Olympiad Number Theory Through Challenging Problems

Authors
Justin Stevens

Editor and LaTeX Manager
David Altizio

Dedicated to my sister Justin

Contents

0

Introduction

0.1 Hello and problem solving tips

In this text, we attack many hard math problems using simple methods and formulae. Each section begins with a theorem or general idea, along with a fully rigorous proof. By the end of this text, I hope the reader has mastered the method of induction. Each section is then filled with problems off of the main idea of the section. Instead of including many computational problems, we begin with a few "easier" problems and then dig right into olympiad problems. While this may be hard or challenging to those just getting acquainted with mathematics, through personal experience, this is the best way to learn number theory. I highly recommend the reader spends time on each and every problem before reading the given solution. If you do not solve the problem immediately, do not fret, it took me a very long time to solve most of the problem myself.[1] A few general tips for solving hard number theory problems:

- Experiment with small cases. For example, while solving the following problem:

  Example 0.1.1 (2007 ISL). *Let $b, n > 1$ be integers. For all $k > 1$, there exists an integer a_k so that $k \mid (b - a_k^n)$. Prove that $b = m^n$ for some integer m.*

[1] Disclaimer: I did not solve all of the problems myself, the solutions that were reworded are sourced accordingly with numbers.

I first off tried $n = 2$ then $n = 3$ until I finally got the main idea that broke through the problem (this problem is included later in the text).

- Simplify the problem. For example, while solving the following problem:

> **Example 0.1.2** (China TST 2009)**.** *Let $a > b > 1$ be positive integers and b be an odd number, let n be a positive integer. If $b^n \mid a^n - 1$ prove that $a^b > \frac{3^n}{n}$.*

I first off simplified the problem to just the case where b is prime, and later proceeded to solve the full problem. This problem is also included later in the text (in the lifting the exponent section).

- Find patterns. Make a table. For example, when observing 2^n modulo 5, we observe that

n	$2^n \pmod 5$
0	1
1	2
2	4
3	3
4	1
5	2
6	4
7	3

We hypothesize that $2^n \equiv 2^{n \pmod 4} \pmod 5$. We later go on to prove this and other important relationship in the modular section.

- Use problem solving techniques found throughout this book. Many techniques are repeated throughout many problems. One of the most famous techniques used to show that $n \nmid 2^n - 1$ when $n > 1$ is to let p be the smallest prime divisor of n. This technique is very important, and later showed up on two IMO problems!

Spend your time and struggle through the problems, and enjoy this text!

0.2 Motivation

When reading solutions to problems, the reader is often left to wonder "how would someone go about solving that". The solution makes sense, but to readers that attempted the problems themselves, they are left to wonder. Because of this, for more challenging problems, I provide the problem solving steps I took when solving the problem. The reader may choose to skip the motivated solution if they wish, as the fully rigorous solution is also included, however, I recommend taking a look especially if the reader wants to fully understand the problem solving strategies illustrated above.

0.3 Terminology and definitions

To make sure we are all caught up on the same page, we begin this book with some basic terminology and definitions. If you are unfamiliar with any of the stuff below, we suggest you visit these topics in further detail as they are assumed knowledge throughout the text. Later in this text, we revisit all of these topics

0.3.1 Sets

- The real numbers $\mathbb{R}$ are any positive or negative number including 0, such as $1, 1+\sqrt{2}, -\pi, e$, etc
- The integers $\mathbb{Z}$ are defined as the integers:
  $$\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$
  $\mathbb{Z}^+$ denotes the positive integers $\{1, 2, 3, \cdots\}$ while $\mathbb{Z}^-$ denotes the negative integers $\{\cdots, -3, -2, -1\}$.
- The natural numbers $\mathbb{N}$ are defined as the positive integers or $\mathbb{Z}^+$. The natural numbers including 0 are defined as $\mathbb{N}^0$.
- The rational numbers $\mathbb{Q}$ are defined as the ratio of two integers, such as $\frac{2}{3}$ or $\frac{17}{29}$.
- The complex numbers $\mathbb{C}$ are defined as $a + bi$ where $a, b \in \mathbb{R}$.
- The set of polynomials with integer coefficients is defined as $\mathbb{Z}[x]$. For example, $x^3 - 19x^{18} + 1 \in \mathbb{Z}[x]$, however, $x^2 - \pi x \notin \mathbb{Z}[x]$.

- The set of polynomials with rational coefficients is defined as $\mathbb{Q}[x]$. For example, $x^2 - \frac{1}{2}x \in \mathbb{Q}[x]$.

0.3.2 Divisibility

We say that a divides b if $\frac{b}{a}$ is an integer. For example, 4 divides 12 since $\frac{12}{4} = 3$, however, 4 does not divide 13 since $\frac{13}{4} = 3.25$. We write a divides b as $a \mid b$. In this, b is also a multiple of a. **In this text, when we say "divisors" we assume positive divisors.** When considering divisors of natural n, we only have to work up to $\sqrt{n}$. The reason for this is if $n = ab$ then we obviously cannot have $a, b > \sqrt{n}$.

0.3.3 Induction

Induction is a proof technique used often in math. As it can be tricky to those who are understanding it for the first time, we begin with an example problem and explain the method of induction as we solve this problem.

Example 0.3.1. *Show that for all natural n, $1+2+3+\cdots+n = \frac{n(n+1)}{2}$.*

Solution. In induction, we first off have to show a statement holds for a base case, typically $n = 1$. In this case,

$$1 = \frac{1 \times 2}{2}$$

so the base case holds. We now show that if the problem statement holds for $n = k$, then it holds for $n = k+1$. This essentially sets off a chain, where we have

$$n = 1 \implies n = 2 \implies n = 3 \implies \cdots$$

The reason we have to show the base case is because it is the offseter of the chain. Because of this reason, we can think of induction as a chain of dominoes. Once we knock down the first domino, and show that hitting a domino will knock down the proceeding domino, we know all the dominoes will be knocked down. Our inductive hypothesis is that the problem statement holds for $n = k$, or henceforth

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$$

We now need to show that it holds for $n = k + 1$ or we need to show that $1 + 2 + 3 + \cdots + (k + 1) = \frac{(k+1)(k+2)}{2}$. Now, notice that

$$\begin{aligned} 1 + 2 + 3 + \cdots + (k + 1) &= (1 + 2 + 3 + \cdots + k) + k + 1 \\ &= \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2} \end{aligned}$$

As desired. Therefore, we have completed our induction. □

Theorem 0.3.1 (Induction)**.** *Let's say we have a statement $P(n)$ that we wish to show holds for all natural n. It is sufficient to show the statement holds for $n = 1$ and that $P(k) \implies P(k+1)$ for natural k, then the statement is true for all natural n.*

NOTE: *The statement $P(k) \implies P(k+1)$ means that if $P(k)$ is true (meaning the statement holds for $n = k$), then $P(k+1)$ is true. This is used for ease of communication.*

Proof. We use the **well ordering principle**. The well ordering principle states that every set has a smallest element. In this case, assume that for sake of contradiction, $P(n)$ is not true for some $n = x \in S$. Let y be the smallest element of S and since $y > 1$ (from us showing the base case), we have $y - 1 \geq 1$. Therefore $P(y-1)$ is true. We also know that $P(k) \implies P(k+1)$. Therefore, $P(y-1) \implies P(y)$, contradiction. □

Theorem 0.3.2 (Strong induction)**.** *For a statement $P(n)$ that we wish to show holds for all natural n, it is sufficient to show a base case $(n = 1)$ and that if $P(n)$ is true for $n \in \{1, 2, 3, \cdots, k\}$ it implies $P(k+1)$ is true.*

Proof. The proof is identical to the above proof verbatum. □

It is assumed the reader has prior knowledge of induction, so this should be review. If induction is still confusing at this point, we recommend the reader reads up on induction as it is vital for this text.

0.3.4 Other

This section includes formulas it is assumed the reader knows.

Theorem 0.3.3 (Binomial Theorem)**.** *For n natural,*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

Definition 0.3.1. The greatest common divisor of two integers a, b is denoted $\gcd(a, b)$. For example, $\gcd(4, 12) = 4$.

Definition 0.3.2. The least common multiple of two integers a, b is denoted $\operatorname{lcm}[a, b]$. For example $\operatorname{lcm}[4, 15] = 60$

Definition 0.3.3. We define

$$a \equiv b \pmod{c} \iff c \mid a - b$$

For example $13 \equiv 1 \pmod{4}$ since $4 \mid 12$.

Definition 0.3.4. A number is said to be prime if the only divisors of the number are 1 and itself. For example, 5 is prime since $1 \mid 5, 2 \nmid 5, 3 \nmid 5, 4 \nmid 5, 5 \mid 5$. On the other hand, 6 is not prime as $1, 2, 3, 6 \mid 6$. A number is said to be composite if n can be expressed in the form ab for a, b being positive integers greater than 1. 1 is said to be neither prime nor composite.

Definition 0.3.5. $\longrightarrow\!\longleftarrow$ means "contradiction"

Definition 0.3.6. The degree of a polynomial is defined as the highest exponent in its expansion. For example, $\deg(x^3 - 2x^2 + 1) = 3$ and $\deg(-x^2 + x^4 - 1) = 4$.

1

Divisibility: The building blocks of number theory

In this chapter we explore the building blocks behind number theory: divisibility. We will explore algorithms and other vital theorems for number theory, along with a few problems they apply too. While this section is smaller in length then other sections, it is the building blocks and foundations of all number theory. These proofs can be repeated in similar vein for unique factorization domains, something we will not get into in this paper. I apologize in advance for the number of induction posts, however, when we are laying down the ground blocks and don't have many tools to use, we must use induction in many cases to prove theorems (or we can just "assume they're true" which I don't like to do).

