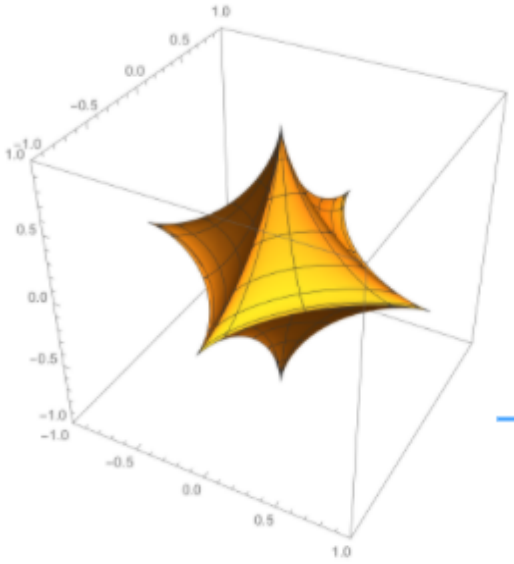
Gaussian Curvature



Number Theory

Lifting The $\sum$ ponent

Aritra Mondal

Mohammad Imran
Aniruddha Sharma

Contents

0.1 Acknowledgements

This handout is one of the many handouts of Gaussian Curvature. This handout is intended for Intermediate to Advanced problem solvers in Number Theory; it covers topics like LTE, Zsigmondy's, Legendre's Formula and etcetra. This handout is authored by Mohammed Imran aka Rama1728, Aniruddha Sharma aka Aniruddha07 and one mysterious alien Aritra12.

Nevertheless also Mr.C, phoenixfire, Aritra12, NJOY and Aryan-23 pointed out numerous errors and refined the manuscript.

We are also thankful to the several users on AoPS who posted problems and solutions and many resources which we noted down or also we forgot some to refer to. We hope that this handout is error free. We also hope that you find this handout helpful.

Remark. No handout is all perfect so there might be typos. If you find any, feel free to mail them at gaussiancurv180@gmail.com

Definition (Typos)— The errors which are done by human beings accidentally!
Note that **not** all authors are human beings so there are no faults of non-humans or aliens..

0.2 Notation

Notation	Meaning
$\mathbb{R}$	The set of reals and $\mathbb{R}^+$ will denote positive reals accordingly.
$\mathbb{N}$	The set of positive integers.
$\mathbb{Z}$	The set of integers
$\mathbb{Q}$	The set of rational numbers
$a \mid b$	a divides b
$\in$	In
$\exists$	There exists
$\forall$	For All
$\gcd(a,b)$	The greatest common divisor of a and b
$\operatorname{lcm}(a,b)$	The least common multiple of a and b.
WLOG	Without loss of generality
FTSOC	For the Sake of Contradiction

Chapter 1

The yoga of *p*-adic valuations

In this chapter, we aim to do a rather detailed study of the p-adic valuations map $v_p : \mathbb{N} \to \mathbb{N}$, where p is a fixed prime.

We now introduce a very important definition: If n is a positive integer more than 1, then $v_p(n)$ is the power of p in the prime factorization of n.

After surfing through the basic properties of the map v_p, we will use them to derive some important and intriguing results.

1.1 Introduction

Let p be a fixed prime. It will be more convenient if we extend the map $v_p : \mathbb{N} \to \mathbb{N}$ to a map $v_p : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ by defining $v_p(n) = v_p(|n|)$ for all $n \in \mathbb{N}/\{0, \pm 1\}$, $v_p(\pm 1) = 0$ and $v_p(0) = \infty$. In other words, we say that $v_p(n)$ is the largest non-negative integer k such that $p^k | n$. In particular, if $v_p(n) \geq 1$, then $p|n$.

We call $v_p(n)$ as the p-adic valuation of n.

After familiarizing ourselves with the definitions, we can now move on to some elementary properties of the map v_p.

`Properties:`

- ☐ For integers a, b and prime p, we have $v_p(ab) = v_p(a) + v_p(b)$
- ☐ For integers a, b with $b|a$ and prime p, we have $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$
- ☐ For integer a and non-negative integer n, we have $v_p(a^n) = nv_p(n)$
- ☐ For integers a, b and prime p with $v_p(a) > v_p(b)$, we have $v_p(a+b) = v_p(b)$

Presented below is a theorem which contains some of the elementary properties of p-adic valuations.

Theorem 1.1.1 (Basic Properties) — a) If n is a non-zero integer, then we can write $n = p^{v_p(n)} \cdot m$, where m is an integer with $\gcd(m,p) = 1$.

b) For each $n > 1$ we have

$$n = \prod_{p|n} p^{v_p(n)}$$

c) For all integers a, b we have

$$v_p(ab) = v_p(a) + v_p(b) \text{ and } v_p(a+b) \geq \min(v_p(a), v_p(b))$$

Proof. a) Note that if $p|n$, and $v_p(n) = k$, then clearly from the definition of the map v_p, we have $p^{v_p(n)} = p^k | n$. So, $n = p^{v_p(n)} \cdot m$ for some integer m. Note that m cannot be divisible by p, as if it was, then $p^{k+1}|n$, implying that $v_p(n) \geq k+1$ contradicting the fact that $v_p(n) = k$. So, we must have $1 = \gcd(m,p) = \gcd\left(m, p^k\right) = \gcd\left(m, p^{v_p(n)}\right)$ and we are done. □

b) Let $n = P_1^{a_1} \cdot P_2^{a_2} \cdots P_k^{a_k}$. Then, note that $v_{P_i}(n) = a_i$ for $i = 1, 2, 3, \cdots k$. Thus,

$$n = \prod_{i=1}^{k} P_i^{a_i} = \prod_{i=1}^{k} P_i^{v_{P_i}(n)} = \prod_{p|n} p^{v_p(n)}$$

and we are done. □

c) Note that this is obvious when one of a or b is 0, so suppose $ab \neq 0$. By a), we can write $a = p^{v_p(a)} \cdot u$ and $b = p^{v_p(b)} \cdot v$, where $\gcd(u,p) = \gcd(v,p) = 1$. Then, $\gcd(uv, p) = 1$ and $ab = p^{v_p(u)+v_p(v)} \cdot (uv)$. Hence $v_p(a) + v_p(b) = v_p(ab)$. Next, $p^{\min(v_p(a), v_p(b))}$ divides both a and b, and hence it divides $a+b$. Therefore, $v_p(a+b) \geq \min\left(v_p(a), v_p(b)\right)$, with equality if and only if $v_p(a) \neq v_p(b)$. □

The following theorem although quite elementary is the root to tackling various complex problems.

Theorem 1.1.2 — If a, b are integers then $a|b$ if and only if $v_p(a) \leq v_p(b)$ for all primes p.

Proof. Without loss of generality, let a and b be non-zero. Then, if $a|b$, and $b = ac$, we have $v_p(b) = v_p(a) + v_p(c) \geq v_p(a)$ for every prime p. Now, assume that $v_p(b) \geq v_p(a)$ for all primes p. Then according to Theorem 1.1.1 b), we have

$$a = \prod_p p^{v_p(a)} \text{ and } b = \prod_p b^{v_p(b)}$$

where the product ranges for all primes p. Since $v_p(a) \leq v_p(b)$ for all primes p, the powers of the primes in the prime factorisation of b is greater than or equal to that of a. Therefore, we have $a|b$, and we may conclude.

Remark. This theorem has an interesting consequence:

If a, b are integers then $a^n | b^n$ if and only if $a|b$

The proof of this is left for the reader as an easy exercise.

Consequently, one may wonder whether or not there exists a connection between powers of integers and their p-adic valuations. The answer is yes. We present a theorem explaining the connection.

Theorem 1.1.3 — Let a and n be positive integers. Then a is a n^{th} power of an integer if and only if $v_p(a) \equiv 0 (\text{mod } n)$.

Proof. First, let $a = b^n$ for some integer b. Then,

$$v_p(a) = v_p(b^n) = nv_p(b) \equiv 0 (\text{mod } n)$$

Next, let $v_p(a) = n \cdot b_p$.Then,

$$a = \prod_p p^{v_p(a)} = \prod_p p^{n \cdot b_p} = \left(\prod_p p^{b_p} \right)^n = b^n$$

and we are done.

Remark. This theorem has an immediate and interesting result:

If a and b are relatively prime numbers such that ab is a perfect n^{th} power, then so are a and b.

The proof of this is left for the reader as an easy exercise.

Lemma 1.1.4 — For all integers a and b we have

$$v_p(\gcd(a,b)) = \min(v_p(a), v_p(b)) \text{ and } v_p(\text{lcm}(a,b)) = \max(v_p(a), v_p(b))$$

Proof. If one of a or b is 0, then this is trivial. Thus, we may assume that $ab \neq 0$. Now let $a = p^{a_1} \cdot a_2 and b = p^{b_1} \cdot b_2$, where a_1 and b_1 are nonnegative integers. Then, $\gcd(a,b) = p^{\min(a_1,b_1)} \cdot \gcd(a_2,b_2)$, where $v_p(a_2) = v_p(b_2) = 0$. Thus, if we assume $a_1 \leq b_1$, then we have

$$v_p(\gcd(a,b)) = v_p(p^{a_1}) + v_p(gcd(a_2,b_2)) = a_1 = \min(v_p(a), v_p(b))$$

where the second-last equality follows from the fact that $v_p(\gcd(a_2,b_2) = 0$(since a_2 and b_2 are not

divisible by p, their gcd is not divisible by p, and hence $v_p(\gcd(a_2,b_2)=0)$. We may now conclude. The proof of the second part of the problem is left as an exercise for the reader.

Remark. Note that, we can generalize this lemma to:

$$v_p\left(\gcd(x_1,x_2,\cdots x_n)\right)=\min_{1\le i\le n} v_p(x_i)$$

and

$$v_p\left(\operatorname{lcm}(x_1,x_2,\cdots x_n)\right)=\max_{1\le i\le n} v_p(x_i)$$

for arbitrary integers $x_1,x_2,\cdots x_n$.

We shall now move on and tackle some concrete and challenging problems.

Problem 1.1.1. Show that a rational number q is an integer if and only if $v_p(q)\ge 0$ for every prime p.

Solution. Let $q=\frac{a}{b}$. Then, $v_p(q)=v_p(a)-v_p(b)$. Thus, it suffices to show that $b\mid a$ if and only if $v_p(a)\ge v_p(b)$, but this is exactly what we showed in Theorem 1.1.2!

