of the case when $a \equiv 0 \pmod{p}$ and extend it, as required. $\square$

Problem 2.6.2

Let a, b be integers and p a prime. Show that p divides $ab^p - a^p b$.

By Fermat's Little Theorem,

$$ab^p - a^p b \equiv ab - ab \equiv 0 \pmod{p}$$

as required. $\square$

Problem 2.6.3

Find

$$2^{50} \pmod{7}.$$

By FLT,

$$2^{50} \equiv 2^2 \equiv 4 \pmod{7}$$

as desired. $\square$

2.7 Inverses

Problem 2.7.1

Show that inverses multiply like fractions.

Follows since multiplication is commutative. $\square$

Problem 2.7.2

Find the inverse of all $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ modulo 11.

This is just the set $\{1, 6, 4, 3, 9, 2, 8, 7, 5, 10\}$ where each number is mapped to the respective number in the other set. $\square$

Problem 2.7.3

Show that 0 does not have an inverse modulo p. What about p?

Since 0 times anything is 0, it cannot equal 1 at any point. Similarly, since p is equivalent to 0 in $\mathbb{F}_p$, we have the required conclusion. $\square$

Problem 2.7.4

Prove that if $a \neq 0 \pmod p$, then

$$a^{p-2} \equiv a^{-1} \pmod p.$$

Follows by dividing FLT by a. $\square$

Problem 2.7.5

Prove that the inverse of a^n is the nth power of the inverse of a. That is,

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

Using this, find the inverse of 256 modulo 47.

The first part follows by exponent rules. The second,

$$256^{-1} \equiv (2^8)^{-1} \equiv (2^{-1})^8 \equiv 24^8 \equiv 9 \pmod{47}$$

as required. $\square$

2.8 Simple Properties of Inverses and Wilson's Theorem

Problem 2.8.1

Prove that if n is any natural satisfying $(n-1)! \equiv -1 \pmod n$, then n must be a prime.

Follows by CRT and decomposition if n is composite. $\square$

Problem 2.8.2

Let p be a prime. Show that the remainder when $(p-1)!$ is divided by $p(p-1)$ is $p-1$.

Follows by CRT and Wilson's Theorem. $\square$

Problem 2.8.3

Let n be an integer. Calculate

$$\gcd(n! + 1, (n+1)!).$$

We split into cases based on if $n+1$ is prime.

If $n+1$ is prime, then it suffices to calculate $\gcd(n!+1, n+1)$. However, by Wilson's Theorem, this is just $n+1$, so we have the required answer.

If $n+1$ is composite, then let q be a prime dividing $(n+1)!$. Then, we know that $q \leq n$, so it divides $n!$ but not $n!+1$, so $\gcd(n!+1,(n+1)!) = 1$. $\square$

2.9 General Equal Sets

No problems.

2.10 Euler's Theorem

Problem 2.10.1

Find $2^{98} \pmod{33}$

Since $\phi(33) = 20$, this reduces to

$$2^{-2} \equiv 4^{-1} \equiv 25 \pmod{33}$$

as required. $\square$

Problem 2.10.2

Find $5^{30} \pmod{62}$.

Since $\phi(62) = 30$, this is just $1 \pmod{62}$. $\square$

Problem 2.10.3

What happens if $\gcd(a,n) \neq 1$? Does there exist any integer m such that $a^m \neq 1 \pmod{n}$?

No, since a^m and n will share a common factor. $\square$

Problem 2.10.4

Show that $n \mid 2^{n!} - 1$ for all odd n.

Notice that $\phi(n)$ will only have prime factors that are less than n, and $\phi(n) < n$, so we apply Euler's Theorem to win. $\square$

2.11 General Inverses

Problem 2.11.1

Find the inverse of all $\{1,3,5,7\}$ modulo 8. What do you observe? Can you explain this?

It is the set $\{1,5,3,7\}$. It is just a permutation of the original set, but this is clear, since in order for it not to be, it would have to contain some number divisible by 2, which cannot work. $\square$

Problem 2.11.2

Does there exist an inverse for 5 modulo 10? What about 4?

No for both. $\square$

Problem 2.11.3

Show that $\gcd(a^{-1}, n)$ is also 1.

Because $aa^{-1} \equiv 1 \pmod{n}$, if $\gcd(a^{-1}, n) \neq 1$, then they must share a common prime factor, which means that we cannot have a, contradiction. □

Problem 2.11.4

Prove that if $\gcd(a, n) \neq 1$, then a cannot have an inverse.

Then, a and n must share a common prime factor, which means that there cannot exist an inverse. □

2.12 Extra Results as Problems

Problem 2.12.1

Use Freshman's dream and induction to prove Fermat's Little Theorem.

We proceed using induction. For the base case, it is clearly true for 0:

$$0^p \equiv 0 \pmod{p}.$$

Now, assume it is true for some k. Then, by Freshman's Dream,

$$(k+1)^p \equiv k^p + 1 \equiv k + 1 \pmod{p}$$

as required. Hence, we are done. □

Problem 2.12.2

Use induction to show that

$$(a+b)^{p^i} \equiv a^{p^i} + b^{p^i} \pmod{p}$$

for any prime p and any non-negative integer i.

For the base case, it is clearly true for $i = 0$. Hence, assume it is true for some i. Then, we will show that it is correct for $i + 1$. Notice that

$$(a+b)^{p^{i+1}} \equiv \left((a+b)^{p^i}\right)^p \equiv \left(a^{p^i} + b^{p^i}\right)^p \equiv a^{p+(i+1)} + b^{p+(i+1)} \pmod{p}$$

as required. □

2.13 Example Problems

No problems.