1.1 Euclidean Algorithm

Before we get into the Euclidean Algorithm, we must first introduce the division algorithm which is vital for use in the Euclidean Algorithm.

Theorem 1.1.1. *The division algorithm states for every natural pair a, b with $a > b$, one can find exactly one distinct pair of quotient and remainder (q and r respectively) such that*

$$a = bq + r \quad 0 \leq r < b$$

Proof. We have to show every number can be represented under the division algorithm, and that each representation is distinct. Assume for sake of contradiction that we cannot for any b constant. Notice that $b = b \times 1$ and $b + 1 = b \times 1 + 1$ therefore we have shown the base cases. Assume that the division algorithm holds for all $a \leq x$ and does not for $a = x + 1$. Let the representations of $a = x$ be

$$x = bq_1 + r_1$$

Then, notice that

$$x + 1 = bq_1 + r_1 + 1$$

If $r_1 + 1 = b$, then we have $x + 1 = b(q_1 + 1)$, and if not then we have $r_1 + 1 < b$ and this is a contradiction.

The second part is to show uniqueness. Assume for the sake of contradiction that a can be represented in two ways:

$$\begin{aligned} a = bq_1 + r_1 &= bq_2 + r_2 \\ b(q_1 - q_2) &= r_2 - r_1 \end{aligned}$$

This implies that $b \mid r_2 - r_1$. However,

$$b > r_2 - r_1 > -b$$

since $0 \leq r_1, r_2 < b$, therefore we must have $r_2 - r_1 = 0$ implying $r_2 = r_1$ and $q_1 = q_2$. □

Example. $13 = 4 \times 3 + 1$, $14 = 7 \times 2$, etc.

Theorem 1.1.2. *For two natural a, b, $a > b$, to find $\gcd(a, b)$ we use the division algorithm repeatedly*

$$\begin{array}{rcl} a & = & bq_1 + r_1 \\ b & = & r_1q_2 + r_2 \\ r_1 & = & r_2q_3 + r_3 \\ \cdots & & \\ r_{n-2} & = & r_{n-1}q_n + r_n \\ r_{n-1} & = & r_nq_{n+1} \end{array}$$

Then we have $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = r_n$

Proof. We induct on $a+b$. Assume the Euclidean algorithm holds for all pairs of $a+b<k$ and we show it holds for $a+b=k$. First off, we must do a base case, which is when $a=2, b=1$. Trivially then, $2=1\times 2+0$, and so $\gcd(a,b)=r_0=b=1$ and the algorithm holds.

Now, if we can show that $\gcd(a,b)=\gcd(b,r_1)$ then by induction since $b+r_1<k$, we can use the Euclidean algorithm on b, r_1 and we will be done. Let $\gcd(a,b)=d$, and we have $d \mid b, r_1$ (since $r_1=a-bq_1$). Now, all that remains is to show that we cannot have $c \mid b, r_1$ with $c>d$. If $c \mid b, r_1$ then since $a=r_1+bq_1$ we will have $c \mid a$ and then $\gcd(a,b)\geq c>d$ contradiction. Therefore $\gcd(b,r_1)=d$ and we are done. □

Example 1.1.1. *Find* $\gcd(110,490)$.

Solution.

$$\begin{aligned} 490 &= 110\times 4+50 \\ 110 &= 50\times 2+\boxed{10} \\ 50 &= 10\times 5 \end{aligned}$$

If this method is long or tedious, another way you could do this question is as follows:

$$\begin{aligned} \gcd(110,490) &= \gcd(110, 490-4\times 110) \\ &= \gcd(110,50)=\gcd(110-50\times 2, 50) \\ &= \gcd(10,50)=10 \end{aligned}$$

A very common method used in Euclidean Algorithm problems is to reduce numbers using modulos:

$$\begin{gathered} 490\equiv 50 \pmod{110} \\ 110\equiv 10 \pmod{50} \\ 50\equiv 0 \pmod{10} \\ \gcd(490,110)=10 \end{gathered}$$

□

Euclidean Algorithm works for polynomials too. On this rare occasion, we omit the proof. Let $a(x)$ and $b(x)$ be two polynomials that we wish to find the greatest common divisor of. The division algorithm similarly works for polynomials: If $\deg(a(x)) \geq \deg(b(x))$ then there exists polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that

$$a(x) = b(x)q(x) + r(x), \deg(r) < \deg(q) \text{ or } r(x) = 0$$

Then the following algorithm calculuates $\gcd(a(x), b(x))$:

$$\begin{aligned}
a(x) &= b(x)q_1(x) + r_1(x) \\
b(x) &= r_1(x)q_2(x) + r_2(x) \\
r_1(x) &= r_2(x)q_3(x) + r_3(x) \\
&\cdots \\
r_{n-1}(x) &= r_n(x)q_{n+1}(x) + r_{n+1}(x) \\
r_n(x) &= r_{n+1}(x)q_{n+2}(x)
\end{aligned}$$

Then $\gcd(a(x), b(x)) = r_{n+1}(x)$. The greatest common divisor of two polynomials is chosen to be **monic**, meaning the leading coefficient is 1. Notice that polynomials during this process may have fractional coefficients. The method of modulo reduction works in polynomials as well, as we will see later in this section.

The following problem serves as an example as to why sometimes $q(x), r(x) \in \mathbb{Q}[x]$, as this may be unclear to some readers

Example 1.1.2. *Find the greatest common divisor of $x^2 - 4x + 1$ and $5x$.*

Solution. We proceed with the division algorithm:

$$\begin{aligned}
x^2 - 4x + 1 &= 5x(\frac{x}{5} - \frac{4}{5}) + 5 \\
5x &= 5 \times x
\end{aligned}$$

At this point we may be tempted to say that $\gcd(x^2 - 4x + 1, 5x) = 5$. However, we have to keep in mind that the greatest common divisor of polynomials is monic, therefore $\gcd(x^2 - 4x + 1, 5x) = 1$.

□

Comment. As a quick check, notice that the roots of $x^2 - 4x + 1$ are $x = 2 \pm \sqrt{3}$ and the roots of $5x$ are $x = 0$, therefore the two polynomials share no common roots. □

Example 1.1.3 (AIME 1985)**.** *The numbers in the sequence 101, 104, 109, 116, … are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.*

Solution. To do this, we notice that:

$$\begin{aligned} \gcd(100+n^2, 100+(n+1)^2) &= \gcd(100+n^2, 100+(n+1)^2-100-n^2) \\ = \gcd(100+n^2, 2n+1) &= \gcd(200+2n^2, 2n+1) \\ = \gcd(200+2n^2-n(2n+1), 2n+1) &= \gcd(200-n, 2n+1) \\ = \gcd(400-2n, 2n+1) &= \gcd(401, 2n+1) \end{aligned}$$

The answer is hence $\boxed{401}$ obtained when $n = 200$. □

Example 1.1.4 (IMO 1959)**.** *Prove that for natural n the fraction $\frac{21n+4}{14n+3}$ is irreducible.*

Solution.

$$\begin{aligned} \gcd(21n+4, 14n+3) &= \gcd(7n+1, 14n+3) \\ &= \gcd(7n+1, 14n+3-2(7n+1)) = \gcd(7n+1, 1) = 1 \end{aligned}$$

□

Example 1.1.5. *Let n be a positive integer. Calculate*

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

Solution.

$$\begin{aligned} \gcd(n!+1, (n+1)!) &= \gcd(n!+1, (n+1)!-(n+1)(n!+1)) \\ &= \gcd(n!+1, -(n+1)) \\ &= \gcd(n!+1, n+1) \end{aligned}$$

Let p be a prime divisor of $n+1$. Unless $n+1$ is prime, we have

$$p \le n \implies n!+1 \equiv 1 \pmod{p}$$

It turns out that when $n+1$ is prime, we have $n!+1 \equiv 0 \pmod{n+1}$, which we will prove in the Wilson's theorem section. Therefore, the answer is

$$\gcd(n!+1,(n+1)!) = \begin{cases} 1 & \text{if } n+1 \text{ is composite} \\ n+1 & \text{if } n+1 \text{ is prime} \end{cases}$$

□

Example 1.1.6 (AIME 1986)**.** *What is the largest positive integer n such that n^3+100 is divisible by $n+10$?*

Solution. Let

$$\begin{aligned} n^3+100 &= \left(n^2+an+b\right)(n+10)+c \\ &= n^3+n^2(10+a)+n(b+10a)+10b+c \end{aligned}$$

Equating coefficients yields

$$\begin{cases} 10+a=0 \\ b+10a=0, 10b+c=100 \end{cases}$$

Solving this system yields $a=-10, b=100$, and $c=-900$. Therefore, by the Euclidean Algorithm, we get

$$n+10 = \gcd(n^3+100, n+10) = \gcd(-900, n+10) = \gcd(900, n+10)$$

The maximum value for n is hence $n = \boxed{890}$. □

Example 1.1.7 (Iran 2005)**.** *Let $n, p > 1$ be positive integers and p be prime. We know that $n \mid p-1$ and $p \mid n^3-1$. Prove that $4p-3$ is a perfect square.*

Solution. Let $p = kn+1$. Now, notice that $n \mid p-1$ implies that $p \geq n+1$. Therefore $\gcd(p, n-1) = 1$ (since p is a prime). Therefore

$$p = kn+1 \mid n^2+n+1 \mid kn^2+kn+k$$

Now,

$$\begin{aligned} \gcd(kn+1, kn^2+kn+k) &= \gcd(kn+1, kn^2+kn+k-n(kn+1)) \\ &= \gcd(kn+1, kn+k-n) \end{aligned}$$