Note. Though we defined v_p for the integers, we can also slightly modify it and define it for rationals, and that is possible due to property 2.

Problem 1.1.2. Prove the identity

$$\frac{\operatorname{lcm}(a,b,c)^2}{\operatorname{lcm}(a,b)\cdot\operatorname{lcm}(b,c)\cdot\operatorname{lcm}(c,a)}=\frac{\gcd(a,b,c)^2}{\gcd(a,b)\cdot\gcd(b,c)\cdot\gcd(c,a)}$$

for all positive integers a,b,c.

Solution. Let for all primes p, $v_p(a)=x_p$, $v_p(b)=y_p$ and $v_p(c)=z_p$. Then, taking the p-adic valuations on both sides of the equality we have to prove, it suffices to show that

$$v_p\left(\frac{\operatorname{lcm}(a,b,c)^2}{\operatorname{lcm}(a,b)\cdot\operatorname{lcm}(b,c)\cdot\operatorname{lcm}(c,a)}\right)=v_p\left(\frac{\gcd(a,b,c)^2}{\gcd(a,b)\cdot\gcd(b,c)\cdot\gcd(c,a)}\right)$$

for all primes p. This is equivalent to each of the following:

$$v_p\left(\operatorname{lcm}(a,b,c)^2\right)-v_p\prod_{cyc}\operatorname{lcm}(a,b)=v_p\left(\gcd(a,b,c)^2\right)-v_p\prod_{cyc}\gcd(a,b)$$

$$2v_p(\text{lcm}(a,b,c)) - \sum_{cyc} v_p(\text{lcm}(a,b)) = 2v_p(\gcd(a,b,c)) - \sum_{cyc} v_p(\gcd(a,b))$$

$$2\max(x_p,y_p,z_p) - \sum_{cyc} \max(x_p,y_p) = 2\min(x_p,y_p,z_p) - \sum_{cyc} \min(x_p,y_p)$$

Now, since this equation is symmetric, we can assume that $x_p \le y_p \le z_p$. Then,it suffices to prove that

$$2x_p - x_p - y_p - x_p = 2z_p - z_p - y_p - z_p$$

which is clear. This completes the proof.

Remark. This problem can also be solved using the fact that

$$\text{lcm}(x,y) = \frac{xy}{\gcd(x,y)}$$

The rest of the proof is left for the reader as an easy exercise.

Problem 1.1.3 (IMO 1974 Shortlist). Let $a_1,a_2,\cdots,a_k$ and $b_1,b_2,\cdots,b_k$ be positive integers such that $\gcd(a_i,b_i)=1$ for all $1 \le i \le k$. Prove that

$$\gcd\left(\frac{a_1 m}{b_1}, \frac{a_2 m}{b_2} \cdots, \frac{a_k m}{b_k}\right) = \gcd(a_1,a_2,\cdots,a_k)$$

where $m = \text{lcm}(b_1,b_2,\cdots,b_k)$

Solution. Fix a prime p and let $x_i = v_p(a_i)$ and $y_i = v_p(b_i)$. By hypothesis, we have $\min(x_i,y_i)=0$ for all i and we need to prove that if

$$z = \max(y_1,y_2,\cdots,y_k),$$

then

$$\min(x_1-y_1+z, x_2-y_2+z, \cdots, x_k-y_k+z) = \min(x_1,x_2,\cdots,x_k)$$

Note that $x_i - y_i + z \ge x_i$ for all i, so the right hand side is at least the left hand side. Now, if $z=0$, then our assumption forces all y_i to be 0 and the equality is clear. Otherwise, let $y_j = z > 0$ for some j, forcing $x_j = 0$, implying $x_j - y_j + z = 0$ and we may conclude.

Problem 1.1.4. Prove that for all $n \ge 2$, we have

$$\text{lcm}(1,2,3,\cdots,n) \le n^{\pi(n)}$$

where $\pi(n)$ is the number of primes less than n.

Solution. We prove a claim,

Claim— If $n > 1$ is an integer and p a prime, then

$$v_p(\text{lcm}(1,2,3,\cdots,n)) = \lfloor \log_p(n) \rfloor$$

Proof. By lemma 1.1.4, we have

$$v_p(\text{lcm}(1,2,3,\cdots,n)) = \max_{1\leq i\leq n} v_p(i)$$

Let $k = \lfloor \log_p(n) \rfloor$, so that $p^k \leq n < p^{k+1}$. Then, for any $i \in \{1,2,3,\cdots,n\}$ is i divisile by p^{k+1} and so

$$\max_{1\leq i\leq n} v_p(i) = v_p(p^k) = k$$

as desired. This completes the proof.

Returning to the problem, by our lemma we have

$$p^{v_p(\text{lcm}(1,2,3,\cdots,n))} \leq n$$

and multiplying for all primes p less than n yields the desired result. This settles the proof.

Problem 1.1.5 (IMO 2007 Shortlist). Let $b,n > 1$ be integers. Suppose that for each $k > 1$, there exists an integer a_k such that $b - a_k^n$ is divisible by k. Prove that $b = A^n$ for some integer A.

Solution. Let the prime factorization of b be $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. It suffices to show that all the exponents α_i are divisible by n. Apply the condition for $k = b^2$. The number $b - a_k^n$ is divisible by b^2 and hence, for each $1 \leq i \leq s$, it is divisible by $p_i^{2\alpha_i} > p_i^{\alpha_i}$ as well. Therefore,

$$a_k^n \equiv b \equiv 0 \pmod{p_i^{\alpha_i}}$$

and

$$a_k^n \equiv b \not\equiv 0 \pmod{p_i^{\alpha_{i+1}}}$$

which implies that the largest power of p_i dividing a_k^n is $p_i^{\alpha_i}$. Since a_k^n is a complete n^{th} power, this implies that α_i is divisible by n as desired.

Problem 1.1.6. Prove that

$$\sum_{i=1}^{n} \frac{1}{i}$$

is not an integer for $n \geq 2$.

Solution. The key idea for the problems is to find a prime that divides into the denominator more than in the numerator. Notice that

$$\sum_{i=1}^{n} \frac{1}{i} = \sum_{i=1}^{n} \frac{\frac{n!}{i}}{n!}$$

We consider $v_2\left(\sum_{i=1}^{n} \frac{n!}{i}\right)$. Then, as

$$v_2\left(\frac{n!}{2i-1}\right) > v_2\left(\frac{n!}{2i}\right) = v_2\left(\frac{n!}{2i-1} + \frac{n!}{2i}\right).$$

We then get $v_2\left(\frac{n!}{4i-2}\right) + \left(\frac{n!}{4i}\right) = v_2\left(\frac{n!}{4i}\right)$ and repeating to sum up the factorial in this way we arrive at

$$v_2\left(\sum_{i=1}^{n} \frac{n!}{i}\right) = v_2\left(\frac{n!}{2^{\lfloor \log_2 n \rfloor}}\right)$$

However for $\sum_{i=1}^{n} \frac{1}{i}$ to be an integer we need

$$v_2\left(\sum_{i=1}^{n} \frac{n!}{i}\right) \geq v_2(n!)$$

$$v_2\left(\frac{n!}{2^{\lfloor \log_2 n \rfloor}}\right) \geq v_2(n!)$$

$$0 \geq \lfloor \log_2 n \rfloor$$

a contradiction. This completes the proof.

Problem 1.1.7 (Saint Petersburg Olympiad 2006). Let $a_1, a_2, ..., a_{101}$ be positive integers such that $\gcd(a_1, a_2, \ldots, a_{101}) = 1$ and the product of any 51 of these numbers is divisible by the product of the remaining 50. Prove that $a_1 a_2 \ldots a_{101}$ is a perfect square.

Solution. The problem readily forces us to check if we can show $a_1 a_2 \ldots a_{101}$ is a perfect square and in order to show that $a_1 a_2 \ldots a_{101}$ is a perfect square, it's equivalent to showing that given a prime number p that divides $a_1 a_2 \ldots a_{101}$, we have $v_p(a_1 a_2 \ldots a_{101}) = v_p(a_1) + v_p(a_2) + \ldots + v_p(a_{101})$ is an even integer.

From the given fact that $\gcd(a_1, a_2, \ldots, a_{101}) = 1$, we get $\min\{v_p(a_1), v_p(a_2), \ldots, v_p(a_{101})\} = 0$. This means that there must be at least one a_i such that $v_p(a_i) = 0$. WLOG, let

$v_p(a_1) \geq v_p(a_2) \geq \ldots \geq v_p(a_{101}) = 0$, by the second given property, we have

$$v_p(a_1) + v_p(a_2) + \ldots + v_p(a_{50}) \leq v_p(a_{51}) + v_p(a_{52}) + \ldots + v_p(a_{101})$$

and

$$v_p(a_1) + v_p(a_2) + \ldots + v_p(a_{50}) + v_p(a_{101}) \geq v_p(a_{51}) + v_p(a_{52}) + \ldots + v_p(a_{100}).$$

Now, notice that since $v_p(a_{101}) = 0$, we have

$$v_p(a_1) + v_p(a_2) + \ldots + v_p(a_{50}) \leq v_p(a_{51}) + v_p(a_{52}) + \ldots + v_p(a_{100})$$

and

$$v_p(a_1) + v_p(a_2) + \ldots + v_p(a_{50}) \geq v_p(a_{51}) + v_p(a_{52}) + \ldots + v_p(a_{100})$$

which means

$$v_p(a_1) + v_p(a_2) + \ldots + v_p(a_{50}) = v_p(a_{51}) + v_p(a_{52}) + \ldots + v_p(a_{100})$$

and so

$$v_p(a_1 a_2 \ldots a_{101}) = v_p(a_1) + v_p(a_2) + \ldots + v_p(a_{101}) = 2\left(v_p(a_1) + v_p(a_2) + \ldots + v_p(a_{50})\right).$$

This shows $a_1 a_2 \ldots a_{101}$ is a perfect square.

Problem 1.1.8. Find all positive integers a and b for which $(a+b^2)(a^2+b)$ is a power of 2.