2.14 Practice Problems

Problem 2.14.1

How many prime numbers p are there such that $29^p + 1$ is a multiple of p?

We have that

$$29^p + 1 \equiv 30 \pmod{p}$$

so the answer is $p = \boxed{2, 3, 5}$, which we can check to work. $\square$

Problem 2.14.2

Let p be a prime and $0 \leq k \leq p - 1$ be an intger. Prove that

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

We may write that

$$\binom{p-1}{k} \equiv \frac{(p-1)!}{k!(p-1-k)!} \equiv \frac{-1}{k!(p-1-k)!} \equiv \frac{-1}{(-1)^k(p-1)!} \equiv (-1)^k \pmod{p}$$

so we have the required conclusion. $\square$

Problem 2.14.3 (IMO 1979/1)

Let a and b be natural numbers such that

$$\frac{a}{b} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319}.$$

Prove that a is divisible by 1979. (Note: 1979 is a prime)

We know that

$$\frac{a}{b} = \left(1 + \frac{1}{2} + \cdots + \frac{1}{1319}\right) - \left(1 + \frac{1}{2} + \cdots + \frac{1}{659}\right) = \frac{1}{660} + \frac{1}{661} + \cdots + \frac{1}{1319}.$$

Now, by combining opposite fractions, each one is divisible by 1979, so we have the required conclusion (and the number of fractions is even). $\square$

Problem 2.14.4 (RMO 2016/6)

Let $\{a\}$ be a strictly increasing sequence of positive integers in an arithmetic progression. Prove that there is an infinite subsequence of the given sequence whose terms are in a geometric progression.

Notice that the terms of the form $a_1(d+1)^n$, where d is the common difference, for some n have the property that they are in the arithmetic sequence since by subtracting a, they are divisible by d, so we have the required conclusion. $\square$

Problem 2.14.5

Let $f(x)$ be a polynomial with integer coefficients. Show that there does not exist a N such that $f(x)$ is a prime for all $x \geq N$. In other words, $f(x)$ is not eventually always a prime. This problem shows that prime numbers don't follow any polynomial pattern either.

Notice that if $f(a)$ is prime, then $f(a + kp)$ must be composite infinitely many times, otherwise $f(x)$ is constant, so it suffices to pick $f(x) = p$ for a prime p. $\square$

Problem 2.14.6 (IMO 2005/4)

Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n = 2^n + 3^n + 6^n - 1, n \geq 1.$$

Notice that for any prime p, selecting $n = p - 2$ gives that

$$2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \equiv 0 \pmod{p}$$

so the only answer is $\boxed{1}$. $\square$

Problem 2.14.7 (IMO 1986/1)

Let d be any positive integer not equal to 2, 5, or 13. Show that one can find distinct a and b in the set $\{2, 5, 13, d\}$ such that $ab - 1$ is not a perfect square.

The problem is equivalent to showing that there exists $a \in \{2, 5, 13\}$ such that $ad - 1$ is not a perfect square. Notice that if $\nu_2(d) \geq 1$, then taking $a = 2$ and modulo 4 gives that it must be 3 (mod 4), which is not possible, as required. Hence, assume a is odd. Now, $5d - 1$ is 2 (mod 4) if $d \equiv 3 \pmod{4}$, so assume that $d \equiv 1 \pmod{4}$. Then, we write $d = 4k + 1$, so that it is equivalent to $4ka + a - 1$. However, substituting $a = 5$ and $a = 13$ respectively give that $5k + 1$ and $13k + 3$ are perfect squares, which is impossible by modulo 4. Hence, one must not be a perfect square, and we are done. $\square$

Problem 2.14.8

Let a and b be two relatively prime positive integers, and consider the arithmetic progression a, $a + b$, $a + 2b$, $a + 3b$, $\ldots$.

1. Prove that there are infinitely many terms in the arithmetic progression that have the same prime divisors.

2. Prove that there are infinitely many pairwise relatively prime terms in the arithmetic progression.

We begin with the first part. Clearly, for any prime p, the terms that it divides is periodic modulo p, and it must be achieved at least once. Hence, we are done.

We finish with the second part. Suppose that there are finitely pany pairwise relatively prime terms in the arithmetic progression, and let them be r_1, r_2, $\ldots$, r_n. Then, let $P = r_1 r_2 \cdots r_n$.

Claim

There exists a non-negative integer k such that for any prime $p \mid P$, $p \nmid a + kb$.

Proof. This is equivalent to

$$kb \not\equiv -a \pmod{p}.$$

Now, since $\gcd(b,p)=1$, b is invertible modulo p, so

$$k \not\equiv -\frac{a}{b} \pmod{p}.$$

Now, by CRT, we can construct such an k, so we are done. □

Hence, this contradicts the fact that we only have finitely many r, so we are done. □

Remark

The second part immediately follows from Dirichlet's Theorem on Arithmetic Progressions.

Problem 2.14.9

Prove that:

1. Every positive integer has at least as many divisors of the form $4k+1$ as divisors of the form $4k+3$.

2. There exist infinitely many positive integers which have as many divisors of the form $4k+1$ as divisors of the form $4k+3$.

3. There exist infinitely many positive integers which have more divisors of the form $4k+1$ than divisors of the form $4k+3$.

We begin with the first part and perform an strong induction. Clearly, the statement is true for $n=1$. We now make a claim.

Claim

If the statement is true for some n and all d dividing it, then it is true for any np where p is a prime.

Proof. We split into cases. If $p \nmid n$, then split into further cases.

- If $p \equiv 1 \pmod{4}$, then the result is clear.