Therefore either $kn+k-n=0$ or $k-n \geq 1$. Obviously, the first condition is impossible, therefore $k-n \geq 1$. Also, $kn+1 \leq n^2+n+1$ so $k \leq n+1$ implying $k=n+1$. Therefore $p=n^2+n+1$ giving

$$4p-3 = 4n^2+4n+4-3 = (2n+1)^2.$$

□

Theorem 1.1.3. *For natural a, m, n, $\gcd(a^m-1, a^n-1) = a^{\gcd(m,n)}-1$*

Proof. We again induct on $m+n$ for any a. WLOG assume $m > n$. Now, for $(m,n)=(2,1)$ we have

$$\gcd(a^2-1, a-1) = a-1 = a^{\gcd(1,2)}-1$$

Next, we use strong induction and assume the problem statement holds for $m+n<k$ and we show that it holds for $m+n=k$. Notice that

$$\begin{aligned} \gcd(a^m-1, a^n-1) &= \gcd(a^m-1-a^{m-n}(a^n-1), a^n-1) \\ &= \gcd(a^{m-n}-1, a^n-1) \end{aligned}$$

Now, by the induction hypothesis and the Euclidean Algorithm

$$\gcd(a^{m-n}-1, a^n-1) = a^{\gcd(m-n,n)}-1 = a^{\gcd(m,n)}-1$$

We are therefore done by strong induction. □

Example 1.1.8 (PUMAC 2013)**.** *The greatest common divisor of* $2^{30^{10}}-2$ *and* $2^{30^{45}}-2$ *can be expressed in the form* 2^x-2*. Calculuate* x*.*

Using the above theorem,

$$\begin{aligned} \gcd(2^{30^{10}}-2, 2^{30^{45}}-2) &= 2\left[2^{\gcd(30^{10}-1, 30^{45}-1)}-1\right] \\ &= 2\left[2^{30^{\gcd(10,45)-1}}-1\right] \\ &= 2\left(2^{30^5-1}-1\right) = 2^{30^5}-2 \end{aligned}$$

Therefore, $x = 30^5$.

Comment. The actual problem asked for the remainder when the greatest common divisor was divided by 2013. This, however, involves Euler's Totient Theorem, something we will get to later in the text. □

Example 1.1.9. *Prove that for positive integers $a, b > 2$ we cannot have $2^b - 1 \mid 2^a + 1$.*

Solution. Assume for the sake of contradiction that $2^b - 1 \mid 2^a + 1$. We obviously have $a > b$, so write $a = bq + r$ using the division algorithm. We must have $\gcd(2^b - 1, 2^a + 1) = 2^b - 1$. We then have

$$\begin{aligned}\gcd(2^b - 1, 2^a + 1) &= \gcd(2^b - 1, 2^a + 1 + 2^b - 1) \\ &= \gcd(2^b - 1, 2^b\left(2^{a-b} + 1\right) = \gcd(2^b - 1, 2^{a-b} + 1)\end{aligned}$$

Repeating this process, we arrive at

$$\gcd(2^b - 1, 2^a + 1) = \gcd(2^b - 1, 2^{a-qb} + 1) = \gcd(2^b - 1, 2^r + 1)$$

Since $r < b$, we have $2^r + 1 \le 2^{b-1} + 1 < 2^b - 1$ for $a, b > 2$. □

Example 1.1.10. *Prove that if $m \neq n$, then*

$$\gcd(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 \textit{ if a is even} \\ 2 \textit{ if a is odd} \end{cases}$$

Proof. First off, WLOG let $m > n$. Then we have

$$a^{2^n} + 1 \mid a^{2^{n+1}} - 1 \mid a^{2^m} - 1$$

The last step follows from the fact that $2^{n+1} \mid 2^m$.

Let $a^{2^m} - 1 = q(a^{2^n} + 1)$. Therefore,

$$\left(a^{2^m} - 1\right) = q(a^{2^n} + 1) - 2$$

By the Euclidean Algorithm,

$$\gcd(a^{2^m} - 1, a^{2^n} + 1) = \gcd(a^{2^n} + 1, -2) = \begin{cases} 1 \text{ if a is even} \\ 2 \text{ if a is odd} \end{cases}$$

□

Example 1.1.11. *If p is an odd prime, and a, b are relatively prime positive integers, prove that*

$$\gcd\left(a+b, \frac{a^p+b^p}{a+b}\right) = 1 \text{ or } p$$

Solution. The following portion of the text will look at experimentation. In other words, how do we come across a solution?

We originally look at this problem and have no idea how to even begin. It looks like an Euclidean Algorithm problem. We use a problem solving strategy of reducing the problem. We set $b = 1$ and our goal is to now show that

$$\gcd(a+1, \frac{a^p+1}{a+1}) = 1 \text{or } p$$

We notice that

$$\frac{a^p+1}{a+1} = a^{p-1} - a^{p-2} + a^{p-3} - a^{p-4} + \cdots - a + 1$$

We try out some small cases. $a = 2$ gives us $\gcd(3, 2^{p-1} - 2^{p-2} + \cdots - 2 + 1)$. Now, notice that

$$\begin{cases} x \equiv 0 \pmod 2 & 2^x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 2 & 2^x \equiv -1 \pmod 3 \end{cases}$$

Now, in the above sum, every term with even exponent is positive and every term with negative exponent is negative (since $p-1$ is even). Therefore, each term of the sum is 1 mod 3, or henceforth the whole sum is p mod 3. Therefore, using the Euclidean Algorithm, we arrive at

$$\gcd(3, 2^{p-1} - 2^{p-2} + \cdots - 2 + 1) = \gcd(3, p)$$

When $p = 3$ this is 3, else this is 1.

We try this method again for $a = 3$ We arrive at $\gcd(4, 3^{p-1} - 3^{p-2} + \cdots - 3 + 1)$. Again, notice that

$$\begin{cases} x \equiv 0 \pmod 2 & 3^x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 2 & 3^x \equiv -1 \pmod 4 \end{cases}$$

Again, every number with an even exponent is positive and every term with a negative exponent is negative, therefore

$$3^{p-1} - 3^{p-2} + \cdots - 3 + 1 \equiv 1 + 1 + 1 + \cdots + 1 \equiv p \pmod 4$$

Now, using the Euclidean Algorithm, we have

$$\gcd(4, 3^{p-1} - 3^{p-2} + \cdots - 3 + 1) = \gcd(4, p) = 1$$

Using the fact that p is an odd prime.

OBSERVATIONS:

- It appears as if we always have $\frac{a^p+1}{a+1} \equiv p \pmod{a+1}$.

We set about proving this. Notice that:

$$\begin{aligned}
\frac{a^p+1}{a+1} &= a^{p-1} - a^{p-2} + \cdots + a^{2x} - a^{2x-1} + \cdots - a + 1 \\
&\equiv (-1)^{p-1} - (-1)^{p-2} + \cdots + (-1)^{2x} - (-1)^{2x-1} - a + 1 \pmod{a+1} \\
&\equiv \underbrace{1 + 1 + \cdots + 1}_{\text{p terms}} \equiv p \pmod{a+1}
\end{aligned}$$

Now, by the Euclidan Algorithm, we have

$$\gcd(a+1, \frac{a^p+1}{a+1}) = \gcd(a+1, p) = 1 \text{ or } p$$

We have now solved the problem for $b = 1$. We wish to generalize the method to any b.

Notice that

$$\frac{a^p+b^p}{a+b} = a^{p-1} - a^{p-2}b + a^{p-3}b^2 - a^{p-4}b^3 + \cdots - ab^{p-2} + b^{p-1}$$

Next, notice that

$$\begin{aligned}
a^{p-1} - a^{p-2}b + a^{p-3}b^2 - a^{p-4}b^3 + \cdots - ab^{p-2} + b^{p-1} &\equiv (-b)^{p-1} - (-b)^{p-2}\,b + \cdots \\
&\equiv pb^{p-1} \pmod{a+b}.
\end{aligned}$$

Therefore, by the Euclidean Algorithm we arrive at

$$\gcd\left(\frac{a^p+b^p}{a+b}, a+b\right) = \gcd(pb^{p-1}, a+b) = \gcd(p, a+b) = 1 \text{ or } p$$

The last fact follows from the fact that $\gcd(b, a+b) = 1$. □

Wow, that was a really nice problem!

- We first off test out $b = 1$ to see if we can solve the problem for a smaller case.

- We test some small values of a and get the idea to use the modulo idea in the Euclidean Algorithm.
- We extend the solution to general b.

Solution. (Rigorous) Notice that

$$\frac{a^p+b^p}{a+b} = \sum_{i=0}^{p-1} (-1)^i \, a^{p-1-i} b^i \equiv pb^{p-1} \pmod{a+b}$$

Now, by the Euclidean Algorithm we arrive at

$$\gcd\left(\frac{a^p+b^p}{a+b}, a+b\right) = \gcd(pb^{p-1}, a+b) = \gcd(p, a+b) = 1 \text{ or } p$$

Since $\gcd(b, a+b) = 1$. □

1.1.1 Excercises

Problem 1.1.1. Calculate $\gcd(301, 603)$.

Problem 1.1.2. Calculate $\gcd(133, 189)$.

Problem 1.1.3. Calculate $\gcd(486, 1674)$. [Recommended Calculator Use]

Problem 1.1.4. Prove that the sum and product of two positive relatively prime integers are themselves relatively prime.

Problem 1.1.5. For positive integers $a, b, n > 1$, prove that

$$a^n - b^n \nmid a^n + b^n$$

Problem 1.1.6. Use the Euclidean Algorithm for polynomials to calculate $\gcd(x^4 - x^3, x^3 - x)$.

Problem 1.1.7. Let $n \geq 2$ and k be positive integers. Prove that $(n-1)^2 \mid (n^k - 1)$ if and only if $(n-1) \mid k$. [1]

Problem 1.1.8 (HMMT)**.** Compute $\gcd(2002+2, 2002^2+2, 2002^3+2, \cdots)$.