Solution. We will prove that $a = b = 1$ is the unique solution of the problem. Assume that $(a,b) \neq (1,1)$ and without loss of generality, that $a > 1$. Write $a + b^2 = 2^m$ and $b + a^2 = 2^n$ for some $m, n \geq 1$. If a is even then so is b and since $v_2(a) < m = v_2(2^m)$, we have $v_2(2^m - a) = v_2(a)$, thus

$$2v_2(b) = v_2(b^2) = v_2(2^m - a) = v_2(a),$$

and similarly $2v_2(a) = v_2(b)$, contradicting our assumption that $v_2(a) > 0$.
Hence a is odd. If $b > 1$, then a similar argument as above yields

$$v_2(b+1) < v_2(b^2 - 1) = v_2(2^m - (a+1)) = v_2(a+1)$$

and

$$v_2(a+1) < v_2(a^2 - 1) = v_2(2^n - (b+1)) = v_2(b+1)$$

a contradiction. Thus the only possible solution is $(a,b) = (1,1)$.

Problem 1.1.9 (Erdos-Turan). Let $a_1 < a_2 < \cdots$ be an increasing sequence of positive integers. Prove that for any N we can find $i \neq j$ such that $a_i + a_j$ has a prime factor greater than N.

Solution. Fix N and let $p_1, p_2, \cdots p_k$ be all primes not exceeding N. Suppose that for all $i \neq j$, all prime factors of $a_i + a_j$ are among $p_1, p_2, \cdots, p_k$. Fix any positive integer d greater than all the numbers $a_v - a_u$ with $1 \leq u < v \leq k+1$. Fix also $n > (p_1 p_2 \cdots p_k)^d$ and note that for all $1 \leq i \leq n$ we have

$$a_n + a_i > (p_1 p_2 \cdots p_k)^d$$

, thus there is $j_i \in \{1, 2, 3, \cdots, k\}$ such that $v_{p_{i_j}}(a_n + a_i) > d$. Since $j_1, j_2, \cdots, j_{k+1}$ are all between 1 and k, two of them must be equal, say $j_u = j_v$ with $1 \leq u < v \leq k+1$. Let $p = p_{j_u}$, so that

$$v_p(a_n + a_u) > d \text{ and } v_p(a_n + a_v) > d.$$

It follows that $v_p(a_v - a_u) > d$ contradicting the fact that d is greater than $a_v - a_u$. This completes the proof.

Problem 1.1.10 (IMO Shortlist 2009). Let $f : \mathbb{N} \to \mathbb{N}$ be a non-constant function such that $a - b$ divides $f(a) - f(b)$ for all $a, b \in \mathbb{N}$. Prove that there exist infinitely many primes p such that p divides $f(c)$ for some positive integer c.

Solution. Suppose that the conclusion fails and let $p_1, p_2, \cdots, p_k$ be all primes appearing in the prime factorization of the numbers $f(1), f(2), \cdots$. Take any positive integer x and write $f(x) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ for some non-negative integers $\alpha_1, \alpha_2 \cdots \alpha_k$. Let

$$a_s = s p_1^{\alpha_1 + 1} p_2^{\alpha_2 + 1} \cdots p_k^{\alpha_k + 1} \text{ for } s \geq 1.$$

Since a_s divides $f(x + a_s) - f(x)$ and since $v_{p_i}(f(x)) < v_{p_i}(a_s)$, it follows that

$$v_{p_i}(f(x + a_s)) = v_{p_i}(f(x)) \text{ for all } i.$$

But since all prime factors of $f(x + a_s)$ are among $p_1, p_2, \cdots, p_k$, it follows that

$$f(x + a_s) = f(x),$$

and this holds for all $s \geq 1$. But then $x + a_s - 1$ divides $f(x) - f(1) = f(x + a_s) - f(1)$ for all $s \geq 1$, so

$$f(x) = f(1).$$

Since x was arbitrary, this means that f is a constant function, contradicting the hypothesis of the problem. This completes the proof.

Problem 1.1.11 (Tuymaada 2004). Let a, n be positive integers such that $a \geq \text{lcm}(1, 2, \cdots, n-1)$. Prove that there are pairwise distinct prime numbers $p_1, p_2, \cdots, p_n$ such that $p_i \mid a + i$ for $1 \leq i \leq n$.

Solution. Let $b = \text{lcm}(1,2,\cdots,n-1)$, thus $a \geq b$. Consider the numbers

$$x_i = \frac{a+i}{\gcd(a+i,b)}, \quad 1 \leq i \leq n$$

We claim that $x_1, x_2, \cdots, x_n$ are pairwise relatively prime integers and $x_i > 1$ for all i. Note that this immediately implies the result, by taking p_i to be an arbitrary prime divisor of x_i. To prove the claim, note that $x_i > 1$ is clear, since the equality $a+i = \gcd(a+i,b)$ would force $a+1 \leq b$. Assume now that a prime p divides both x_i and x_j, for some $1 \leq i < j \leq n$. Let $k = v_p(b)$. Then

$$\min(v_p(a+i), v_p(a+j)) \leq v_p((a+j)-(a+i)) = v_p(j-i) \leq v_p(b) = k$$

We may assume that $v_p(a+i) \leq k$, but then

$$v_p(x_i) = v_p(a+i) - \min(v_p(a+i), k) = 0,$$

a contradiction. This completes the proof.

Problem 1.1.12 (IMO Shortlist 2011). Let $d_1, d_2, \ldots, d_9$ be pairwise distinct integers. Prove that if x is a sufficiently large integer, then $(x+d_1)(x+d_2)\ldots(x+d_9)$ has a prime divisor greater than 20 .

Solution. We will try to prove this by taking the contrary that $P(x)$ has no prime factors greater than 20and we need to show that x is bounded.
Let $D = \prod_{1 \leq i < j \leq 9} (d_j - d_i)$. Observe for all x that $\gcd(x+d_i, x+d_j) \mid d_j - d_i \mid D$. In particular, for all primes $p \leq 20$,

$$\min\{v_p(x+d_i), v_p(x+d_j)\} \leq v_p(D),$$

so there is at most one $j = 1, \ldots, 9$ with $v_p(x+d_j) > v_p(D)$.
But there are eight primes $p \leq 20$, so by Pigeonhole for some $j = 1, \ldots, 9$, we have $v_p(x+d_j) \leq v_p(D)$ for all p, so $x + d_j \leq D$, implying that x is bounded above by a constant, which is a contradiction as x tends to infinity.

Problem 1.1.13 (APMO 2017). Call a rational number r powerful if r can be expressed in the form $\frac{p^k}{q}$ for some relatively prime positive integers p, q and some integer $k > 1$. Let a, b, c be positive rational numbers such that $abc = 1$. Suppose there exist positive integers x, y, z such that $a^x + b^y + c^z$ is an integer. Prove that a, b, c are all powerful.

Solution. Fix a prime p and look at v_p's. Note $v_p(a) + v_p(b) + v_p(c) = 0$.
Let p be a prime for which $v_p(a) > 0$. WLOG $v_p(c) < 0$; then it follows $v_p(b) < 0$ too.

Then we conclude $y\nu_p(b) = z\nu_p(c)$, so set $\nu_p(b) = -z'k$ and $\nu_p(c) = -y'k$ where $y' = \frac{y}{\gcd(y,z)}$ and $z' = \frac{z}{\gcd(y,z)}$.

$$0 < \nu_p(a) = -\nu_p(b) - \nu_p(c) = k \cdot (y' + z').$$

Thus, in conclusion, whenever $\nu_p(a) > 0$ we have $y' + z'$ divides $\nu_p(a)$.

Problem 1.1.14 (India 2019 TST). Show that there do not exist natural numbes $a_1, a_2, \cdots, a_{2018}$ such that the numbers

$$(a_1)^{2018} + a_2, (a_2)^{2018} + a_3, \cdots, (a_{2018})^{2018} + a_1$$

are all powers of 5

Solution. We love our method of contrary as usual. No sins here to use that as our weapon and therefore we hold on the contrary that all the given sums are powers of 5. For a prime p and a natural number n, let $v_p(n)$ denote the highest exponent of p dividing n. In what follows, indices are considered modulo 2018.

Suppose that 5 divides a_i for some $1 \leq i \leq 2018$. Then clearly 5 divides a_j for all $1 \leq j \leq 2018$. Let k be such that

$$v_5(a_k) = \max\{v_5(a_1), v_5(a_2). \cdots, v_5(a_{2019})\}.$$

Then $v_5(a_k^{2018} + a_{k+1}) = v_5(a_{k+1})$ and hence

$$a_k^{2018} + a_{k+1} \leq a_{k+1},$$

a contradiction. This implies that 5 does not divide a_i for any $i = 1, 2, \cdots, 2018$.

Now let $b_i = a_i^{2018} + a_{i+1}$ for $i = 1, 2, \cdots, 2018$. Without loss of generality, assume $b_1 = \min\{b_1, b_2, \cdots, b_{2018}\}$. Let $b = b_1$. Then since all b_i's are powers of 5 it follows that $b_i \equiv 0 \pmod{b}$ for all $i = 1, 2, \cdots, 2018$. Note that $a_2 \equiv -a_1^{2018} \pmod{b}$. Therefore $a_3 \equiv -a_2^{2018} \equiv -a_1^{2018^2}$. Proceeding similarly, $a_{k+1} \equiv -a_1^{2018^k}$ for $k = 3, 4, \cdots, 2018$; in particular, it follows that b divides $a_1 + a_1^{2018^{2018}}$. Since $(a_1, b) = (a_1, 5) = 1$, we see that b divides $a_1^{2018^{2018}-1} + 1$.

Let d denote the smallest natural number such that $a_1^d \equiv 1 \pmod{b}$. Then d divides $\varphi(b) = 4b/5$. Also, since $a_1^{2018^{2018}-1} \equiv -1 \pmod{b}$ it follows that d is even and that it divides $2(2018^{2018} - 1)$. Therefore d divides the quantity $\gcd(4b/5, 2(2018^{2018} - 1)) = 2$, so $d = 2$ and therefore $b = a_{2018} + a_2$ divides $a_1 + 1$, implying $a_1 = a_2 = 1$ and thus $5|2$, which is absurd. This completes the proof.

Problem 1.1.15 (ELMO 2017 Shortlist). For each integer $C > 1$ decide whether there exist pairwise distinct positive integers $a_1, a_2, a_3, \ldots$ such that for every $k \geq 1$, a_{k+1}^k divides $C^k a_1 a_2 \ldots a_k$

Note. In this solution, we use estimates for $\mathbb{H}_n$ (the nth harmonic number). If you do not know about that, then you can skip this.