- If $p \equiv 3 \pmod{4}$, then the number of divisors that are $1 \pmod{4}$ and divide n (call it d_1) is at least the number of divisors that are $3 \pmod{4}$ and divide n (call it d_3). On the other hand, if the number of divisors that don't divide n but do divide pn and are congruent to $1 \pmod{4}$ is equal to d_3, while the number congruent to $3 \pmod{4}$ and divide pn but not n is d_1. Hence, the total amounts are equal.

Now, if $p \mid n$, then we can apply the same logic on $n = p^{\nu_p(n)+1} \cdot \frac{n}{p^{\nu_p(n)}}$ since $\frac{n}{p^{\nu_p(n)}} \mid n$ (by the strong induction). Hence, we are done. □

This then shows that all positive integers work.

We finish with the second and third part. Notice that the number $n = 3^\ell$ has $\left\lfloor \frac{1}{2}\ell \right\rfloor + 1$ divisors congruent to $1 \pmod{4}$, while it has $\ell + 1 - \left\lfloor \frac{1}{2}\ell \right\rfloor$ divisors congruent to $3 \pmod{4}$. Now, these two are equal as long as ℓ is odd, and the first is greater than the second as long as ℓ is even, so we have the required conclusion. □

Remark
The second and third parts follow directly from Dirichlet's Theorem on Arithmetic Progressions on the sequences $a_i = 4i+1$ and $b_i = 4i+3$.

Problem 2.14.10 (Iberoamerican 2005/3)
Let $p \geq 5$ be a prime. Prove that if
$$\sum_{i=1}^{p-1} \frac{1}{i^p} = \frac{m}{n}$$
with $\gcd(m,n) = 1$, then $p^3 \mid m$.

We know that
$$\sum_{i=1}^{p-1} \frac{1}{i^p} = \sum_{i=1}^{\frac{p-1}{2}} \frac{i^p + (p-i)^p}{(i(p-i))^p}.$$
We now make a claim.

Claim
For any prime $p \geq 5$,
$$i^p + (p-i)^p \pmod{p^2} \equiv 0.$$

Proof. Notice that by the Binomial Theorem, the coefficient of the p^0 term is 0, and the coefficient of the p term is 0 when working in $\mathbb{F}_{p^2}$. Hence, we have the required conclusion. $\square$

As a result, it suffices to show that
$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{(i(p-i))^p} \equiv \sum_{i=1}^{\frac{p-1}{2}} -i^{-2p} \equiv \sum_{i=1}^{\frac{p-1}{2}} -i^{-2} \equiv 0 \pmod{p}$$
which is clear from the proof of Wolstenholme's Theorem (for a quick outline, each i^{-2} maps to another distinct number by the properties of inverses, and we may sum all these normally). $\square$

Problem 2.14.11 (Sierpinski)
Prove that for any positive integer s, there is a positive integer n whose sum of digits is s and $s \mid n$.

Notice that it suffices to find a sequence $\{a\}$ of non-negative distinct integers such that
$$\sum_{i=1}^{s} 10^{a_i} \equiv 0 \pmod{s}$$
since one can just add sufficiently many zeros to the end to take care of the factors of 2 and 5. However we can select a_i such that $\phi(s) \mid a_i$ over all i, and then we are done. $\square$

Problem 2.14.12 (ISL 2001/N4)
Let $p \geq 5$ be a prime number. Prove that there exists an integer a with $1 \leq a \leq p-2$ such that neither $a^{p-1} - 1$ nor $(a+1)^{p-1} - 1$ is divisible by p^2.

Notice that there are exactly $p-1$ numbers $1 \le a \le p^2$ such that

$$a^{p-1} \equiv 1 \pmod{p^2}$$

so let these make the set $\mathcal{A}$. In addition, let m be the largest integer such that $a_m \le p-1$. Then, if the given claim is false, then in each pair $\{1,2\}$, $\{3,4\}$, $\dots$, $\{p-2, p-1\}$, at least one of the numbers must be in $\mathcal{A}$. As a result, notice that $m \ge \frac{p-1}{2}$. However, if a is a solution, so it $-a$, so all the solutions in $\mathcal{A}$ must lie in the interval $[1, p-1] \cup [p^2-p+1, p^2-1]$. However, we can clearly give a construction for a number not in this range, simply take the product of the two solutions in the pairs

$$\left\{\frac{p-3}{2}, \frac{p-1}{2}\right\}, \left\{\frac{p+1}{2}, \frac{p+3}{2}\right\}$$

which suffices as long as $p \ge 7$, contradiction. We may manually verify for $p = 5$ that the given assertion is true, so we are done. $\square$

Problem 2.14.13 (USAMO 2018/4)

Let p be a prime, and let $a_1, \dots, a_p$ be integers. Show that there exists an integer k such that the numbers

$$a_1 + k, a_2 + 2k, \dots, a_p + pk$$

produce at least $\frac{1}{2}p$ distinct remainders upon division by p.

Consider the graph G_k where we join two nodes $\{i, j\}$ if and only if

$$k \equiv \frac{a_i - a_j}{j - i} \pmod{p}.$$

Then, it is equivalent to show that there exists some G_k such that there exists at most $\frac{1}{2}p$ edges. Now, notice that the each $\{i, j\}$ will only be counted in one of the graphs $\{G_0, G_1, \cdots, G_{p-1}\}$. As a result, there exists some graph with at most $\frac{1}{p}\binom{p}{2} = \frac{p-1}{2}$ edges, so we find the required conclusion. $\square$

Problem 2.14.14 (Balkan 2016/3)

Find all monic polynomials f with integer coefficients satisfying the following condition: there exists a positive integer N such that p divides $2(f(p)!) + 1$ for every prime $p > N$ for which $f(p)$ is a positive integer. (A monic polynomial has a leading coefficient equal to 1.)