Problem 1.1.9. Prove that any two consecutive terms in the Fibonacci sequence are relatively prime.

[1] *Hint:* This has nothing to do with the Euclidean Algorithm, use the main idea used in the final problem of this section

Problem 1.1.10 (Japan 1996)**.** Let m, n be relatively prime odd integers. Calculuate $\gcd(5^m + 7^m, 5^n + 7^n)$.

Problem 1.1.11. Let the integers a_n and b_n be defined by the relationship

$$a_n + b_n\sqrt{2} = \left(1 + \sqrt{2}\right)^n$$

for all integers $n \geq 1$. Prove that $\gcd(a_n, b_n) = 1$ for all integers $n \geq 1$.

Problem 1.1.12 (Poland 2004)**.** Find all natural $n > 1$ for which value of the sum $2^2 + 3^2 + \cdots + n^2$ equals p^k where p is prime and k is natural.

1.2 Bezout's Theorem

Theorem 1.2.1. *For a, b natural, there exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$*

Proof. (Outline) Run Euclid's algorithm backwards:

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})\, q_n \\ &= r_{n-2}(1 + q_nq_{n-1}) - (r_{n-3}) \\ &= \cdots \\ &= r_1c_1 + bc_2 \\ &= c_1(a - bq_1) + bc_2 \\ &= a(c_1) + b(c_2 - q_1c_1) \end{aligned}$$

In conclusion, the two variables in the equation run through:

$$(r_{n-2}, r_{n-1}) \to (r_{n-2}, r_{n-3}) \to (r_{n-4}, r_{n-3} \cdots \to (b, r_1) \to (a, b)$$

The following fully rigorous proof can be read lightly, and is only included for completion. □

Proof. (Rigorous) We again induct on $a + b$ assuming WLOG that $a > b$. First off, for $(a, b) = (2, 1)$ we clearly have $2 \times 1 - 1 = 1$. Next, we assume that we can express $\gcd(a_1, b_1)$ in terms of a_1 and b_1 for all $a_1 + b_1 < k$. We show that for $a_1 + b_1 = k$, we can as well express $\gcd(a_1, b_1)$ in terms of a_1 and b_1.

Notice that via induction hypothesis, we can express $\gcd(b_1, r_1) = \gcd(a_1, b_1)$ in terms of b_1, r_1. Let

$$\gcd(b_1, r_1) = b_1c_1 + r_1c_2$$

Now, $r_1 = a_1 - b_1q_1$ using the Euclid Algorithm, therefore we have

$$\gcd(b_1, r_1) = \gcd(a_1, b_1) = \gcd(ab_1c_1 + c_2(a_1 - b_1q_1) = b_1(c_1 - c_2q_1) + a_1(c_2)$$

We are now done by induction. □

After reading that proof, I fear things may be dull. To lighten the mood, many functions go to a party. Functions such as $\sin(x), x^2, \ln(x)$ and others are having a great time. Unfortunately, e^x is sitting alone on a couch. Midway through the party, $\cos(x)$ walks up to him and says "hey man, how about you integrate your self into the party". Sighing, e^x responds, "why bother, it won't make a difference." Anyways, back to math.

Example 1.2.1. *Express* 5 *in terms of* 45 *and* 65*.*

Solution. We use the Euclidean Algorithm in reverse. Using the Euclidean Algorithm on 45 and 65, we arrive at

$$\begin{aligned} 65 &= 45 \times 1 + 20 \\ 45 &= 20 \times 2 + 5 \\ 20 &= 5 \times 4 \end{aligned}$$

Therefore, we run the process in reverse to arrive at

$$\begin{aligned} 5 &= 45 - 20 \times 2 \\ &= 45 - (65 - 45 \times 1)2 \\ &= 45 \times 3 - 65 \times 2 \end{aligned}$$

□

Example 1.2.2. *Express* 10 *in terms of* 110 *and* 380

Solution. We again, use the Euclidean Algorithm to arrive at

$$\begin{aligned} 380 &= 110 \times 3 + 50 \\ 110 &= 50 \times 2 + 10 \\ 50 &= 10 \times 5 \end{aligned}$$

Now, running the Euclidean Algorithm in reverse gives us

$$\begin{aligned} 10 &= 110 - 50 \times 2 \\ &= 110 - (380 - 110 \times 3) \times 2 \\ &= 7 \times 110 - 2 \times 380 \end{aligned}$$

□

The above two examples the reader could likely do using their head/just guess and check. Here is a clear example where this approach won't work.

Example 1.2.3. *Express* 3 *in terms of* 1011 *and* $11,202$.

Solution. We use the Euclidean Algorithm to arrive at

$$\begin{aligned} 11202 &= 1011 \times 11 + 81 \\ 1011 &= 81 \times 12 + 39 \\ 81 &= 39 \times 2 + 3 \\ 39 &= 3 \times 13 \end{aligned}$$

Now, runing the Euclidean Algorithm in reverse, we arrive at:

$$\begin{aligned} 3 &= 81 - 39 \times 2 \\ &= 81 - (1011 - 81 \times 12) \times 2 = 81 \times 25 - 1011 \times 2 \\ &= (11202 - 1011 \times 11) \times 25 - 1011 \times 2 = 11202 \times 25 - 1011 \times 277 \end{aligned}$$

□

Theorem 1.2.2 (Classic)**.** *If* $a \mid bc$ *and* $\gcd(a, b) = 1$, *prove* $a \mid c$.

Proof. While this theorem seems intuitively obvious, I will provide the rigorous proof. By Bezout's lemma, $\gcd(a, b) = 1$ implies that there exist x, y such that $ax + by = 1$. Next, multiply this equation by c to arrive at

$$c(ax) + c(by) = c$$

Furthermore, since $a \mid ac, a \mid bc$ we have

$$a \mid c(ax) + c(by) = c$$

□

Comment. Clever proof, huh? This theorem is actually incredibly important as we will see when we get to the fundamental theorem of arithmetic. □

Here is a problem that require more advanced applications of Bezout's Lemma.

Example 1.2.4. *(Putnam 2001) Prove that the expression*

$$\frac{\gcd(m, n)}{n}\binom{m}{n}$$

is an integer for all pairs of integers $n > m \geq 1$.

Solution. By Bezout's Lemma, there exist integers a and b such $\gcd(m, n) = am + bn$. Next, notice that

$$\frac{\gcd(m, n)}{n}\binom{m}{n} = \frac{am + bn}{n}\binom{m}{n} = \frac{am}{n}\binom{m}{n} + b\binom{m}{n}.$$

We therefore must prove that $\frac{am}{n}\binom{m}{n}$ is an integer. From a well known binomial identity,

$$a\frac{m}{n}\binom{m}{n} = a\binom{m-1}{n-1}.$$

As a result

$$\frac{\gcd(m, n)}{n}\binom{m}{n} = a\binom{m-1}{n-1} + b\binom{m}{n}$$

Which is clearly an integer. □

Bezout's Theorem for polynomials works the same exact way as it does for integers. Assume $f(x), g(x) \in \mathbb{Z}[x]$, then using Euclid's Algorithm, we can find $u(x), v(x) \in \mathbb{Q}[x]$ such that

$$f(x)u(x) + g(x)v(x) = \gcd(f(x), g(x))$$

Here is an example for clarity.

Example 1.2.5. *Find polynomials $u, v \in \mathbb{Z}[x]$ such that*

$$(x^4 - 1)u(x) + (x^7 - 1)v(x) = (x - 1).$$

Solution. First off, we use Euclid's Algorithm on $x^4 - 1, x^7 - 1$. Notice that

$$\begin{aligned} x^7 - 1 &= (x^4 - 1)x^3 + x^3 - 1 \\ x^4 - 1 &= x(x^3 - 1) + x - 1 \\ x^3 - 1 &= (x - 1)(x^2 + x + 1) \end{aligned}$$

Therefore,

$$\begin{aligned} x - 1 &= x^4 - 1 - x(x^3 - 1) \\ &= x^4 - 1 - x\left[x^7 - 1 - \left(x^4 - 1\right)x^3\right] \\ &= \left(x^4 - 1\right) + x^4\left(x^4 - 1\right) - x\left(x^7 - 1\right) \\ &= \left(x^4 - 1\right)\left(x^4 + 1\right) - x\left(x^7 - 1\right) \end{aligned}$$

Therefore $u(x) = x^4 + 1, v(x) = -x$. □

The reason that $u(x), v(x) \in \mathbb{Q}[x]$ is explained in this problem.