Solution. The answer is no. Suppose not for a fixed C. Consider any prime p. Then the problem gives

$$k\nu_p(a_{k+1}) \leq k\nu_p(C) + \nu_p(a_1) + \cdots + \nu_p(a_k). \tag{1.1}$$

Now we have the following key claim (guessed by small values)

Claim— Let $\mathbb{H}_n$ denote the nth harmonic number defined by

$$\mathbb{H}_n = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Then

$$\nu_p(a_n) - \nu_p(a_1) \leq \mathbb{H}_{n-1}\nu_p(C).$$

Proof. The proof is just strong induction on n. Firstly, put $k = 1$ in Equation 1 to get

$$\nu_p(a_2) - \nu_p(a_1) \leq 1\nu_p(C),$$

which serves as the base case since $\mathbb{H}_1 = 1$. Now assume the result till some n. Then putting $k = n$ in Equation 1, we find

$$\begin{aligned} n\nu_p(a_{n+1}) &\leq n\nu_p(C) + \nu_p(a_1) + \nu_p(a_2) + \cdots + \nu_p(a_n) \\ &\leq n\nu_p(C) + \nu_p(a_1) + (\nu_p(a_1) + \mathbb{H}_1\nu_p(C)) + \cdots + (\nu_p(a_1) + \mathbb{H}_{n-1}\nu_p(C)) \\ &= n\nu_p(a_1) + (n + \mathbb{H}_1 + \cdots + \mathbb{H}_{n-1}). \end{aligned}$$

and hence

$$\begin{aligned} \nu_p(a_{n+1}) - \nu_p(a_1) &\leq \frac{1}{n}\left(n + \left(\frac{1}{1}\right) + \cdots + \left(\frac{1}{1} + \cdots + \frac{1}{n-1}\right)\right) \\ &= \frac{1}{n}\left(\left(1 + \underbrace{\frac{1}{2} + \frac{1}{2}}_{2} + \cdots + \underbrace{\frac{1}{n} + \cdots + \frac{1}{n}}_{n}\right) + \left(\frac{1}{1}\right) + \cdots + \left(\frac{1}{1} + \cdots + \frac{1}{n-1}\right)\right) \\ &= \frac{1}{n}\left(n \cdot \frac{1}{1} + n \cdot \frac{1}{2} + \cdots + n \cdot \frac{1}{n}\right) = \mathbb{H}_n. \end{aligned}$$

and the induction is complete.

The key hypothesis we need now is that a_i are pairwise distinct. We want to try to force $\nu_p(a_i)$ to be equal for all primes to get a contradiction. The claim gives $\nu_p(C) = 0 \implies \nu_p(a_n) \leq \nu_p(a_1)$. In particular $\nu_p(a_m)$ is eventually constant. So ignore primes for which $\nu_p(C) = 0$. This means we only have a finite set of prime factors to worry about for the sequence now.
Now we have the following very famous estimate for $\mathbb{H}_N$:

$$\mathbb{H}_n \leq 1 + \log(n+1) \implies \mathbb{H}_n \leq \log n + \log n^2 = 3\log n.$$

(basically $\mathbb{H}_n = \mathcal{O}(\log n)$).
So the claim clearly gives $\nu_p(a_n/a_1) \le A\log n$ for some constant A and all primes p. The idea now is that if we have $\lfloor A\log x \rfloor$ equals some constant w for $x = n, n+1, \ldots, m$, then $\nu_p(a_x) \le w + \nu_p(a_1)$ for $n \le x \le m$. Also, if we can show $w < m-n$, then by Pigeonhole Principle, we would find two i, j such that $\nu_p(a_i) = \nu_p(a_j)$. So if the interval $[n,m]$ is large enough, then this will hold for all primes p (since there are only a finite number of them by our previous assumption), and we would have $a_i = a_j$. So we prove the following:

***Claim*—** For any large k, there exists an interval I of length k such that $\lfloor A\log x \rfloor$ is constant over I and less than k.

Proof. The proof is not as hard as it looks. Firstly, observe that $A\log x < k \iff x < e^{k/A}$. Next,

$$A\log(x+k) - A\log x = A\log\left(1+\frac{k}{x}\right).$$

So even if we pick $x = \left\lfloor e^{k/A} \right\rfloor$, for large enough k the above expression will be very small. Hence we can ensure $A\log(x+k), A\log(x)$ lie between the same two integers.

Problem 1.1.16 (Fake USAMO 2020). Suppose that C is a positive integer and $a_1, a_2, a_3, \ldots$ is an infinite sequence of positive integers satisfying

$$a_{n+1} = \sqrt{a_n^3 - Ca_n}$$

for all positive integers n. Prove that this sequence must be eventually constant, i.e. there exists a positive integer N such that $a_N = a_{N+1} = a_{N+2} = \ldots$.

Solution. Define $\text{rad}(n)$ is the largest square-free factor of n.

We begin by deriving some restrictions on the primes that divide a_n, for any n. Suppose that, for some n, $p \mid a_n$ but $p \nmid C$. Then, $\nu_p(a_n^3 - Ca_n) = \nu_p(a_n)$, so $\nu_p(a_{n+1}) = \frac{\nu_p(a_n)}{2}$. Repeating this, we find that $\nu_p(a_{n+k}) = \frac{\nu_p(a_n)}{2^k}$, which is impossible for sufficiently large k (since $\nu_p(a_{n+k})$ must be an integer). Hence, if $p \mid a_n$, we must have $p \mid C$. Additionally, suppose $p \mid a_{n+1}$ for some $n \ge 1$. Since $p \mid C$, we have

$$\begin{aligned} p &\mid a_n^3 - Ca_n \\ p &\mid a_n^3 \\ p &\mid a_n. \end{aligned}$$

Repeating this, we must have $p \mid a_1$. These two claims together imply that, for all k, we have $\text{rad}(a_k) = \text{rad}(a_1) \mid \text{rad}(c)$ Now, pick $p \mid a_1$. Note that

$$\nu_p(a_{n+1}) = \frac{1}{2}\nu_p(a_n^3 - Ca_n) \ge \frac{1}{2}\min\left(3\nu_p(a_n), \nu_p(C) + \nu_p(a_n)\right) = \frac{1}{2}\left(\nu_p(a_n) + \min\left(2\nu_p(a_n), \nu_p(C)\right)\right),$$

where equality holds unless $\nu_p(a_n) = \frac{1}{2}\nu_p(C)$. We will prove that, for some ℓ, $\nu_p(a_\ell) = \nu_p(C)$. Suppose for some n that $\nu_p(a_n) \leq \frac{1}{2}\nu_p(C)$. In this case,

$$\nu_p(a_{n+1}) \geq \frac{3}{2}\nu_p(a_n).$$

Hence, for some $j > n$, we will have $\nu_p(a_n) > \frac{1}{2}\nu_p(C)$.
Now, suppose $\nu_p(C) > \nu_p(a_n) > \frac{1}{2}\nu_p(C)$. Then, we have

$$\begin{aligned} \nu_p(a_{n+1}) &= \frac{1}{2}\left(\nu_p(a_n) + \nu_p(C)\right) \\ \implies \nu_p(C) &> \nu_p(a_{n+1}) > \nu_p(a_n). \end{aligned}$$

By iterating this, we find that $\nu_p(C) > \nu_p(a_{n+k}) > \nu_p(a_{n+k-1}) > \cdots > \nu_p(a_n)$. As the $\nu_p(a_i)$ and $\nu_p(C)$ are all positive integers, this is impossible for large enough k. Finally, if $\nu_p(a_n) > \nu_p(C) > \frac{1}{2}\nu_p(C)$, we find that

$$\begin{aligned} \nu_p(a_{n+1}) &= \frac{1}{2}(\nu_p(a_n) + \nu_p(C)) \\ \implies \nu_p(a_n) &> \nu_p(a_{n+1}) > \nu_p(C). \end{aligned}$$

By iterating this, we find that $\nu_p(a_n) > \nu_p(a_{n+k}) > \nu_p(a_{n+k-1}) > \cdots > \nu_p(C)$, which is, again, impossible for large k.
The previous two paragraphs imply that, for each n, we either have $\nu_p(a_n) \leq \frac{1}{2}\nu_p(C)$ or $\nu_p(a_n) = \nu_p(C)$. As we cannot have $\nu_p(a_n) \leq \frac{1}{2}\nu_p(C)$ for all n, it follows that we have $\nu_p(a_n) = \nu_p(C)$ for some n. However, if $\nu_p(a_n) = \nu_p(C)$,

$$\nu_p(a_{n+1}) = \frac{1}{2}\left(\nu_p(a_n) + \min\left(2\nu_p(a_n), \nu_p(C)\right)\right) = \nu_p(a_n),$$

implying that the sequence $\{\nu_p(a_i)\}_{i=1}^{\infty}$ is eventually constant. It follows by repeating this argument with every prime $p \mid a_1 \mid C$ (of which there are only finitely many) that the sequence $\{a_i\}$ is eventually constant, so we are done.

1.2 Lifting the Exponent Lemma (LTE)

Now that we are familiar with the basic notations of the map v_p and also on how to use the function v_p to tackle extremely challenging problems in those specific, we will go one step further as we learn about the basics of the celebrated "Lifting the Exponent Lemma".

The lemma, is elegant yet very flexible and not difficult to prove and the heart of the solutions to many of the most challenging problems in the diverse field of Olympiad number theory. In this section, however it has a wide range of application in problems.So as usual practising more and more problem will provide you some experience 'where to use how'.

This section implicates its importance and will give you a breif information about it!

Theorem 1.2.1 (Lifting the Exponent lemma) — Let p be an **odd** prime and let a,b be integers not divisible by p such that $p \mid a-b$. Then for all $n \geq 1$, we have

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n)$$

Proof. Call a positive integer $n \geq 1$ good if it satisfies the above condition. We proceed with a claim,

***Claim*—** If m and n are good, then mn is good.

Proof. Notice that,

$$v_p(a^{mn} - b^{mn}) = v_p((a^m)^n - (b^m)^n) = v_p(a^m - b^m) + v_p(n) = v_p(a-b) + v_p(mn)$$

and we are done.