We claim that the only solution is $f(x) = \boxed{x-3}$, which we may verify explicitly easily.

Start by noticing that if $\deg(f) > 1$, then for sufficiently large n, $f(k) > k$ for $n > k$, which should not be allowed. Hence, f is either linear or constant. Clearly, it cannot be constant, so assume it is linear, so that $f(x) = x - c$ for some positive integer c. Now, notice that for any p, we must have that

$$(p-c)! \equiv -\frac{1}{2} \equiv \frac{(p-1)!}{2} \equiv \frac{(p-1)(p-2)(p-3)!}{2} \equiv (p-3)! \pmod{p}.$$

Thus, $c = 1$ and $c = 2$ do not work, while $c = 3$ does work. Henceforth, assume that $c \ge 4$. Then, we know for large primes p, that

$$(p-c)!((p-3)(p-4)\cdots(p-c+1) - 1) \equiv 0 \pmod{p} \implies (-3)(-4)\cdots(-c+1) \equiv 1 \pmod{p}.$$

However, the LHS is constant, and since the RHS expects the LHS to increase, we cannot have this. Hence, the only solution is $f(x) = x + 3$, as required. $\square$

Problem 2.14.15 (Iran MO 2017 Round 3/Final/NT/1)
Let x and y be integers and let p be a prime number. Suppose that there exist relatively prime positive integers m and n such that

$$x^m \equiv y^n \pmod{p}.$$

Prove that there exists an unique integer z modulo p such that

$$x \equiv z^n \pmod{p} \quad \text{and} \quad y \equiv z^m \pmod{p}.$$

Let g be a primitive root modulo p. Then, let $x = g^k$, $y = g^\ell$, and $z = g^r$ so that

$$g^{km} \equiv g^{\ell n} \pmod{p} \implies km \equiv \ell n \pmod{p-1}$$

and we wish to show that there is exactly one r satisfying

$$k \equiv rn \pmod{p-1} \quad \text{and} \quad \ell \equiv rm \pmod{p-1}.$$

Now, since $\gcd(m,n) = 1$, there exists a and b such that $ma + nb = 1$.

We first show that there exists at most one r. Assume there exist at least two, r_1 and r_2. Then, we know that

$$k \equiv r_1 n \equiv r_2 n \pmod{p-1} \quad \text{and} \quad \ell \equiv r_1 m \equiv r_2 m \pmod{p-1}.$$

As a result,

$$\begin{aligned} (r_1 - r_2)n &\equiv 0 \pmod{p-1} \\ (r_1 - r_2)m &\equiv 0 \pmod{p-1}. \end{aligned}$$

Now, multiplying the first equation by b and the second by a and adding, we find that

$$r_1 \equiv r_2 \pmod{p-1}$$

so we have the required conclusion.

We now show that there exists an r. We claim that $r = \ell a + kb$ works. Observe:

$$k \equiv \ell an + kbn \equiv kam + kbn \equiv k \pmod{p-1}$$

and similarly for the other one, as required. □

Problem 2.14.16 (ISL 2015/N3)
Let m and n be positive integers such that $m > n$. Define

$$x_k = \frac{m+k}{n+k}$$

for $k = 1, 2, \ldots, n+1$. Prove that if all the numbers $x_1, x_2, \ldots, x_{n+1}$ are integers, then $x_1 x_2 \cdots x_{n+1} - 1$ is divisible by an odd prime.

Notice that it suffices to show that $x_1 x_2 \cdots x_{n+1} - 1$ cannot be of the form 2^α for some integer α. Now, since

$$n + k \mid m + k \implies n + k \mid m - n$$

over all $k \in \{1, 2, \cdots, n+1\}$, we know that

$$\operatorname{lcm}(n+1, n+2, \cdots, 2n+1) \mid m - n.$$

Now, there exists k such that $\frac{m-n}{n+k}$ has no factors of two, so it must be odd. Adding one, we find that it is even, so the product $x_1 x_2 \cdots x_{n+1}$ must be even as well, and subtracting one makes it odd, as required.

All that is left is to show that it cannot be equal to 1, however this is clear, so we are done. □

Problem 2.14.17 (ELMO 2019/5)

Let $\mathcal{S}$ be a nonempty set of positive integers such that, for any (not necessarily distinct) integers a and b in $\mathcal{S}$, the number $ab+1$ is also in $\mathcal{S}$. Show that the set of primes that do not divide any element of $\mathcal{S}$ is finite.

We begin with a claim.

Claim

Let $\mathcal{S}_p$ be the set $\mathcal{S}$ when reduced modulo p, where p is a prime that does not divide any element of $\mathcal{S}$. We claim that $|S_p| = 1$.

Proof. Assume otherwise. Then, let $\mathcal{S}_p = \{s_1, s_2, \cdots, s_n\}$. Notice that for any $a \in \mathcal{S}_p$,

$$\mathcal{S}_p = \{s_1, s_2, \cdots, s_n\} = \mathcal{S}_p = \{as_1 + 1, as_2 + 1, \cdots, as_n + 1\}.$$

As a result, we must have that

$$s_1 + s_2 + \cdots + s_n \equiv a(s_1 + s_2 + \cdots + s_n) + n \pmod p \implies (a-1)(s_1 + s_2 + \cdots + s_n) \equiv -n \pmod p$$

which needs to be true over all a, which clearly cannot hold, if $n > 2$, as required. □

Hence, if the starting term is x, then we find that

$$x \equiv x^2 + 1 \pmod p \implies p \mid x^2 - x + 1$$

so there are finitely many, as desired. □

Problem 2.14.18

Let a, $b \in \mathbb{N}$ and p be a prime. Prove that

$$\binom{pa}{pb} \equiv \binom{a}{b} \pmod p.$$

This directly follows from Lucas' Theorem. □

Problem 2.14.19

Find a formula for the number of entries in the nth row of Pascal's triangle that are not divisible by p, in terms of the base-p expansion of n.