Example 1.2.6. *Do there exist polynomials $u, v \in \mathbb{Z}[x]$ such that*

$$(5x^2 - 1)u(x) + (x^3 - 1)v(x) = 1?$$

Solution. We claim no such polynomials exist. Assume for the sake of contradiction that there exists $u, v \in \mathbb{Z}[x]$ such that $(5x^2-1)u(x)+(x^3-1)v(x) = 1$. Set $x = 1$ to give

$$4u(1) + 0v(1) = 1 \implies u(1) = \frac{1}{4}$$

, contradicting the assumption that $u \in \mathbb{Z}[x]$. □

Example 1.2.7. *Find polynomials $u, v \in \mathbb{Q}[x]$ such that*

$$(5x^2-1)u(x)+(x^3-1)v(x)=1.$$

Solution. We proceed with the Euclidean Algorithm

$$\begin{aligned}
x^3-1 &= (5x^2-1)\left(\frac{1}{5}x\right)+\frac{x}{5}-1\\
(5x^2-1) &= \left(\frac{x}{5}-1\right)(25x+125)+124\\
1 &= \frac{5x^2-1}{124}-\left(\frac{x}{5}-1\right)\left(\frac{25}{124}x+\frac{125}{124}\right)\\
1 &= \frac{5x^2-1}{124}-\left[x^3-1-\frac{1}{5}x\left(5x^2-1\right)\right]\left(\frac{25}{124}x+\frac{125}{124}\right)\\
1 &= \left(5x^2-1\right)\left[\frac{1}{124}+\frac{1}{5}x\left(\frac{25}{124}x+\frac{125}{124}\right)\right]-\left(x^3-1\right)\left(\frac{25}{124}x+\frac{125}{124}\right)\\
1 &= \left(5x^2-1\right)\left(\frac{5}{124}x^2+\frac{25}{124}x+\frac{1}{124}\right)-\left(x^3-1\right)\left(\frac{25}{124}x+\frac{125}{124}\right)
\end{aligned}$$

Therefore,

$$u(x)=\frac{5}{124}x^2+\frac{25}{124}x+\frac{1}{124} \quad \text{and} \quad v(x)=\frac{-25x}{124}-\frac{125}{124}.$$

□

1.2.1 Problems

Problem 1.2.1. Find integers x, y such that $5x+97y=1$.

Problem 1.2.2. Find integers x, y such that $1011x+1110y=3$.

Problem 1.2.3. Prove that there are no integers x, y such that $1691x+1349y=1$.

Problem 1.2.4. Find **all** integers x, y such that $5x+13y=1$. [2]

[2] *Hint:* If $(x,y)=(a_0,b_0)$ is a solution pair, then so is $(x,y)=(a_0+13k,b_0-5k)$.

Problem 1.2.5 (General Bezout's Theorem)**.** Prove that for integers $a_1, a_2, \cdots, a_n$, there exists integers $x_1, x_2, \cdots, x_n$ such that

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = \sum_{i=1}^{n} a_ix_i = \gcd(a_1, a_2, \cdots, a_n)$$

Problem 1.2.6. Find $u, v \in \mathbb{Z}[x]$ such that $(x^5 - 1)u(x) + (x^8 - 1)v(x) = (x - 1)$.

Problem 1.2.7. For relatively prime naturals m, n, do there exist polynomials $u, v \in \mathbb{Q}[x]$ such that $(x^m - 1)u(x) + (x^n - 1)v(x) = (x - 1)$? [3]

Problem 1.2.8. Without using Euclid's Algorithm, prove that $\gcd(21n + 4, 14n + 3) = 1$.

Problem 1.2.9. Find $u, v \in \mathbb{Q}[x]$ such that $(2x^2-1)u(x)+(3x^3-1)v(x) = 1$

1.3 Fundamental Theorem of Arithmetic

Next, we use Bezout's Theorem to prove the Fundamental Theorem of Arithmetic, which, as the name suggests, is incredibly fundamental to mathematics.

Theorem 1.3.1. *(Fundamental Theorem of Arithmetic) Every natural number n has a distinct prime factorization.*

Now, before we go on to the proof, we must consider exactly what this theorem states. The theorem says that every number n can be decomposed into a product of primes. For example, $15 = 3 \times 5$. The problem statement also states that every number has a distinct prime factorization, for example, it must show that we canot have $3 \times 7 = 5 \times 5$ (even though I know this sounds silly). Now, we can tackle the proof.

Proof. We induct on n. For $n = 1, 2, 3$ the statement obviously holds. Now, assume that the problem statement does for all $n < k$ and we show the statement holds for $n = k$. We have two cases:

- k is prime in which case we are done.

[3] *Hint:* Use $\gcd(x^m - 1, x^n - 1) = x^{\gcd(m,n)} - 1$

- k is composite. Now, let p be a prime divisor of k less than k. Now, we can write
$$k = p \cdot \frac{k}{p}.$$
We know that $\frac{k}{p}$ can be composed into primes by the inductive hypothesis ($\frac{k}{p} < k$), therefore we are done.

The second part of the problem is to prove uniqueness. Again, we use induction. Assume the problem statement holds for up to $n < k$ and we show it holds for $n = k$. The base cases ($n = 1, 2, 3$) are obvious and left to the reader. For the sake of contradiction, assume k has two distinct prime factorizations, let them be:

$$\begin{array}{rcl} n = p_1^{e_1} p_2^{e_2} \cdots p_i^{e_i} & = & q_1^{f_1} q_2^{f_2} \cdots q_j^{f_j} \\ p_1 < p_2 < \cdots < p_i & , & q_1 < q_2 < \cdots < q_j \end{array}$$

WLOG let $p_1 \le q_1$. Now,

$$p_1 \mid \left(q_1^{f_1}\right)\left(q_2^{f_2} \cdots q_j^{f_j}\right)$$

We have
$$\gcd(p_1, q_2^{f_2} \cdots q_j^{f_j}) = 1$$
since $p_1 < q_2 < \cdots < q_j$. Now, by the classical theorem above,

$$p_1 \mid q_1^{f_1} \implies p_1 = q_1$$

Next, divide by p_1 on both sides, and we arrive at

$$\frac{n}{p_1} = p_1^{e_1 - 1} p_2^{e_2} \cdots p_i^{e_i} = q_1^{f_1 - 1} q_2^{f_2} \cdots q_j^{f_j}$$

However, by inductive hypothesis, $\frac{n}{p_1}$ has one distinct prime factorization, henceforth we are done. □

So, what exactly does this theorem say? This theorem says that for every integer n, we can express it in terms of a product of primes. For example, $500 = 2^2 \times 5^3$. While this may seem trivial, this is a key building block for the rest of number theory.

Writing numbers in terms of their prime factorization doesn't have any exact applications, but can lead to some interesting theorems.

Theorem 1.3.2. *Let*

$$a = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}, b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

Where the exponents can be zero and the p_i's are distinct. Prove that

$$\begin{aligned} \gcd(a, b) &= p_1^{min(e_1, f_1)} p_2^{min(e_2, f_2)} \cdots p_k^{min(e_k, f_k)} \\ \textit{and } \operatorname{lcm}[a, b] &= p_1^{max(e_1, f_1)} p_2^{max(e_2, f_2)} \cdots p_k^{max(e_k, f_k)} \end{aligned}$$

Proof. Set $d = \gcd(a, b)$. Then,

$$d \mid a \implies d = p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}$$

Notice that we must have $g_i \le e_i, f_i$, therefore the maximum possible value of g_i is $\min(e_i, f_i)$.

Similarly, set $c = \operatorname{lcm}[a, b]$. Since $a, b \mid \operatorname{lcm}[a, b]$, and we want the **least** common multiple, we have

$$\operatorname{lcm}[a, b] = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$$

We must have $h_i \ge e_i, f_i$, therefore the minimum possible value of h_i is $\max(e_i, f_i)$. □

Corollary 1.3.1. For $a, b \in \mathbb{Z}^+$, $\gcd(a, b) \operatorname{lcm}[a, b] = ab$

Proof. $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$. □

Example 1.3.1. *(AIME 1987) Let [r,s] denote the least common multiple of positive integers r and s. Find the number of ordered triples a, b, c such that $[a, b] = 1,000, [b, c] = 2,000, [c, a] = 2,000$.*

Solution. We look at the prime factorization of the numbers. Notice that $1000 = 2^3 \times 5^3, 2000 = 2^4 \times 5^3$. We set

$$a = 2^{a_1} 5^{a_2}, b = 2^{b_1} 5^{b_2}, c = 2^{c_1} 5^{c_2}$$

Notice that if a_1 or b_1 was at least 4, then we would have at least 4 factors of 2 in $[a, b]$. Also, because $[b, c]$ and $[c, a]$ both have 4 factors of 2, we must have $c_1 = 4$.

Case 1: $c_2 = 3$

In this case, we must now have at least one of a_2, b_2 be 3 in order to have $a, b] = 1,000$. Therefore, we have the pairs

$$(a_1, b_1) = (0, 3), (1, 3), (2, 3), (3, 3), (3, 2), (3, 1), (3, 0)$$

For 7 pairs. Similarly, we must have at least one of a_1, b_1 be 3 in order to have $[a, b] = 1,000$. We have the same pairs as before for 7 pairs, or a total of $7 \times 7 = 49$ for this case.

Case 2: $c_2 < 3$

In this case, we have $c_2 \in \{0, 1, 2\}$ for three choices. Now, since $[b, c] = 2,000$ and $[c, a] = 2,000$, we must have $a_2 = b_2 = 3$. Next, we must have at least one of a_1, a_2 be 3 in order to have $[a, b] = 1,000$ for another 7 pairs. Therefore there are $7 \times 3 = 21$ for this case.

The answer is hence $49 + 21 = \boxed{70}$ □

Example 1.3.2 (Canada 1970). *Given the polynomial*

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

with integer coefficients $a_1, a_2, \ldots, a_n$, and given also that there exist four distinct integers a, b, c and d such that

$$f(a) = f(b) = f(c) = f(d) = 5,$$

show that there is no integer k such that $f(k) = 8$.