It is clear that 1 is good, so it suffices to show that any prime q is good. We divide this into two cases,

Case 1. If $q \neq p$

It suffices to show that

$$\frac{a^q - b^q}{a-b} = a^{q-1} + a^{q-2}b + \cdots b^{q-1}$$

is not divisible by p. But this is clear, since

$$a^{q-1} + a^{q-2}b + \cdots b^{q-1} \equiv qa^{q-1} \not\equiv 0 \pmod{p}$$

Case 2. If $p = q$

We can assume that $a = b + p^k c$ for some integer $k \geq 1$ and some positive integer c not divisible by

p. Then, the binomial formula yields,

$$a^p - b^p = p^{k+1}b^{p-1}c + \binom{p}{2}b^{p-2}p^{2k}c + \cdots + p^{kp}c^p$$

Since $p > 2$, the numbers $\binom{p}{2}b^{p-2}p^{2k}c, \cdots, p^{kp}c^p$ have p-adic valuation greater than $k+1$, whence

$$v_p(a^p - b^p) = v_p(p^{k+1}b^{p-1}c) = 1 + k = 1 + v_p(a-b)$$

as desired.

However there we present an interesting form of this theorem

Corollary 1.2.2 — Let p be an **odd** prime and let a, b be integers not divisible by p such that $p \mid a+b$. Then for all **odd** positive integers n, we have

$$v_p(a^n + b^n) = v_p(n) + v_p(a+b)$$

Now we have seen the case when p is an odd prime, but what about the case when $p = 2$? This case is the most interesting, and surprisingly there is a theorem for that as well.

Theorem 1.2.3 — Let x and y be odd positive integers and let n be an **even** positive integer, then

$$v_2(x^n - y^n) = v_2\left(\frac{x^2 - y^2}{2}\right) + v_2(n)$$

Proof. Write $n = 2^k a$ for some integer $k \geq 1$ and some odd positive integer a. Then, we have

$$x^n - y^n = (x^a - y^a)(x^a + y^a)(x^{2a} + y^{2a}) \cdots \left(x^{2^{k-1}a} + y^{2^{k-1}a}\right)$$

and since for any $c, d \in \mathbb{Z}$, we have $c^2 + d^2 \equiv 2 \pmod 4$, the previous relation yields

$$v_2\left(x^n - y^n\right) = v_2\left(x^{2a} - y^{2a}\right) + k - 1$$

Finally since a, x, y are odd, it is easy to observe that $\frac{x^{2a}-y^{2a}}{x^2-y^2} = x^{2(a-1)} + \cdots + x^{2(a-1)}$ which is clearly odd, and this completes the proof.

Now that we are clear with the theory part, let us move on to tackle some concrete and challenging problems.

Problem 1.2.1 (AoPS). Let k be a positive integer.Find all positive integers n such that

$$3^k \mid 2^n - 1$$

Solution. First, notice that $3 \mid 2^n - 1$ then n is even number, $n = 2m$ for some $m \in \mathbb{N}$. Then $3^k \mid 4^m - 1$. By lifting the exponent Lemma, $V_3(4^m - 1) = 1 + V_3(m)$ which gives $V_3(m) \geq k - 1$. So the answer is $n = 2 \cdot 3^{k-1} \cdot l$ for any $l \in \mathbb{N}$

Problem 1.2.2 (AoPS). Find all natural numbers k such that k first prime $p_1, p_2, \ldots, p_k$ then there are exist 2 numbers a,n satisfy

$$p_1 p_2 \ldots p_k - 1 = a^n$$

Solution. Assume that there exists $(k, a, n) \in \mathbb{Z}_+^3$ with $n > 1$ and $k \geq 2$ for which

$$\prod_{i=1}^{k} p_i = a^n + 1.$$

Since $p_2 = 3$, we have $3 \text{—} a^n + 1$, which implies $2 \nmid n$ and $a > 1$. Since

$$\gcd\left(\prod_{i=1}^{k} p_i, a\right) = 1,$$

we have $a > p_k$. So we also have

$$p_k^n < a^n + 1 = \prod_{i=1}^{k} p_i < p_k^k$$

which implies $n < k$. Since $n > 1$ is odd, we can take an odd prime divisor q of n. Since $q < k$, we must have $q \mid a^n + 1$. Since $q \mid n$ and $q \mid a^n + 1$, by LTE, we must have $q^2 \text{—} a^n + 1$. This is clearly impossible. Therefore, $k = 1$ is the only solution.

Problem 1.2.3 (AoPS). Let $p > 2013$ be a prime. Also let a and b be positive integers such that $p \mid a + b$ but $p \nmid (a + b)^2$. If $p^2 \mid a^{2013} + b^{2013}$, then find the number of positive integers $n \leq 2013$ such that $p^n \mid a^{2013} + b^{2013}$.

Solution. We can rewrite the first condition as $v_p(a + b) = 1$. We must also have $v_p\left(a^{2013} + b^{2013}\right) \geq 2$. Now, if $p \nmid a, b$,Well I think you might like to remember something which we have read

Exercise 1.2.1. Can you recall some corollary which will be useful here? Maybe take corollary 1.2.2 into action.

We don't always like to solve our exercises however we spoil it by application of the corollary point out before we get that

$$v_p\left(a^{2013}+b^{2013}\right)=v_p(a+b)+v_p(2013)=1,$$

a contradiction. Thus $p \mid a,b$ and this implies that $p^{2013} \mid a^{2013}+b^{2013}$ and so all values $n \leq 2013$ satisfy $p^n \mid a^{2013}+b^{2013}$ and so the answer is 2013.

Problem 1.2.4 (2007 Brazil TST). Find all integer solutions to the equation

$$\frac{x^7-1}{x-1}=y^5-1.$$

Solution. We proceed with a claim.

Claim— If x is an integer and p is a prime divisor of $\frac{x^7-1}{x-1}=y^5-1$ then we have $p \equiv 1 \pmod 7$ or $p=7$.

Proof. $p|x^7-1$ and $p|x^{p-1}-1$ (Fermat's Little Theorem).Let us assume that 7 does not divide $p-1$.Then $\gcd(p-1,7)=1$,so $p|x^{\gcd(p-1,7)}-1=x-1$,so $\frac{x^7-1}{x-1}=1+x+....+x^6 \equiv 7 \pmod p$ and hence we get $p=7$.This completes the proof of the lemma.

Let k be a positive divisor of $\frac{x^7-1}{x-1}$.Then $k \equiv 0 \pmod 7$ or $k \equiv 1 \pmod 7$.Let us assume that (x,y) is an integer solution of the equation.Then $y-1|\frac{x^7-1}{x-1} \Rightarrow y \equiv 1 \pmod 7$ or $y \equiv 2 \pmod 7$For the first case,$1+y+y^2+y^3+y^4 \equiv 5 \pmod 7$ while in the second case $1+y+y^2+y^3+y^4 \equiv 3 \pmod 7$.This contradicts the fact that a positive divisor of $\frac{x^7-1}{x-1}$ must be congruent to 0 or 1 modulo 7.So we have no solutions.

Problem 1.2.5 (American Mathematical Monthly). Let a, b, c be positive integers such that $c \mid a^c-b^c$. Show that $c \mid \frac{a^c-b^c}{a-b}$.

Solution. Let $v_p(c)=k$ for some prime p and $k \geq 1$. If $p \nmid a-b$, then we obviously have

$$p^k \mid \frac{a^c-b^c}{a-b}$$

Therefore consider $p \mid a-b$. Then using LTE for $p \neq 2$, we have

$$v_p\left(\frac{a^c-b^c}{a-b}\right) = v_p(a-b)+v_p(c)-v_p(a-b) = k$$

When $p=2$, we have

$$v_2\left(\frac{a^c-b^c}{a-b}\right) = v_2(a-b)+v_2(a+b)+v_2(c)-1 \geq v_2(c) = k$$

and the problem is solved in all cases. This completes the proof.

Problem 1.2.6. Let n be a square-free integer. Show that there is no pair of coprime positive integers (x,y) such that

$$(x+y)^3 \mid (x^n+y^n)$$

Solution. Assume $(x+y)^3 \mid (x^n+y^n)$ with $\gcd(x,y)=1$. We will derive a contradiction. First, suppose n is even. If there is an odd prime $p \mid (x+y)$, then $x^n+y^n \equiv x^n+(-x)^n \equiv 2x^n \bmod p$, so $p \mid x$, so $p \mid y$, contradiction. Since x and y are positive, the only possible way that there is no odd prime p dividing $x+y$ is if $x+y$ is a power of 2. In this case, x and y are both odd since they are coprime, so since n is even x^n and y^n are both $1 \bmod 8$, it follows that $v_2(x^n+y^n)=1$, but $v_2\left((x+y)^3\right) \geq 3$, so again we get a contradiction. Now suppose n is odd. If there is an odd prime $p \mid (x+y)$, then $3v_p(x+y) \leq v_p(x^n+y^n)$. Then LTE gives

$$3v_p(x+y) \leq v_p(x^n+y^n) = v_p(x+y)+v_p(n) \leq v_p(x+y)+1$$

since n is square-free. Simplifying, we get $v_p(x+y) \leq \frac{1}{2}$, which is impossible since $p \mid (x+y)$. As above, the only remaining case is when $x+y$ is a power of 2 . But in this case, $v_2(x^n+y^n) = v_2(x+y)$ if n is odd, because x and y are odd and the expansion of

$$\frac{x^n+y^n}{x+y} = x^{n-1}-x^{n-2}y+\cdots-xy^{n-2}+y^{n-1}$$

has an odd number of terms, all of which are odd. So it is impossible for $(x+y)^3$ to divide x^n+y^n, since the power of 2 on the left exceeds the power of 2 on the right.

Problem 1.2.7. Suppose a and b are positive real numbers such that $a-b$, $a^2-b^2, a^3-b^3, \ldots$ are all positive integers. Show that a and b must be positive integers.

Solution. Since $a-b \in \mathbb{Z}$ and $a^2-b^2 \in \mathbb{Z}, a+b = \frac{a^2-b^2}{a-b} \in \mathbb{Q}$. But then $a = \frac{1}{2}(a-b)+\frac{1}{2}(a+b)$ and $b = \frac{1}{2}(a+b)-\frac{1}{2}(a-b)$ are rational numbers as well. Now, write $a = \frac{x}{z}$ and $b = \frac{y}{z}$ as quotients of positive integers, with a common denominator. Choose z as small as possible. Then the conditions

of the problem imply that

$$z^n \mid (x^n - y^n) \text{ for all } n \text{ .}$$

Suppose p is a prime dividing z. Note $z \mid (x-y)$ so $p \mid (x-y)$. If $p \mid x$, then $p \mid y$ as well, but that violates the choice of z : we could write $a = \frac{\frac{z}{p}}{\frac{p}{p}}, b = \frac{\frac{y}{p}}{\frac{p}{p}}$ to get a smaller common denominator. So $p \nmid x, y$ and we are set up to apply LTE. If p is odd, then

$$n \leq v_p(z^n) = v_p(x^n - y^n) = v_p(x-y) + v_p(n).$$

Taking p to both sides gives

$$p^n \leq (x-y)n$$
$$\frac{p^n}{n} \leq (x-y)$$

but this is impossible since the left side tends to infinity as $n \to \infty$, and the right side is a constant independent of n. If $p = 2$, we get

$$n \leq v_2(z^n) = v_2(x^n - y^n) = v_2(x-y) + v_2(n) + v_2(x+y) - 1,$$

so

$$\frac{2^{n+1}}{n} \leq (x-y)(x+y)$$

and we get a similar contradiction. The conclusion is that there is no prime p dividing z. So $z = 1$ and a and b are both positive integers.