If $n = (n_k \cdots n_1 n_0)_p$ then the required answer is:

$$\boxed{\prod_{i=0}^{k} (n_i + 1)}$$

which we can show easily by considering digit by digit. □

Problem 2.14.20 (ELMO 2009/6)

Let p be an odd prime and x be an integer such that $p \mid x^3 - 1$ but $p \nmid x - 1$. Prove that

$$p \mid (p-1)! \left(x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots - \frac{x^{p-1}}{p-1} \right).$$

Notice that the given condition is equivalent to $\operatorname{ord}_p(x) = 3$, so $3 \mid p - 1$ and $p \mid x^2 + x + 1$. Then, since

$$\frac{1}{k} \equiv (-1)^{k-1} \frac{1}{p} \binom{p}{k} \pmod{p}$$

we find that

$$x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots - \frac{x^{p-1}}{p-1} \equiv \frac{x}{p}\binom{p}{1} + \frac{x^2}{p}\binom{p}{2} + \cdots + \frac{x^{p-1}}{p}\binom{p}{p-1} \pmod{p}.$$

Hence, it remains to show that

$$x\binom{p}{1} + x^2\binom{p}{2} + \cdots + x^{p-1}\binom{p}{p-1} \equiv 0 \pmod{p^2}$$

or

$$(x+1)^p \equiv x^p + 1 \pmod{p^2}.$$

Let $x^2 + x + 1 = kp$ for some integer k. Then,

$$(kp - x^2)^p \equiv -x^{2p} \equiv x^p + 1 \pmod{p^2}$$

so we need to show

$$x^{2p} + x^p + 1 \equiv \frac{x^{3p} - 1}{x^p - 1} \equiv 0 \pmod{p^2}.$$

However, this is clear, since $x^3 \equiv 1 \pmod{p}$ implies $x^{3p} \equiv 1 \pmod{p^2}$, and since $x^p \not\equiv 1 \pmod{p}$, we have the required conclusion. $\square$

Problem 2.14.21 (ISL 2011/N7)

Let p be an odd prime number. For every integer a, define the number

$$S_a = \frac{a}{1} + \frac{a^2}{2} + \cdots + \frac{a^{p-1}}{p-1}.$$

Let $m, n \in \mathbb{Z}$, such that

$$S_3 + S_4 - 3S_2 = \frac{m}{n}.$$

Prove that $p \mid m$.

Since

$$\frac{1}{k} \equiv (-1)^{k-1} \frac{1}{p} \binom{p}{k} \pmod{p}$$

we know that

$$S_a \equiv \frac{a}{p}\binom{p}{1} - \frac{a^2}{p}\binom{p}{2} + \cdots - \frac{a^{p-1}}{p}\binom{p}{p-1} \equiv \frac{(a-1)^p - a^p + 1}{p} \pmod{p}.$$

Then, it suffices to show that

$$(2^p - 3^p + 1) + (3^p - 4^p + 1) - 3(1 - 2^p + 1) \equiv -2^{2p} + 4 \cdot 2^p - 4 \equiv 0 \pmod{p^2}.$$

However, this can further be simplified to

$$(2^p - 2)^2 \equiv 0 \pmod{p^2} \implies 2^p - 2 \equiv 0 \pmod{p}$$

which is obviously true, as required. □

3 Arithmetic Functions

3.1 Number of Divisors

No problems.

3.2 Sum of Divisors

No problems.

3.3 Euler's Totient Function

Problem 3.3.1

Prove that for all composite n:

$$\phi(n) \leq n - \sqrt{n}.$$

In addition, prove that for all $n \notin \{2, 6\}$,

$$\phi(n) \geq \sqrt{n}.$$

We start with the first part. Consider the smallest prime p dividing n. We know that $p \leq \sqrt{n}$, and there will be exactly n/p multiples of p that are not relatively prime to n. Hence,

$$\phi(n) \leq n - \frac{n}{p} \leq n - \sqrt{n}$$

as required.

We now show the second part. It suffices to show that

$$\prod_{i=1}^{k} (p_i - 1) p_i^{\frac{e_i}{2} - 1} \geq 1$$

where $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, and let $\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$. Now, clearly if $2, 3 \notin \mathcal{P}$ then we have the necessary conclusion as every term would be greater than 1. Hence, we split into cases.

- If $2, 3 \in \mathcal{P}$, then in order for
$$2 \cdot 2^{\frac{e_1}{2} - 1} \cdot 3^{\frac{e_2}{2} - 1} < 1$$
we must have $e_1 = e_2 = 1$, which clearly does not work. However, when multiplying by any other $(p_i - 1) p_i^{\frac{e_i}{2} - 1}$, this must then be at least 1, as required. Hence, 6 does not work.
- If $2 \notin \mathcal{P}$, but $3 \in \mathcal{P}$, then the term
$$2 \cdot 3^{\frac{e_2}{2} - 1}$$
will exceed 1, as required.

- If $2 \in \mathcal{P}$, but $3 \notin \mathcal{P}$, then notice that in order for

$$2^{\frac{e_1}{2}-1} < 1$$

we must have $e_1 = 1$, and then multiplying by any other term will bring it back up. Hence, 2 does not work.