Solution. Set $g(x) = f(x) - 5$. Therefore, we must have

$$g(x) = c\,(x - a)\,(x - b)\,(x - c)\,(x - d)\,h(x)$$

for some $h(x) \in \mathbb{Z}[x]$. Let k be such that $f(k) = 8$. Therefore, $g(k) = 3$, and we get

$$3 = c\,(k - a)\,(k - b)\,(k - c)\,(k - d)\,h(x)$$

By the Fundamental Theorem of Arithmetic, we can only express 3 as the product of at most three integers $(-3, 1, -1)$. Since $x - a, x - b, x - c, x - d$ are all distinct integers, this is an obvious contradiction. □

Example 1.3.3 (USAMO 1973)**.** *Show that the cube roots of three distinct prime numbers cannot be three terms (not necessarily consecutive) of an arithmetic progression.*

Solution. Let the primes in the sequence be $\sqrt[3]{p_1}$, $\sqrt[3]{p_2}$, $\sqrt[3]{p_3}$. By definition of an arithmetic sequence, set

$$\sqrt[3]{p_1} = a, \sqrt[3]{p_2} = a + kd, \sqrt[3]{p_3} = a + md, m > k$$

This implies that:

$$\begin{gathered} \sqrt[3]{p_2} - \sqrt[3]{p_1} = kd \ , \ \sqrt[3]{p_3} - \sqrt[3]{p_1} = md \\ \implies m\sqrt[3]{p_2} - m\sqrt[3]{p_1} = k\sqrt[3]{p_3} - k\sqrt[3]{p_1} = mkd \end{gathered}$$

Using this equation and some rearrangement, we get:

$$\begin{aligned} m\sqrt[3]{p_2} - k\sqrt[3]{p_3} &= (m-k)\sqrt[3]{p_1} \\ m^3p_2 - 3m^2p_2^{\frac{2}{3}}kp_3^{\frac{1}{3}} + 3mp_2^{\frac{1}{3}}k^2p_3^{\frac{2}{3}} - k^3p_3 &= (m-k)^3 p_1 \\ 3mkp_2^{\frac{1}{3}}p_3^{\frac{1}{3}}\left(kp_3^{\frac{1}{3}} - mp_2^{\frac{1}{3}}\right) &= (m-k)^3 p_1 - m^3p_2 + k^3p_3 \\ 3mkp_2^{\frac{1}{3}}p_3^{\frac{1}{3}}(k-m)\,p_1^{\frac{1}{3}} &= (m-k)^3 p_1 - m^3p_2 + k^3p_3 \\ \sqrt[3]{p_1p_2p_3} &= \frac{m^3p_2 - (m-k)^3 p_1 - k^3p_3}{3mk(m-k)} \end{aligned}$$

Lemma. If $\sqrt[3]{a}$ is rational, then $\sqrt[3]{a}$ is an integer.

Proof. Set

$$\sqrt[3]{a} = \frac{x}{y} \implies ay^3 = x^3, \gcd(x,y) = 1$$

If $p \mid y$, then using $\gcd(x,y) = 1$ we get $p \nmid x$, contradicting the Fundamental Theorem of Arithmetic. Therefore, $y = 1$. □

Therefore, $\sqrt[3]{p_1p_2p_3}$ must be an integer, implying $p_1 = p_2 = p_3$ from the Fundamental Theorem of Arithmetic, contradiction.

□

1.3.1 Problems for the reader

Problem 1.3.1. The product of the greatest common factor and least common multiple of two numbers is 384. If one number is 8 more than the other number, compute the sum of two numbers.

Problem 1.3.2. Prove that $\sqrt{2}$ is irrational.

Problem 1.3.3. Prove that $\log_{10}(2)$ is irrational.

Problem 1.3.4. Prove that for $m, n \in \mathbb{Z}$,

$$m^5 + 3m^4n - 5m^3n^2 - 15m^2n^3 + 4mn^4 + 12n^5 \neq 33$$

1.4 Challenging Division Problems

Example 1.4.1 (St. Petersburg 1996)**.** *Find all positive integers n such that*

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

Solution. Notice that

$$3^{n-1} + 5^{n-1} \mid 5 \cdot \left(3^{n-1} + 5^{n-1}\right) = 5^n + 3^n + 2 \cdot 3^{n-1}$$

Therefore combining this with the given equation we get

$$3^{n-1} + 5^{n-1} \mid 2 \cdot 3^{n-1}$$

However, $3^{n-1} + 5^{n-1} > 2 \cdots 3^{n-1}$ for $n > 1$. We check that $n = 1$ is the only solution. □

Example 1.4.2 (APMO 2002)**.** *Find all pairs of positive integers a, b such that*

$$\frac{a^2 + b}{b^2 - a} \text{ and } \frac{b^2 + a}{a^2 - b}$$

are both integers.

Solution. For these conditions to be met, we must have

$$\begin{aligned} a^2+b &\geq b^2-a & b^2+a &\geq a^2-b \\ (a-b+1)(a+b) &\geq 0 & (b-a+1)(a+b) &\geq 0 \\ a &\geq b-1 & b &\geq a-1 \end{aligned}$$

Therefore, $a = b, b-1, b+1$. Notice that we can only account for $a = b-1$, and then reverse the solutions.

Case 1: $a = b$

We must then have $\frac{a^2+a}{a^2-a}$ is an integer. Notice that

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

This gives the solution pairs $(a, b) = (2, 2), (3, 3)$.

Case 2: $a = b-1$

We notice that in this case $a^2+b = b^2-a$, therefore we only ahve to consider:

$$\begin{aligned} \frac{b^2+a}{a^2-b} &= \frac{(a+1)^2+a}{a^2-a-1} = \frac{a^2+3a+1}{a^2-a-1} \\ &= 1 + \frac{4a+2}{a^2-a-1} \end{aligned}$$

Notice that for $a \geq 6$, however, then we ahve $a^2-a-1 \geq 4a+2$, contradiction. Therefore, we consider $a \in \{1, 2, 3, 4, 5\}$. Testing these, we see that only $a = 1, 2$ give solutions. We therefore get the solution pair $(a, b) = (1, 2), (2, 3)$ and permutations (for $a = b+1$).

In conclusion, all solutions are of the form $(a, b) = (1, 2), (2, 1), (2, 3), (3, 2), (2, 2), (3, 3)$.

□

Example 1.4.3. *(1998 IMO) Determine all pairs (x, y) of positive integers such that $x^2y + x + y$ is divisible by $xy^2 + y + 7$.*

Solution. The given condition is equivalent to

$$xy^2 + y + 7 \mid y\left(x^2y + x + y\right) - x\left(xy^2 + y + 7\right) = y^2 - 7x$$

If $y^2 - 7x > 0$ then we must have $y^2 - 7x \geq xy^2 + y + 7$ clearly absurd. Therefore $y^2 - 7x \leq 0$. If $y^2 - 7x = 0$ we arrive at the solution $(x, y) = (7m^2, 7m)$.

Now for d positive set

$$\begin{aligned} 7x - y^2 &= d(xy^2 + y + 7) \\ x(7 - dy^2) &= y^2 + dy + 7 \end{aligned}$$

We therefore must test $y = 1, 2$. If $y = 1$ we arrive at

$$\begin{aligned} x + 8 &\mid 1 - 7x \\ \frac{1 - 7x}{x + 8} &= -7 + \frac{57}{x + 8} \end{aligned}$$

Since $57 = 3 \cdot 19$ and keeping in mind x is positive we arrive at $x = 11, 49$ and the solutions $(x, y) = (11, 1), (49, 1)$.

Now if $y = 2$ then $d = 1$ and we arrive at $7x - 4 = 4x + 9$ or hence $3x = 13$ contradiction.

The solutions are hence $(x, y) = \boxed{(11, 1), (49, 1), (7m^2, 7m)}$. □

Example 1.4.4. *(1992 IMO) Find all integers a, b, c with $1 < a < b < c$ such that*

$$(a - 1)(b - 1)(c - 1)$$

divides $abc - 1$.

Solution. Set $a = x + 1, b = y + 1, c = y + 1$. We then arrive at

$$\begin{aligned} xyz &\mid (x + 1)(y + 1)(z + 1) - 1 \\ xyz &\mid xyz + xy + xz + yz + x + y + z + 1 - 1 \\ xyz &\mid xy + xz + yz + x + y + z \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} &+ \frac{1}{xy} + \frac{1}{xz} + \frac{1}{yz} \in \mathbb{Z} \end{aligned}$$

Now, notice that

$$S = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{xy} + \frac{1}{xz} + \frac{1}{yz} \le \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{1 \times 2} + \frac{1}{1 \times 3} + \frac{1}{2 \times 3} = 2\frac{5}{6}$$
$$S \implies \in \{1, 2\}$$

From $1 < a < b < c$, we get $1 \le x < y < z$. If we have $x, y, z \ge 4$, then we would have

$$S \le \frac{89}{120} \text{ (at (x,y,z)=(4,5,6))}$$

Contradiction. Therefore, because x is the smallest, $x \in \{1, 2, 3\}$. For each of the cases, we immediately set up the analogious equation set up from multiplying by yz and factoring. The reduction details are not included.

Case 1: $S = 1$

$$\begin{cases} x = 1 & \frac{1}{1} + \frac{1}{y} + \frac{1}{z} + \frac{1}{y} + \frac{1}{z} + \frac{1}{yz} = 1 \rightarrow\leftarrow \\ x = 2 & (y-3)(z-3) = 11 \implies (y, z) = (4, 14) \implies (x, y, z) = (2, 4, 14) \\ x = 3 & 4y + 4z + 3 = 2yz \implies 2 \mid 3 \rightarrow\leftarrow \end{cases}$$

Case 2: $S = 2$

$$\begin{cases} x = 1 & (y-2)(z-2) = 5 \implies (y, z) = (3, 7) \\ x = 2 & 3y + 3z + 2 = 3yz \rightarrow\leftarrow \\ x = 3 & (5y-4)(5z-4) = 31 \implies (y, z) = (1, 7) \end{cases} \implies (x, y, z) = (1, 3, 7), (3, 1, 7)$$

Keeping in mind $x < y < z$, we only have $(x, y, z) = (1, 3, 7)$. Therefore, the two solution pairs we have are

$$(x, y, z) = (2, 4, 14), (1, 3, 7) \implies (a, b, c) = (3, 5, 15), (2, 4, 8)$$

□

Example 1.4.5. *(Iran 1998) Suppose that a and b are natural numbers such that*

$$p = \frac{b}{4}\sqrt{\frac{2a-b}{2a+b}}$$

is a prime number. What is the maximum possible value of p?