Problem 1.2.8 (Russia 1996). Find all positive integers n for which there exist positive integers x, y and k such that $\gcd(x,y) = 1$ and $3^n = x^k + y^k$.

Solution. Note that k must be odd (why?). Now, let p be a prime dividing $x+y$, clearly p is odd. Then by corollary 1.2.2, we have that $v_p(3^n) = v_p(x^k + y^k) = v_p(k) + v_p(x+y) > 0$, as $v_p(x+y) \geq 1 > 0$. Thus, $p \mid 3^k$, implying that $p = 3$. Thus $x + y = 3^m$ for some positive integer m. Note that $n = v_3(k) + m$. We proceed with two cases,

Case 1. If $m > 1$.
We can prove by induction that $3^a \geq a + 2$ for all integers $a \geq 1$, and so we have $v_3(k) \leq k - 2$ (if $v_3(k) = a$, then $v_3(k) + 2 = a + 2 \leq 3^a \leq k$). Let $M = \max(x,y)$. Since $x + y = 3^m \geq 9$, we have $M \geq 5$. Then

$$x^k + y^k \geq M^k = M \cdot M^{k-1} \geq \frac{x+y}{2} \cdot 5^{k-1} = \frac{1}{2} 3^m \cdot 5^{k-1} > 3^m \cdot 5^{k-2} \geq 3^{m+k-2} \geq 3^{m+v_3(k)} = 3^n$$

, a contradiction.

Case 2. If $m = 1$.
Then $x + y = 3$, so $x = 1$ and $y = 2$ (or $x = 2$ and $y = 1$). Thus $3^{1+v_3(k)} = 1 + 2^k$. But note that

$3^{v_3(k)} \mid k$, so $3^{v_3(k)} \leq k$. Therefore

$$1+2^k = 3^{1+v_3(k)} = 3 \cdot 3^{v_3(k)} \leq 3k \implies 2^k + 1 \leq 3k$$

and one can easily see that the only odd value of $k > 1$ satisfying the above inequality is $k = 3$. Thus, $(x,y,n,k) = \{(1,2,2,3),(2,1,2,3)\}$, implying that the only value is $n = 2$.

Problem 1.2.9. (Iran 2008 Round 2) Let a be a natural number. Suppose that $4(a^n+1)$ is a perfect cube for every natural number n. Prove that $a = 1$

Solution. If an odd prime p divides a^n+1 for some n, then $v_p(a^n+1)$ must be divisible by 3 , since $\gcd(p,4) = 1$. This is the key insight.
The expression

$$v_p(a^n+1)$$

motivates us to try LTE and hence why not try ? So, we want the 3 conditions. By assumption, $p > 2$. Also, $p \nmid a$. We just want $p \mid a+1$ and n odd. So let's start by this assumption. Pick an odd prime p divisor of $a+1$, if it exists . Then by Fermat's Little Theorem, $p|a+1|a^{pk}+1$ for all k. So, by LTE

$$v_p\left(a^{pk}+1\right) = v_p(a+1) + v_p(k) + 1 \quad \forall \text{ odd } k$$

We know this is divisible by 3 for all odd k (why do we need odd k?). However, since $v_p(a+1)+1$ is fixed, hence we can choose (odd) k such that $v_p(a+1)+v_p(k)+1 \neq 0 \pmod 3$, which is a contradiction. Hence, our assumption that $a+1$ has an odd prime factor was false. So $a+1$ can't have an odd prime factor.
Write $a+1 = 2^k$. Here's the clever trick now: since $\gcd\left(a^2+1, a+1\right) = \gcd(a+1,2) = 2$, hence a^2+1 will have an odd prime factor p if $k > 1$. So, you can repeat the process above with a^2 instead of a and still get a contradiction (convince yourself that this argument works). Hence, $k = 1$, meaning $a+1 = 2$, i.e. $a = 1$, as needed.

Problem 1.2.10 (AoPS). Find all $f : \mathbb{N} \to \mathbb{N}$ such that:

- There exists $M \in \mathbb{N}$ such that $f(n) \neq 1$ for all $n \geq M$,
- $f(a)^n | f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}$ holds for all $a,b,n \in \mathbb{N}$.

Solution. We proceed with a claim.

***Claim*—** For any natural numbers a, f is either a-periodic (i.e. $f(a+b) = f(b)$ for all $b \in \mathbb{N}$) or $f(a)|a$.

Proof. Suppose that $f(a+b) \neq f(b)$ for some $b \in \mathbb{N}$. Consider any prime number p. Plugging in n yields $f(a)|f(a+b)-f(b)$. Thus, by Lifting The Exponent Lemma, if p is odd,

$$v_p(f(a)^n) \leq v_p\left(f(a+b)^{a^{n-1}} - f(b)^{a^{n-1}}\right)$$
$$nv_p(f(a)) \leq v_p(f(a+b)-f(b)) + (n-1)v_p(a)$$

If $p=2$, one would obtain $nv_2(f(a)) \leq v_2(f(a+b)^2 - f(b)^2) + (n-1)v_p(a) - 1$. Either way, $v_p(f(a)) > v_p(a)$ yields a contradiction for some n big enough, so in fact we have $v_p(f(a)) \leq v_p(a)$ for all p prime, and thus $f(a)|a$.
Otherwise, $f(a+b) = f(b)$ for all $b \in \mathbb{N}$ and f would be a-periodic.

Returning back to the main problem, the lemma implies that if $f(1) \neq 1$, then f is 1-periodic and thus constant. So, now we assume f is non-constant, and thus $f(1) = 1$. By the first point, f cannot be periodic; otherwise there exists $n \geq M$ such that $f(n) = 1$.
Now, fix a positive integer a, and let p be a prime number with $p > \max\{M, a\}$. Then, since $f(p) \neq 1$, we have $f(p) = p$. Hence,

$$p|f(p+a) - f(a)$$

But $0 < f(p+a) \leq p+a < 2p$ and $0 < f(a) \leq a < p$, so $-p < f(p+a) - f(a) < 2p$ and thus we get either $f(p+a) = f(a)$ or $f(p+a) = p + f(a)$. However, if $f(p+a) = f(a)$, then $f(p+a)$ divides both $p+a$ and a. But $\gcd(p+a, a) = \gcd(p, a) = 1$, so $f(p+a) = 1$. But $p+a \geq M$; a contradiction.
Hence, $f(p+a) = p + f(a)$, so $p + f(a) | p+a$. Since $p + f(a) > \frac{p+a}{2}$, then $p + f(a) = p + a$ and thus $f(a) = a$.
Since this holds for all $a \in \mathbb{N}$, we conclude that f is the identity function on $\mathbb{N}$.

1.3 Zsigmondy's Theorem

This is the last section of this chapter. To make this chapter firm, we employ one of the strongest techniques in Olympiad Number Theory, the celebrated Zsigmondy's Theorem. This theorem has cracked numerous amount of challenging Olympiad problems around the world, such as USA(J)MO, IMO, Bulgaria, Balkan, China, India, and many more. This technique lies in the heart in one of the author. We hope you will be able to learn how and when to employ this new technique, though we haven't included the proof.

Before the main theorem, we state what a primitive prime factor is.

Definition— We say that p is a primitive prime factor of $a^n - b^n$, where $a, b, n \in \mathbb{N}$ if p is a prime factor of $a^n - b^n$ and for all $1 \leq k < n$, $p \nmid a^k - b^k$.

Theorem 1.3.1 (Zsigmondy) — Let a and b be relatively prime positive integers. Then, $a^n - b^n$ always has a primitive prime factor for $n \in \mathbb{N}$ with the following exceptions,

- $2^6 - 1^6$
- $n = 2$ and $a + b$ is a power of 2

We now discuss a second variant of Zsigmondy's.

Theorem 1.3.2 (Zsigmondy's Variant) — Let a and b be relatively prime positive integers. Then, there exists a primitive prime factor of $a^n + b^n$, where $n \in \mathbb{N}$ with the following exception: $2^3 + 1^3$

Note. The proof of this uses Zsigmondy, we hope the reader can prove this.

Now that we are clear with the basics, we move on to tackle some concrete problems.

Problem 1.3.1 (Poland 2010). Let p and q be prime numbers with $p > q > 2$. Prove that $2^{pq} - 1$ has at least three prime factors.

Solution. First, note that $2^p - 1$ and $2^q - 1$ are divisors of $2^{pq} - 1$, so we have at least two prime factors with us. Now, since $p > q > 2$, by Zsigmondy, we have that $2^{pq} - 1$ has a primitive prime factor, and hence we have at least three prime factors in addition, completing the proof.

Problem 1.3.2 (IMO 2000 Shortlist). Find all triples (a,m,n) of positive integers that satisfy the divisibility condition

$$a^m+1 \mid (a+1)^n$$

Solution. If $a=1$ then the divisibility condition obviously work. Assume now that $a \geq 2$. If $m=1$ then the divisibility condition obviously work. Assume now that $a \geq 2$, $m \geq 2$. If the two conditions $a=2$, $m=3$ are not both true then by Zsigmondy's there must exist a prime factor p of a^m+1 which does not divide $a+1$ (and of course so does not $(a+1)^n$). Hence there is no solution in this case. It suffices for us to consider the single case $a=2$, $m=3$, in which only all $n \geq 2$ satisfy the divisibility condition. Therefore the solutions are only $(1,m,n),(a,1,n),(2,3,k)$ where $k \geq 2$.

Problem 1.3.3. Find all natural numbers n, k, l, m with $l>1$ such that

$$(1+n^k)^l = 1+n^m$$

Solution. First, note that $k<m$. Next Zsigmondy guarantees the existence of a primitive prime factor of n^m+1 except for $n=2$ and $m=3$. If n and m are not the respective values given, then n^m+1 has a prime divisor not dividing n^k+1, a contradiction. If $n=2$ and $m=3$, we find that $(k,l,m,n)=(1,2,2,3)$ is the only solution.