Thus, having exhausted all cases, we have the necessary conclusion. □

Problem 3.3.2 (The Zeta Function)
The zeta function is defined as

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots .$$

Note that this is an infinite sum, and does not always converge to a single value. For instance, $\zeta(-1) = 1 + 2 + 3 + 4 + \cdots$ clearly diverges.

1. Use the integral test to show that $\zeta(s)$ converges if and only if $s > 1$. In particular, show that $\zeta(1)$ diverges.

2. Use the Fundamental Theorem of Arithmetic, prove that

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_{p \text{ prime}} \frac{p^s}{p^s - 1}.$$

3. Use the result above to show that there are an infinite number of primes.

Now, a famous theorem (Basel's problem) states that

$$\frac{1}{1^2} + \frac{1}{2^2} + \cdots = \zeta(2) = \frac{\pi^2}{6}$$

Prove that,

$$\left(\frac{6}{\pi^2}\right) n^2 < \sigma(n)\phi(n) < n^2.$$

We begin with the first part. Notice that

$$\int_1^\infty x^{-s}\, dx = \frac{x^{1-s}}{1-s}\bigg|_1^\infty$$

which clearly diverges is $1 - s > 0$ or $s < 1$. To take care of the $\zeta(1)$ case, notice that

$$\left(\frac{1}{1}\right) + \left(\frac{1}{2} + \frac{1}{3}\right) + \left(\frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7}\right) + \cdots > \frac{1}{2} + \frac{2}{4} + \frac{4}{8} + \cdots$$

which clearly diverges.

We continue with the second part. Notice that the product

$$\prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right)$$

simply generates all the natural numbers starting from 1 since the expansion of the product will lead to every possible prime factorization exactly once. Hence, this is simply equal to $\zeta(s)$.

We continue with the third part. Suppose there are finitely many primes. Then, the product above is finitely, so it converges. However, $\zeta(1)$ actually diverges, which is a contradiction.

We finish with the last part. We start by letting $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then, notice that

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p_i - 1}$$

and

$$\phi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}.$$

Hence,

$$\sigma(n)\phi(n) = \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p_i - 1} \cdot (p_i - 1) p_i^{e_i - 1} = \prod_{i=1}^{k} \left(p_i^{e_i+1} - 1\right)\left(p_i^{e_i - 1}\right) = \prod_{i=1}^{k} p_i^{2e_i} - p_i^{e_i - 1}.$$

Dividing this by n^2, it remains to show that

$$\frac{6}{\pi^2} < \prod_{i=1}^{k} \left(1 - \frac{1}{p_i^{e_i+1}}\right) < 1.$$

The upper bound is clear, and the lower bound follows since for any i, $e_i + 1 \geq 2$, as required. $\square$

3.4 Multiplicative Functions

Problem 3.4.1

Prove

$$\sum_{d \mid n} \mu(d) = \delta(n).$$

Clearly, it is correct for $n = 1$. Now, assume $n \geq 2$ and $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Clearly, it is irrelevant what the exponent of p_i is, so reduce the problem to only consider squarefree n. Then, there will be a -1 if an odd number of p_i are chosen, and 1 is an even number of the p_i are chosen. However, it is well known that

$$\sum_{\alpha \text{ even}} \binom{n}{\alpha} = \sum_{\alpha \text{ odd}} \binom{n}{\alpha}.$$

Hence, we have that the sum is equal to 0 for $n \geq 2$ as required. $\square$

Problem 3.4.2

For a positive integer n we define $f(n)$ as

$$f(n) = \tau(k_1) + \tau(k_2) + \cdots + \tau(k_m)$$

where $1 = k_1 < k_2 < \cdots < k_m = n$ are all divisors of the number n. Find a formula for $f(n)$ in terms of the prime factorization of n.

Notice that we have

$$f(n) = \sum_{d \mid n} \tau(d).$$

Now, since τ is multiplicative, so is f, and as a result, it suffices to calculate it for prime powers. Let $n = p^k$. Then,

$$f(p^k) = \sum_{d \mid p^k} \tau(d) = \frac{(k+1)(k+2)}{2}.$$

Hence, for $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, we find that

$$f(n) = \prod_{i=1}^{m} \frac{(e_i+1)(e_i+2)}{2}$$

as required. $\square$

Problem 3.4.3

Prove that:

1. $\mu * \mathbf{1} = \delta$
2. $\mathbf{1} * \mathbf{1} = \tau$
3. $\mathrm{id} * \mathbf{1} = \sigma$
4. $\phi * \mathbf{1} = \mathrm{id}$.

In addition, show that:

1. $*$ is commutative and associative.
2. The identity of $*$ is δ.
3. $*$ distributes over addition.
4. The convolution of two multiplicative functions is multiplicative.

We start with the first part. The first problem is addressed in Problem 3.4.1, and the second is obvious. The third is also obvious by definition. The fourth is obvious by the fourth problem of the second part, which we show in the relavent section below.

We finish with the second part. Clearly, $*$ is commutative. It is also associative, since both expressions will just equate to

$$\sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3).$$

In addition, it is clear that the identity is δ, since it is only 1 when the input is 1, so

$$f(n) = \delta(1) f(n) = \sum_{d \mid n} \delta(d) f\left(\frac{n}{d}\right).$$

In addition, it clearly distributes over addition, since multiplication and sums distribute over addition as well. Finally, we show that the convolution of two multiplicative functions is also multiplicative. Suppose a and b are natural numbers satisfying $\gcd(a, b) = 1$, and g, h are multiplicative functions. Then,

$$f(ab) = \sum_{d \mid ab} g(d) h\left(\frac{ab}{d}\right) = \left(\sum_{d \mid a} g(d) h\left(\frac{a}{d}\right)\right)\left(\sum_{d \mid b} g(d) h\left(\frac{b}{d}\right)\right) = f(a) f(b)$$

as required. $\square$

Problem 3.4.4

Show that

$$\sigma(n) = \sum_{d|n} \phi(d)\tau\left(\frac{n}{d}\right).$$

In other words, show $\phi * \tau = \sigma$.