Solution. If b is odd then $2a - b$ is odd so henceforth $\frac{b}{4}\sqrt{\frac{2a-b}{2a+b}}$ cannot be an integer. We consider two cases: $b = 4k$, or $b = 2m$ where m is odd.

Case 1: $b = 4k$

$$\begin{aligned} p = k\sqrt{\frac{2a-4k}{2a+4k}} &= k\sqrt{\frac{a-2k}{a+2k}} \\ \left(\frac{p}{k}\right)^2 &= \frac{a-2k}{a+2k} \\ p^2a + 2p^2k &= k^2a - 2k^3 \\ a(k^2 - p^2) &= 2k(k^2 + p^2) \\ a &= \frac{2k(k^2 + p^2)}{k^2 - p^2} \end{aligned}$$

We know that a must be an integer. Consider the cases $p \mid k$ and $p \nmid k$. The first case gives us $k = mp$. Therefore

$$a = \frac{2mp(m^2p^2 + p^2)}{m^2p^2 - p^2} = \frac{2mp(m^2+1)}{m^2-1}$$

We have $\gcd(m, m^2 - 1) = 1$ therefore we must have

$$\begin{aligned} \frac{2p(m^2+1)}{m^2-1} &= 2p\left(1 + \frac{2}{m^2-1}\right) \in \mathbb{Z} \\ &\implies \frac{4p}{m^2-1} \in \mathbb{Z} \end{aligned}$$

When m is even we must have $(m^2 - 1) \mid p \implies p = m^2 - 1 = (m-1)(m+1)$ since p is a prime. Therefore $m - 1 = 1$ which gives us $(p, m) = (3, 2)$. When m is odd we must have $\frac{m^2-1}{4} \mid p$ therefore $p = \frac{m^2-1}{2}$ or $p = \frac{m^2-1}{4}$. The first case renders no solutions while the second renders the solution $p = 2, m = 3$.

$p = 2$ gives the solution $(a, b, p) = (15, 24, 2)$ and $p = 3$ gives us $(a, b, p) = (20, 24, 3)$ by plugging into the above formulas.

Now when $p \nmid k$ we must have

$$\begin{aligned} a &= \frac{2k(k^2+p^2)}{k^2-p^2} \in \mathbb{Z} \\ \big(\text{using } \gcd(k, k^2-p^2) = 1\big) \implies \frac{2(k^2+p^2)}{k^2-p^2} &= 2 + \frac{4p^2}{k^2-p^2} \in \mathbb{Z} \\ \big(\text{using } \gcd(p^2, k^2-p^2) = 1\big) \implies \frac{4}{k^2-p^2} \in \mathbb{Z} \end{aligned}$$

However, this gives $\begin{cases} k^2 - p^2 = 1 \\ k^2 - p^2 = 2 \\ k^2 - p^2 = 4 \end{cases}$ of which gives no positive solution for p.

Case 2: $b = 2m$ where m is odd

$$\begin{aligned}
p &= \frac{m}{2}\sqrt{\frac{2a-2m}{2a+2m}} \\
p &= \frac{m}{2}\sqrt{\frac{a-m}{a+m}} \\
\left(\frac{2p}{m}\right)^2 &= \frac{a-m}{a+m} \\
4p^2a+4p^2m &= am^2-m^3 \\
a(m^2-4p^2) &= m(4p^2+m^2) \\
a &= \frac{m(4p^2+m^2)}{m^2-4p^2} = \frac{m(m^2+n^2)}{m^2-n^2}
\end{aligned}$$

Where $n = 2p$. Since $\gcd(m, 2) = 1$ we have two cases to consider: $p \mid m$ and $\gcd(m, n) = 1$.

When $\gcd(m, n) = 1$ however we have:

$$\begin{aligned}
\big(\text{using } \gcd(m, m^2-n^2)=1\big) \implies \frac{m^2+n^2}{m^2-n^2} &= 1+\frac{2n^2}{m^2-n^2} \in \mathbb{Z} \\
\gcd(n^2, m^2-n^2) = 1 \implies \frac{2}{m^2-n^2} \in \mathbb{Z}
\end{aligned}$$

This gives the cases: $\begin{cases} m^2-n^2=1 \\ m^2-n^2=2 \end{cases}$ which yields no valid solutions.

Therefore $p \mid m$. Let $m = pk$. We arrive at

$$a = \frac{pk(4p^2+p^2k^2)}{p^2(k^2-4)} = \frac{pk(4+k^2)}{k^2-4}$$

Keeping in mind the fact that k must be odd we arrive at $\gcd(k(k^2+4), k^2-4) = 1$. Therefore we must have $\frac{p}{k^2-4}$ be an integer or henceforth $k^2-4 \mid p$. Since p is prime we arrive at $p = k^2-4$. This is only solved when $k = 3$ which gives $p = 5$. This gives the solution pair $(a, b, p) = (39, 30, 5)$.

In conclusion the answer is $p = 5$. □

Example 1.4.6. *(David M. Bloom) Let p be a prime with $p > 5$, and let $S = \{p - n^2 | n \in \mathbb{N}, n^2 < p\}$. Prove that S contains two elements a*

and b such that $a|b$ and $1 < a < b$

Solution. (Rigorous) Let n be so that

$$(n+1)^2 > p > n^2 \tag{1.1}$$

Assume for the time being that $p - n^2 \neq 1$. Let $m = p - n^2$. We have

$$m|p - (n-m)^2$$

Set $a = m$ and $b = p - (n-m)^2$. All we need is for $n - m \neq 0$ and $|n - m| < n$ to satisfy the sets condition. If $m = n$ then we have $m + m^2 = p \implies m(m+1) = p$ absurd. Now we must prove $|n-m| < n$. If $n > m$ then it is obvious that $|n - m| = n - m < n$. If $m > n$ we must prove $m - n < n$ or $m < 2n$. Notice that via (1.1) we have $m < (n+1)^2 - n^2 = 2n + 1$. Therefore $m \leq 2n$. If $m = 2n$ then we would have $p = n^2 + 2n = n(n+2)$ hence $m < 2n$.

Now we must consider when $p-n^2 = 1$. In this case set $a = p-(n-1)^2 = 2n$. Since p is a prime we must have n is even (take mod 2 of the first equation). Therefore setting $b = p-1 = n^2$ we have $a|b$ and we are done. □

2

Modular Arithmetic

2.1 Inverses

Definition 2.1.1. We say that the **inverse** of a number a modulo m when a and m are relatively prime is the number b such that $ab \equiv 1 \pmod{m}$.

Example. The inverse of 3 mod 4 is 3 because $3 \cdot 3 = 9 \equiv 1 \pmod{4}$. The inverse of 3 mod 5 is 2 because $3 \cdot 2 = 6 \equiv 1 \pmod{5}$.

The following theorem is incredibly important and helps us to prove Euler's Totient Theorem and the existence of an inverse. Make sure that you understand the proof and theorem as we will be using it down the road.

Theorem 2.1.1. *Let a and m be relatively prime positive integers. Let the set of positive integers relatively prime to m and less than m be $R = \{a_1, a_2, \cdots, a_{\phi(m)}\}$. Prove that $S = \{aa_1, aa_2, aa_3, \cdots, aa_{\phi(m)}\}$ is the same as R when reduced mod m.*

Proof. Notice that every element of S is relatively prime to m. Also R and S have the same number of elements. Because of this, if we can prove that no two elements of S are congruent mod m we would be done. However

$$aa_x \equiv aa_y \pmod{m} \implies a(a_x - a_y) \equiv 0 \pmod{m} \implies a_x \equiv a_y \pmod{m}$$

which happens only when $x = y$ therefore the elements of S are distinct mod m and we are done. □

Theorem 2.1.2. *When* $\gcd(a, m) = 1$*,* a *always has a distinct inverse mod* m*.*

Proof. We notice that $1 \in R$ where we define $R = \{a_1, a_2, \cdots, a_{\phi(m)}\}$ to be the same as above. This must be the same mod m as an element in $\{aa_1, aa_2, \cdots, aa_{\phi(m)}\}$ by Theorem 1 henceforth there exists some a_x such that $aa_x \equiv 1 \pmod{m}$. □

Corollary 2.1.1. The equation $ax \equiv b \pmod{m}$ always has a solution when $\gcd(a, m) = 1$.

Proof. Set $x \equiv a^{-1}b \pmod{m}$. □

Example. Find the inverse of 9 mod 82.

Solution. Notice that $9 \cdot 9 \equiv -1 \pmod{82}$ therefore $9 \cdot (-9) \equiv 1 \pmod{82}$. The inverse of 9 mod 82 is hence $82 - 9 = 73$. □

Example 2.1.1. *Let* m *and* n *be positive integers posessing the following property: the equation*

$$\gcd(11k - 1, m) = \gcd(11k - 1, n)$$

holds for all positive integers k*. Prove that* $m = 11^r n$ *for some integer* r*.*

Solution. Define $v_p(a)$ to be the number of times that the prime p occurs in the prime factorization of a [1]. The given statement is equivalent to proving that $v_p(m) = v_p(n)$ when $p \neq 11$ is a prime. To prove this, assume on the contrary that WLOG we have

$$v_p(m) > v_p(n)$$

Write $m = p^a b, n = p^c d$ where b and d are relatively prime to p. We have $a > c$.