Problem 1.3.4 (AoPS). Let a and b be positive integers such that $a^n+b^n \mid c^n$ holds for all $n>1$, then show that $a=b$.

Solution. Without loss of generality, let $\gcd(a,b)=1$ because we can just divide both sides of the divisibility by $\gcd(a,b)$ if this is not true. By Zsigmondy's theorem, for $n \geq 3$ and $a \neq b$ we must have that $a^{n+1}+b^{n+1}$ has a prime factor that didn't appear for a^k+b^k and $1 \leq k \leq n$. However, the number of prime factors of c is finite, so sooner or later we will run out of new prime factors of a^k+b^k, contradiction. The only other option is $a=b$, hence proved.

Problem 1.3.5 (Baltic Way 2012). Let $d(n)$ denote the number of positive divisors of n. Find all triples (n,k,p), where n and k are positive integers and p is a prime number, such that

$$n^{d(n)}-1=p^k.$$

Solution. We split the problem into two cases,
Case 1. $n=2$
This immediately gives $p=3$ and $k=1$

Case 2. $n \geq 3$.
f $d(n) \neq 2$, by Zsigmondy's theorem, there exists a prime q such that $q|n^{d(n)}-1, q \nmid n-1$. Since $n-1|n^{d(n)}-1$, this is absurd. Hence $d(n)=2$. Then $(n+1)(n-1)=p^k$. For $s>t\geq 0$,

$$\begin{cases} n+1=p^s \\ n-1=p^t \end{cases}$$

which implies that $2=p^t(p^{s-t}-1)$.If $t=0$,then $p=3, s=1, n=2$ which is absurd. Thus $t\geq 1$ and $p=2, t=1, s=2, n=3, k=3$. which satisfies the condition.

Problem 1.3.6 (Japan MO 2011). Find all of quintuple of positive integers (a,n,p,q,r) such that $a^n-1=(a^p-1)(a^q-1)(a^r-1)$.

Solution. We split the problem into two cases.
Case 1. $a=1$
$(1,n,p,q,r)$ satisfies the condition.
Case 2. $a\geq 2$ Then, $n\geq p,q,r$. We break this into two subcases.

Case 2.1 $n=max\{p,q,r\}$
Without loss of generality, let $n=p$. Obviously $a=2$ and $q=r=1$. By symmetry,$(2,n,n,1,1),(2,n,1,n,1),(2,n,1,1,n)$ satisfy the condition.

Case 2.2 $n>max\{p,q,r\}$
Then, we have $n\geq 2$. We break this further into two subcases.

Case 2.2.1 $n=2$
Thus, $p=q=r=1$ and $(a^2-1)=(a-1)^3$, which implies to and is implied by $a=0,3$. Then $a=3$, and so $(3,2,1,1,1)$ satisfies the condition.

Case 2.2.2 $n\geq 3$
If not $(a,n)=(2,6)$, by Zsigmondy's theorem there is prime number p_0 such that $p_0|a^n-1, p_0\nmid a^p-1, p_0\nmid a^q-1, p_0\nmid a^r-1$ which is absurd. Hence $(a,n)=(2,6)$ and $3^27=(2^p-1)(2^q-1)(2^r-1)$.By $6>p,q,r$,then $(p,q,r)=(3,2,2),(2,3,2),(2,2,3).(2,6,3,2,2),(2,6,2,3,2),(2,6,2,2,3)$ satisfy the condition.

Well you can point out yourselves the answer now by looking over the cases.

Chapter 2

Legendre's Formula

In this chapter, we will discuss Legendre's formula, which finds the p-adic valuation of $n!$. After fully understanding the Legendre's formula, we will move on to some beautiful applications of Legendre's.

2.1 The p-adic valuation of $n!$ (factorial-n)

In this section, we aim to find the exact formula of $v_p(n!)$ for any prime p. Now, if you note that the number of multiples of p in the first n consecutive naturals is just $\lfloor \frac{n}{p} \rfloor$, implying that is the power of p in $n!$. But what about multiples of p that are multiples of p^2 or p^3? This means that the answer is definitely not $\lfloor \frac{n}{p} \rfloor$, so there is a slight catch to evaluate the number $v_p(n!)$, or the exponent of p in the prime factorisation of $n!$. The proof of Legendre uses just this basic fact, but it's applications are really diverse.

Theorem 2.1.1 (Legendre) — For all primes p and positive integers n, we have

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Proof. By basic properties of p-adic valuations, note that

$$v_p(n!) = v_p(1) + v_p(2) + \cdots v_p(n)$$

As pointed out in the introduction of this chapter, there are $\lfloor \frac{n}{p^i} \rfloor$ multiples of p^i in $n!$. Since the number of multiples of p but not p^2 contribute 1 to the sum, the multiples of p^2 but not p^3 contribute 2 to the sum,$\cdots$ we have that

$$v_p(n!) = \left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + 2\left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + 3\left(\left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^4} \right\rfloor \right) + \cdots$$

which telescopes to the desired formula.

We shall now move on to some concrete examples.

Problem 2.1.1 (China 2004 TST). Let $m_1, m_2, \ldots, m_r$ and $n_1, n_2, \ldots, n_s$ be positive integers such that for any integer $d > 1$, there are more or equal multiples of d in $m_1, m_2, \ldots, m_r$ than those of $n_1, n_2, \ldots, n_s$. Prove that $n_1 n_2 \cdots n_s \mid m_1 m_2 \cdots m_r$.

Solution. Let M_d and N_d be the number of multiples of d in $m_1, m_2, \ldots, m_r$ and $n_1, n_2, \ldots, n_s$ respectively. By hypothesis, we have $M_d \geq N_d$ for all $d > 1$. Therefore, for all primes p, we have

$$v_p(m_1 m_2 \cdots m_r) = M_p + M_{p^2} + \cdots + M_{p^n} + \cdots \geq N_p + N_{p^2} + \cdots + N_{p^n} + \cdots = v_p(n_1 n_2 \cdots n_s)$$

where the above equation follows from equivalent arguments as in the proof of Legendre's Formula.

Problem 2.1.2 (USAMO 2016). Prove that for any positive integer k,

$$(k^2)! \cdot \prod_{j=0}^{k-1} \frac{j!}{(j+k)!}$$

is an integer.

Solution. We need to prove that $(k^2)! \cdot \frac{1! \cdots (k-1)!}{k! \cdots (2k-1)!} \in \mathbb{Z}$. Applying Legendre's formula, it suffices to prove

$$\sum_{i=0}^{k-1} \left\lfloor \frac{k+i}{p^i} \right\rfloor \leq \left\lfloor \frac{k^2}{p^i} \right\rfloor + \sum_{i=0}^{k-1} \left\lfloor \frac{i}{p^i} \right\rfloor,$$

for any $p < 2k$ prime. Since $\lfloor a \rfloor + 1 > a$ so it's suffices to prove that

$$\frac{k^2}{p^i} > \sum_{j=0}^{k-1} \left(\left\lfloor \frac{k+j}{p^i} \right\rfloor - \left\lfloor \frac{j}{p^i} \right\rfloor \right).$$

We prove this by induction. Assume that it's true for k, we need to prove that it's also true for $k+1$, or

$$\frac{(k+1)^2}{p^i} > \sum_{j=0}^{k} \left(\left\lfloor \frac{k+1+j}{p^i} \right\rfloor - \left\lfloor \frac{j}{p^i} \right\rfloor \right).$$

Indeed, using $\lfloor a+b\rfloor - 1 \leq \lfloor a\rfloor + \lfloor b\rfloor \leq \lfloor a+b\rfloor$ and the induction hypothesis we have

$$\begin{aligned}
\frac{(k+1)^2}{p^i} &= \frac{k^2}{p^i} + \frac{2k+1}{p^i}, \\
&\geq \sum_{j=0}^{k-1}\left(\left\lfloor\frac{k+j}{p^i}\right\rfloor - \left\lfloor\frac{j}{p^i}\right\rfloor\right) + 1 + \frac{2k+1}{p^i}, \\
&= \sum_{j=0}^{k}\left(\left\lfloor\frac{k+1+j}{p^i}\right\rfloor - \left\lfloor\frac{j}{p^i}\right\rfloor\right) + \left(\frac{2k+1}{p^i} - \left\lfloor\frac{2k+1}{p^i}\right\rfloor\right) + \left(2\left\lfloor\frac{k}{p^i}\right\rfloor - \left\lfloor\frac{2k}{p^i}\right\rfloor + 1\right), \\
&\geq \sum_{j=0}^{k}\left(\left\lfloor\frac{k+1+j}{p^i}\right\rfloor - \left\lfloor\frac{j}{p^i}\right\rfloor\right).
\end{aligned}$$

We are done.

Problem 2.1.3 (RMM 2009). For $a_i \in \mathbb{Z}^+$, $i = 1,\ldots,k$, and $n = \sum_{i=1}^{k} a_i$, let $d = \gcd(a_1,\ldots,a_k)$ denote the greatest common divisor of $a_1,\ldots,a_k$. Prove that

$$\frac{d}{n}\cdot\frac{n!}{\prod_{i=1}^{k}(a_i!)}$$

is an integer.