We rewrite

$$\tau(n) = \sum_{d|n} \mathbf{1}$$

so that the sum becomes

$$\sigma(n) = \sum_{d|n} \sum_{e|d} \phi\left(\frac{n}{d}\right).$$

Now, swap the sums so that

$$\sigma(n) = \sum_{e|n} \sum_{d|n/e} \phi\left(\frac{n}{de}\right) = \sum_{e|n} \frac{n}{e} = \sigma(n)$$

as required.

Problem 3.4.5

Prove the other direction of the Möbius Inversion formula.

It suffices to show that $f = g * \mu$ implies $f * 1 = g$. However,

$$f = g * \mu \implies f * 1 = (g * \mu) * 1 = g * (mu * 1) = g * \delta = g$$

as required. □

Problem 3.4.6

The idea in Example 3.4.2 is the fact the following:

$$\left\{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n}\right\} = \left\{\left\{\frac{k}{d} : 1 \le k \le d, \gcd(k,d) = 1\right\} : d \mid n\right\}.$$

Remember this idea and use it to prove for any n,

$$\sum_{d|n} \sum_{\substack{1 \le k \le d \\ \gcd(k,d)=1}} \mathbf{1} = n.$$

Use the above to show $\phi * \mathbf{1} = \mathrm{id}$. Is this the same proof as the one we gave in 3.3.1?

This problem is trivial by the given lemma, as it is counting over the exact same objects.

For the second statement, it is the same as the proof given in the book of the fact that $\phi * \mathbf{1} = \mathrm{id}$ since

$$\sum_{\substack{1 \le k \le d \\ \gcd(k,d)=1}} \mathbf{1} = \phi(d).$$

Hence, we are done. □

3.5 Floor and Ceiling Functions

Problem 3.5.1

One result we will use again and again throughout the book is the following: If $n \in \mathbb{N}$ and $x \in \mathbb{R}$, then

$$n \leq x \implies n \leq \lfloor x \rfloor .$$

This helps to strengthen our bounds. Keep this in mind whenever you have real numbers in integer type inequalities!

Since n has no fractional part, we may remove the fractional part from x and the inequality will still hold. Hence, we are done. $\square$

Problem 3.5.2

Let p, $q \in \mathbb{Z}$, $q \neq 0$, and r be the remainder when p is divided by q. Show that

$$\left\lfloor \frac{p}{q} \right\rfloor = \frac{p-r}{q}.$$

If $m = \left\lfloor \frac{p}{q} \right\rfloor$ is the greatest number less than $\frac{p}{q}$, then we know that

$$p = qm + r$$

so subtracting r from both sides and dividing by q finishes. $\square$

Problem 3.5.3

Prove for odd n

$$\left\lfloor \frac{k^n}{p} \right\rfloor + \left\lfloor \frac{(p-k)^n}{p} \right\rfloor = \frac{k^n + (p-k)^n}{p} - 1.$$

We rewrite as follows:

$$\left\lfloor \frac{k^n}{p} \right\rfloor + \left\lfloor \frac{(p-k)^n}{p} \right\rfloor = \left\lfloor \frac{k^n}{p} \right\rfloor + \left\lfloor \frac{((p-k)^n + k^n) - k^n}{p} \right\rfloor .$$

However, this is just equal to

$$\left\lfloor \frac{k^n}{p} \right\rfloor + \left\lfloor \frac{-k^n}{p} \right\rfloor + \frac{(p-k)^n + k^n}{p} = \frac{(p-k)^n + k^n}{p} - 1$$

as required. $\square$

Problem 3.5.4

The function $\tau(n)$ doesn't have a nice formula, and is far from continuous. It is very large at some points and very small at just the next input. However, the average function

$$f(n) = \frac{\tau(1) + \tau(2) + \cdots + \tau(n)}{n}$$

is more stable. Show that $\ln n - 1 \leq f(n) \leq \ln n + 1$. In other words, $f(n) = \Theta(\ln n)$, i.e. growth-wise it behaves like $\ln n$.

We know that

$$\tau(1) + \tau(2) + \cdots + \tau(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor.$$

Now, we first show the lower bound:

$$\begin{aligned}\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor &\geq \frac{n}{1} + \frac{n}{2} + \cdots + \frac{n}{n} - n \\ &= nH_n - n \\ &> n\ln(n) - n\end{aligned}$$

as required. We now show the upper bound:

$$\begin{aligned}\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor &\leq \frac{n}{1} + \frac{n}{2} + \cdots + \frac{n}{n} \\ &= nH_n \\ &\leq n\ln(n) + n\end{aligned}$$

so we are done. $\square$

Problem 3.5.5

Prove that

$$\sigma(1) + \sigma(2) + \cdots + \sigma(n) \leq n^2.$$

This follows from the fact that

$$\sigma(1) + \sigma(2) + \cdots + \sigma(n) \leq \sum_{i=1}^{n} i \left\lfloor \frac{n}{i} \right\rfloor \leq \sum_{i=1}^{n} n = n^2$$

so we are done. $\square$

Problem 3.5.6

Prove that $\sigma(n) < n \ln n$.

Not true; consider $n = 6$. $\square$

3.6 Example Problems

No problems.