Solution. The main idea is to observe that we can rewrite this as

$$\text{To prove } \frac{n}{d} \text{ divides } \binom{n}{a_1, a_2, \cdots, a_k}$$

Let p be a prime divisor of the LHS. It therefore suffices to show that for each $1 \leq i \leq k$

$$v_p(n) - v_p(a_i) \leq v_p(n!) - \sum_{l=1}^{k} v_p(a_l!)$$

By Legendre's formula, we have each of the following identities,

$$\begin{aligned}
v_p(n!) &= \sum_{j=1}^{\infty}\left\lfloor\frac{n}{p^j}\right\rfloor \\
v_p(n) &= v_p(n!) - v_p((n-1)!) \\
&= \sum_{j=1}^{\infty}\left(\left\lfloor\frac{n}{p^j}\right\rfloor - \left\lfloor\frac{n-1}{p^j}\right\rfloor\right)
\end{aligned}$$

Thus, it suffices to show that

$$\sum_{j=1}^{\infty}\left(\left\lfloor\frac{n}{p^j}\right\rfloor - \left\lfloor\frac{n-1}{p^j}\right\rfloor - \left\lfloor\frac{a_i}{p^j}\right\rfloor + \left\lfloor\frac{a_i-1}{p^j}\right\rfloor\right) \leq \sum_{j=1}^{\infty}\left(\left\lfloor\frac{n}{p^j}\right\rfloor - \left\lfloor\sum_{l=1}^{k}\frac{a_l}{p^j}\right\rfloor\right)$$

It remains to show that for all $j \in \mathbb{N}$ and $1 \leq i \leq k$

$$\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n-1}{p^j} \right\rfloor - \left\lfloor \frac{a_i}{p^j} \right\rfloor + \left\lfloor \frac{a_i - 1}{p^j} \right\rfloor \leq \left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \sum_{l=1}^{k} \frac{a_l}{p^j} \right\rfloor$$

which reduces to

$$\left\lfloor \frac{n-1}{p^j} \right\rfloor \geq \sum_{l \neq i} \left(\left\lfloor \frac{a_l}{p^j} \right\rfloor \right) + \left\lfloor \frac{a_i - 1}{p^j} \right\rfloor$$

But this follows from the fact that for any reals a and b, we have

$$\lfloor a+b \rfloor \geq \lfloor a \rfloor + \lfloor b \rfloor$$

Details are left to the reader. This completes the proof.

We will look over a cool theorem that can be used to solve many cool problems using p-adic valuations that are 'inequality based'. But the proof of this is beyond the scope of this handout.

Theorem 2.1.2 — For all $n > 1$ and primes p, we have that

$$\frac{n}{p} - 1 < v_p(n!) < \frac{n}{p-1}$$

We show one cool example implying it's importance! The example is from MEMO of year 2015.

Problem 2.1.4 (MEMO 2015). Find all pairs (a,b) of positive integers such that

$$a^b + b^a = a! + b!$$

Solution. WLOG, let $a \leq b$. If $a = 1$, the equation becomes $b! = b$, so $(a,b) = (1,1),\ (1,2),\ (2,1)$. Suppose now that $a \geq 2$. Then, $a^b - b! = b^a - a! \geq a^a - a! > 0$, thus $b! > a^b$. On the other hand, by AM-GM Inequality, we have that

$$b! = 1 \cdot 2 \cdot 3 \cdots b \leq \left(\frac{b(b+1)}{2b} \right)^b = \left(\frac{b+1}{2} \right)^b$$

which implies that $2a < b+1$. Thus, $b \geq 2a$.
Suppose p be a prime divisor of a. Then, $p \mid a! + b!$ and $p \mid a^b$ and hence $p \mid b$. Therefore, $v_p(a^b + b^a) \geq a$. On the other hand, since $b \geq 2a$, we have that $p \mid (a+1) \cdot (a+2) \cdots b$, hence

$$v_p(a! + b!) = v_p(a!) + v_p\left(1 + (a+1) \cdot (a+2) \cdots b\right) < a$$

which follows obviously.

Exercise 2.1.1. Can you determine how the last inequality follows? In case search in context previously in this handout !

But this gives $a < a$, a contradiction. Thus the only solutions are $(a,b) = (1,1),\ (1,2),\ (2,1)$.

Chapter 3

Practice Problems

We have now come to the end of the handout, and we therefore conclude with a set of practice problems.

3.1 Introduction and LTE

Exercise 3.1.1. Prove that $\gcd(a,b) \times \operatorname{lcm}(a,b) = a \times b$

Exercise 3.1.2. Let a and b be integers such that

$$a \mid b^2 \mid a^3 \mid b^4 \cdots$$

Show that $a \mid b$.

Exercise 3.1.3. Prove that

$$1 + \frac{1}{3} + \cdots + \frac{1}{2n-1}$$

is not an integer.

Exercise 3.1.4. Let a, b, and c be integers such that

$$\frac{ab}{c} + \frac{ac}{b} + \frac{bc}{a}$$

is an integer. Prove that each of the numbers

$$\frac{ab}{c}, \frac{ac}{b}, \text{ and } \frac{bc}{a}$$

is an integer.

Exercise 3.1.5 (Polish Junior)**.** Let a and b be positive odd integers such that $a^b b^a$ is a perfect square. Show that ab is a perfect square.

Exercise 3.1.6. Find all positive integers a and b such that $\left(a+b^3\right)\left(b+a^3\right)$ is a power of 3.

Exercise 3.1.7 (Iran TST 2013)**.** Find all arithmetic progressions $a_1, a_2, \cdots$ of positive integers for which there is an integer $N > 1$ such that for all $k \geq 1$,

$$a_1 a_2 \cdots a_k \mid a_N a_{N+1} \cdots a_{N+k}$$

Exercise 3.1.8 (Canada)**.** Find all positive integers n such that $2^{n-1} \mid n!$

Exercise 3.1.9 (2019 USA TSTST)**.** Let $f : \mathbb{Z} \to \{1, 2, \ldots, 10^{100}\}$ be a function satisfying

$$\gcd(f(x), f(y)) = \gcd(f(x), x-y)$$

for all integers x and y. Show that there exist positive integers m and n such that $f(x) = \gcd(m+x, n)$ for all integers x.

Exercise 3.1.10 (RMM 2018)**.** Let a, b, c, d be positive integers such that $ad \neq bc$ and $\gcd(a, b, c, d) = 1$. Prove that as n runs through the positive integers, the value $\gcd(an+b, cn+d)$ may achieve, form the set of all positive divisors of some integer.

Exercise 3.1.11 (China 2016 TST)**.** Let $c,d \geq 2$ be naturals. Let $\{a_n\}$ be the sequence satisfying $a_1 = c, a_{n+1} = a_n^d + c$ for $n = 1,2,\cdots$. Prove that for any $n \geq 2$, there exists a prime number p such that $p|a_n$ and $p \not| a_i$ for $i = 1,2,\cdots n-1$.

Exercise 3.1.12 (USAMO 2009)**.** Let $s_1, s_2, s_3, \ldots$ be an infinite, nonconstant sequence of rational numbers, meaning it is not the case that $s_1 = s_2 = s_3 = \ldots$. Suppose that $t_1, t_2, t_3, \ldots$ is also an infinite, nonconstant sequence of rational numbers with the property that $(s_i - s_j)(t_i - t_j)$ is an integer for all i and j. Prove that there exists a rational number r such that $(s_i - s_j)r$ and $(t_i - t_j)/r$ are integers for all i and j.

Exercise 3.1.13 (Saint Petersburg 2020)**.** The sequence a_n is given as

$$a_1 = 1, a_2 = 2 \quad \text{and} \quad a_{n+2} = a_n(a_{n+1} + 1) \quad \forall n \geq 1$$

Prove that a_{a_n} is divisible by $(a_n)^n$ for $n \geq 100$.

Exercise 3.1.14 (2012 ARMO)**.** For a positive integer n define $S_n = 1! + 2! + \ldots + n!$. Prove that there exists an integer n such that S_n has a prime divisor greater than 10^{2012}.

Exercise 3.1.15. Call a sequence of positive integers $\{a_n\}$ good if for any distinct positive integers m, n, one has

$$\gcd(m,n) \mid a_m^2 + a_n^2 \quad \text{and} \quad \gcd(a_m, a_n) \mid m^2 + n^2.$$

Call a positive integer a to be k-good if there exists a good sequence such that $a_k = a$. Does there exists a k such that there are exactly 2019 k-good positive integers?

Exercise 3.1.16 (BMO 2018)**.** Find all primes p and q such that $3p^{q-1} + 1$ divides $11^p + 17^p$

Exercise 3.1.17. Let x, y be non-negative integers. Prove that there exist finitely many non-negative integers n such that $\left(x + \frac{1}{2}\right)^n + \left(y + \frac{1}{2}\right)^n$ is an integer.

Exercise 3.1.18 (2013 JBMO TST). Find all positive integers x, y, z with z odd, which satisfy the equation:

$$2018^x = 100^y + 1918^z$$

Exercise 3.1.19 (2010 Indonesia TST). Let n be a positive integer with $n = p^{2010}q^{2010}$ for two odd primes p and q. Show that there exist exactly $\sqrt[2010]{n}$ positive integers $x \leq n$ such that $p^{2010} | x^p - 1$ and $q^{2010} | x^q - 1$.

3.2 Zsigmondy's Theorem

Exercise 3.2.1 (2017 Japan TST). Find all positive integers k such that there exist positive integer sequences $a_1, a_2, \ldots$ and $r_1, r_2, \ldots$ satisfying the following conditions: - $a_1 < a_2 < a_3 < \ldots$ - $a_1^k + a_2^k + \ldots + a_n^k = (a_1 + a_2 + \ldots + a_n)^{r_n}$ holds for all positive integers n

Exercise 3.2.2. Find all pairs of natural numbers (m, n) for which $2^m 3^n + 1$ is the square of some integer.

Exercise 3.2.3. Let $p_1, p_2, \ldots, p_n$ be distinct primes greater than 3 . Show that $2^{p_1 p_2 \cdots p_3} + 1$ has at least 4^n divisors.

Exercise 3.2.4. If $a^n + b^n \mid c^n$, for all n , then prove that $a = b$.

3.3 Legendre's Formula

Exercise 3.3.1 (Saint Petersburg 2007). Find all positive integers n and k for which

$$1^n + 2^n + \cdots + n^n = k!$$

Exercise 3.3.2 (AMM). Let $n \geq 1$ be an integer. Prove that

$$(n+1)\operatorname{lcm}\left(\binom{n}{0}, \binom{n}{1}, \cdots, \binom{n}{n}\right) = \operatorname{lcm}(1,2,\cdots,n+1)$$

Exercise 3.3.3 (Russia 2012). Prove that there is a positive integer n such that $1!+2!+\cdots+n!$ has a prime factor greater than 10^{2012}

Exercise 3.3.4 (2007 Romania TST). Solve over the positive integers, the equation

$$x^{2007} - y^{2007} = x! - y!$$

Exercise 3.3.5 (Mathematical Reflections). Define a sequence $(a_n)_{n\geq 1}$ by $a_1 = 1$ and $a_{n+1} = 2^n(2^{a_n} - 1)$. Prove that $n! \mid a_n$ for all $n \geq 1$.

References

[1] Number Theory Concepts and Problems

[2] Art of Problem Solving

[3] Problems from around the world

[4] Blogs on AoPS

[5] Olympiad Number Theory Through Challenging Problems

[6] MONT

If we missed any reference feel free to PM us !