3.7 Practice Problems

Problem 3.7.1

Find all $n \in \mathbb{N}$ such that $\lfloor \sqrt{n} \rfloor \mid n$.

Let k be the integer such that
$$k^2 \le n < k^2 + 2k + 1.$$
Then, the condition reduces to $k \mid n$, so n must be of the form k^2, $k^2 + k$, or $k^2 + 2k$ for some positive integer k. $\square$

Problem 3.7.2

Let a, b, n be positive integers with $\gcd(a, n) = 1$. Prove that
$$\sum_k \left\{ \frac{ak + b}{n} \right\} = \frac{n-1}{2}$$
where k runs through a complete system of residues modulo n.

Notice that since a will just permute the elements of k, and so will b, each of
$$\left\{ 0, \frac{1}{n}, \cdots, \frac{n-1}{n} \right\}$$
will occur exactly once, giving a total of $\dfrac{n(n-1)/2}{n} = \boxed{\dfrac{n-1}{2}}$ as required. $\square$

Problem 3.7.3

Let $f(x)$ be defined for all rationals $x \in [0, 1]$. If
$$F(n) = \sum_{k=1}^{n} f\left(\frac{k}{n}\right), \quad G(n) = \sum_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} f\left(\frac{k}{n}\right)$$
then prove that $G = \zeta * F$, where $\zeta(n)$ is the sum of the primitive nth roots of unity.

Notice that $\zeta = \mu$, so the condition is equivalent to showing that $G = \mu * F$. However, undoing the Mobius inversion yields that it is equivalent to show that $G * \mathbf{1} = F$. However, this is clear (as G simply does casework on the simplest form of the fraction), so we are done. $\square$

Problem 3.7.4

Show that for all positive integers n,
$$\left\lfloor \sqrt{n} + \sqrt{n+1} \right\rfloor = \left\lfloor \sqrt{4n+1} \right\rfloor = \left\lfloor \sqrt{4n+2} \right\rfloor = \left\lfloor \sqrt{4n+3} \right\rfloor.$$

Suppose that $k^2 \le 4n + 1 < (k+1)^2$. Then, suppose that $4n + 2 = (k+1)^2$. We find that this is impossible due to the factor of two in the LHS. Suppose that $4n + 3 = (k+1)^2$, but this is impossible since squares cannot be 3 (mod 4). Hence, they all must lie in this range, so they are all equal. Now, we know that

$$\frac{k^2-1}{4} \leq n < \frac{(k+1)^2-1}{4}.$$

If k is even, then notice that the LHS is not an integer, and the ceiling of this is just $\frac{k^2}{4}$. Now, we know that $n < \frac{(k+1)^2}{4}$ by the upper-bound, so we find that

$$\frac{k}{2} \leq \sqrt{n} < \frac{k+1}{2}.$$

Similarly, if k is odd, then the upper bound is not an integer, so taking the ceiling, we find that $n < \frac{(k+1)^2}{4}$, and we get the same conclusion as above. Applying the same logic on $\sqrt{n+1}$, we get that

$$\frac{k}{2} \leq \sqrt{n+1} < \frac{k+1}{2}$$

so adding the two inequalities and taking floors gives the desired result. □

> **Remark**
> The better way to do this is to note that $\sqrt{4n+1} < \sqrt{n} + \sqrt{n+1} < \sqrt{4n+3}$.

Problem 3.7.5

Prove that for any $n \in \mathbb{N}$,

$$\frac{\sigma(n)}{\tau(n)} \geq \sqrt{n}.$$

Let the divisors of n be $d_1, d_2, \cdots, d_{\tau(n)}$. Then, the given statement is just that

$$\frac{d_1 + d_2 + \cdots + d_{\tau(n)}}{\tau(n)} \geq \sqrt[\tau(n)]{n^{\tau(n)/2}}$$

which is just a result of AM-GM. □

Problem 3.7.6 (IMO 1968/6)

Prove that for any positive integer n,

$$\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lfloor \frac{n+2}{4} \right\rfloor + \left\lfloor \frac{n+4}{8} \right\rfloor + \left\lfloor \frac{n+8}{16} \right\rfloor + \cdots = n.$$

Consider the binary representation of $n = (b_k b_{k-1} \cdots b_0)_2$. We know that this sum is just equivalent to the following:

$$b_0 + b_1 + \cdots + b_k + \overline{b_k b_{k-1} \cdots b_1} + \overline{b_k b_{k-1} \cdots b_2} + \cdots + b_k.$$

Now, notice that any singular digit b_i is going to be counted

$$1 + 2^{i-1} + 2^{i-2} + \cdots + 2^0 = 2^i$$

times (for lack of a better term, we also consider the place value it's in in each number), so it will fall into the correct place value in n, and we have the desired conclusion. □

Problem 3.7.7 (INMO 2014/2)
Let n be a natural number. Prove that

$$\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor + \lfloor \sqrt{n} \rfloor$$

is even.

It is equivalent to show that

$$\tau(1) + \tau(2) + \cdots + \tau(n) + \lfloor \sqrt{n} \rfloor$$

is even. Suppose that $\lfloor \sqrt{n} \rfloor$ is odd. Then, we know that $(2k+1)^2 \leq n < (2k+2)^2$ for some non-negative integer k. In that case, notice that the number of $\tau(i)$ where $i \leq n$ that are odd is just the number of perfect squares less than or equal to n, of which there are an odd number. Hence, the total sum will be even. Now, suppose that $\lfloor \sqrt{n} \rfloor$ is even. Then, $(2k)^2 \leq n < (2k+2)^2$ for some non-negative integer k, and the total number of squares less than or equal to n will be even, as desired. Thus, we are done. $\square$