By Theorem 2 we know that there exists a solution for k such that $11k \equiv 1 \pmod{p^a}$. However, we now have

$$p^a \mid \gcd(11k - 1, m)$$

but $p^a \mid \gcd(11k - 1, n)$ implies that $p^a \mid n$ contradicting $a > c$. We are done. □

[1] We explore this function more in depth later

Comment. The reason that this logic does not apply for $p = 11$ is that the equation $11k \equiv 1 \pmod{11^a}$ does not have a solution in k. □

Example 2.1.2. *Let a and b be two relatively prime positive integers, and consider the arithmetic progression $a, a+b, a+2b, a+3b, \cdots$. Prove that there are infinitely many pairwise relatively prime terms in the arithmetic progression.*

Solution. We use induction. The base case is trivial. Assume that we have a set with m elements that are all relatively prime. Let this set be $S = \{a + k_1b, a + k_2b, \cdots, a + k_mb\}$. Let the set $\{p_1, p_2, \cdots, p_n\}$ be the set of all distinct prime divisors of elements of S. I claim that we can construct a new element. Let

$$a + xb \equiv 1 \pmod{p_1 \cdot p_2 \cdots \cdot p_n}$$

We know that there exists a solution in x to this equation which we let be $x = k_{m+1}$. Since $\gcd(a + k_{m+1}b, a + k_ib) = 1$, we have constructed a set with size $m + 1$ and we are done. □

2.2 Chinese Remainder Theorem

Theorem 2.2.1 (Chinese Remainder Theorem)**.** *The system of linear congruences*

$$\begin{cases} x \equiv a_1 \pmod{b_1}, \\ x \equiv a_2 \pmod{b_2}, \\ \cdots \\ x \equiv a_n \pmod{b_n}, \end{cases}$$

where $b_1, b_2, \cdots, b_n$ are pairwise relatively prime (aka $\gcd(b_i, b_j) = 1$ iff $i \neq j$) has one distinct solution for x modulo $b_1b_2\cdots b_n$.

Proof. We use induction. I start with proving that for the case

$$\begin{cases} x \equiv a_1 \pmod{b_1}, \\ x \equiv a_2 \pmod{b_2}, \end{cases}$$

there exists a unique solution mod $b_1 b_2$. To do so, consider the set of numbers

$$S = \{kb_1 + a_1, 0 \le k \le b_2 - 1\}.$$

By Corollary 1 it follows that the equation $kb_1 + a_1 \equiv a_2 \pmod{b_2}$ has a distinct solution in k. We have shown the unique existence of a solution to the above system of linear congruences.

Assume there is a solution for $n = k$ and I prove that there is a solution for $n = k + 1$. Let the following equation have solution $x \equiv z \pmod{b_1 b_2 \cdots b_k}$ by the inductive hypothesis:

$$\begin{cases} x \equiv a_1 \pmod{b_1} \\ x \equiv a_2 \pmod{b_2} \\ \cdots \\ x \equiv a_k \pmod{b_k}. \end{cases}$$

Therefore to find the solutions to the $k + 1$ congruences it is the same as finding the solution to

$$\begin{cases} x \equiv z \pmod{b_1 b_2 \cdots b_k} \\ x \equiv a_{k+1} \pmod{b_{k+1}}. \end{cases}$$

For this we can use the exact same work we used to prove the base case along with noting that from $\gcd(b_{k+1}, b_i) = 1$ for $i \in \{1, 2, \cdots, k\}$, we have $\gcd(b_{k+1}, b_1 b_2 \cdots b_k) = 1$. □

Comment. We sometimes shorthand "Chinese Remainder Theorem" to "CRT". □

Example 2.2.1. *Find the solution to the linear congruence*

$$\begin{cases} x \equiv 3 \pmod{5}, \\ x \equiv 4 \pmod{11}. \end{cases}$$

Solution. Notice that we may write x in the form $5k + 3$ and $11m + 4$.

$$x = 5k + 3 = 11m + 4$$

Taking this equation mod 5 we arrive at $11m + 4 \equiv 3 \pmod{5} \implies m \equiv -1 \pmod{5}$. We substitute $m = 5m_1 - 1$ to give us $x = 11(5m_1 - 1) + 4 = 55m_1 - 7$.

Therefore $x \equiv 48 \pmod{55}$ which means $\boxed{x = 55k + 48}$ for some integer k. □

Example 2.2.2 (AIME II 2012). *For a positive integer p, define the positive integer n to be p-safe if n differs in absolute value by more than 2 from all multiples of p. For example, the set of 10-safe numbers is $3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, \ldots$. Find the number of positive integers less than or equal to 10,000 which are simultaneously 7-safe, 11-safe, and 13-safe.*

Solution. We notice that if x is 7-safe, 11-safe, and 13-safe then we must have

$$\begin{cases} x \equiv 3, 4 \pmod{7} \\ x \equiv 3, 4, 5, 6, 7, 8 \pmod{11} \\ x \equiv 3, 4, 5, 6, 7, 8, 9, 10 \pmod{13} \end{cases}$$

By Chinese Remainder Solution this renders solutions mod 1001. We have 2 choices for the value of x mod 7, 6 choices for the value of x mod 11 and 8 choices for the value of x mod 13. Therefore, we have $2 \cdot 6 \cdot 8 = 96$ total solutions mod 1001.

We consider the number of solutions in the set

$$\{1, 2, \cdots, 1001\}, \{1002, \cdots, 2002\}, \{2003, \cdots, 3003\}, \cdots, \{9009, \cdots, 10010\}.$$

From above there are $96 \cdot 10 = 960$ total solutions. However we must subtract the solutions in the set $\{10,001; 10,002; \cdots; 10,010\}$.

We notice that only $x = 10,006$ and $x = 10,007$ satisfy $x \equiv 3, 4 \pmod{7}$.

	$10,006$	$10,007$
$\pmod{7}$	3	4
$\pmod{11}$	7	8
$\pmod{13}$	9	10

These values are arrived from noting that $10,006 \equiv -4 \pmod{7 \cdot 11 \cdot 13}$ and $10,007 \equiv -3 \pmod{7 \cdot 11 \cdot 13}$. Therefore $x = 10,006$ and $x = 10,007$ are the two values we must subtract off.

In conclusion we have $960 - 2 = \boxed{958}$ solutions. □

Example 2.2.3. *Consider a number line consisting of all positive integers greater than 7. A hole punch traverses the number line, starting frrom 7 and working its way up. It checks each positive integer n and punches it if and only if $\binom{n}{7}$ is divisible by 12. (Here $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.) As the hole punch checks more and more numbers, the fraction of checked numbers that are punched approaches a limiting number ρ. If ρ can be written in the form $\frac{m}{n}$, where m and n are positive integers, find $m+n$.*

Solution. Note that

$$\binom{n}{7} = \frac{n!}{(n-7)!7!} = \frac{n(n-1)(n-2)(n-3)(n-4)(n-5)(n-6)}{2^4 \cdot 3^2 \cdot 5 \cdot 7}.$$

In order for this to be divisible by $12 = 2^2 \cdot 3$, the numerator must be divisible by $2^6 \cdot 3^3$. (We don't care about the 5 or the 7; by the Pigeonhole Principle these will be canceled out by factors in the numerator anyway.) Therefore we wish to find all values of n such that

$$2^6 \cdot 3^3 \,|\, n(n-1)(n-2)(n-3)(n-4)(n-5)(n-6).$$

We start by focusing on the factors of 3, as these are easiest to deal with. By the Pigeonhole Principle, the expression must be divisible by $3^2 = 9$. Now, if $n \equiv 0, 1, 2, 3, 4, 5, \text{ or } 6 \pmod 9$, one of these seven integers will be a multiple of 9 as well as a multiple of 3, and so in this case the expression is divisible by 27. (Another possibility is if the numbers n, $n-3$, and $n-6$ are all divisible by 3, but it is easy to see that this case has already been accounted for.)

Now, we have to determine when the product is divisible by 2^6. If n is even, then each of $n, n-2, n-4, n-6$ is divisible by 2, and in addition exactly two of those numbers must be divisible by 4. Therefore the divisibility is sure. Otherwise, n is odd, and $n-1, n-3, n-5$ are divisible by 2.

- If $n-3$ is the only number divisible by 4, then in order for the product to be divisible by 2^6 it must also be divisible by 16. Therefore $n \equiv 3 \pmod{16}$ in this case.

- If $n-1$ and $n-5$ are both divisible by 4, then in order for the product to be divisible by 2^6 one of these numbers must also be divisible by 8. Therefore $n \equiv 1, 5 \pmod 8 \implies n \equiv 1, 5, 9, 13 \pmod{16}$.

Pooling all our information together, we see that $\binom{n}{7}$ is divisible by 12 iff n is such that

$$\begin{cases} n \equiv 0,1,2,3,4,5,6 & \pmod{9}, \\ n \equiv 0,1,2,3,4,5,6,8,9,10,12,13,14 & \pmod{16}. \end{cases}$$

There are 7 possibilities modulo 9 and 13 possibilities modulo 16, so by CRT there exist $7 \times 13 = 91$ solutions modulo $9 \times 16 = 144$. Therefore, as more and more numbers n are checked, the probability that $\binom{n}{7}$ is divisible by 12 approaches $\frac{91}{144}$. The requested answer is $91 + 144 = \boxed{235}$.

□

Example 2.2.4 (Austin Shapiro)**.** *Call a lattice point "visible" if the greatest common divisor of its coordinates is* 1*. Prove that there exists a* 100×100 *square on the board none of whose points are visible.*

Solution. Let the points on the grid be of the form

$$(x, y) = (a + m, b + n), \qquad 99 \geq m, n \geq 0.$$

We are going to use the Chinese Remainder Theorem to have every single term have a common divisor among the two coordinates. For the remainder of the problem assume that the sequence $\{p_j\}$ is a sequence of distinct prime numbers. Let $a \equiv 0 \left(\bmod \prod_{i=1}^{100} p_i\right)$. Then let

$$\begin{cases} b & \equiv 0 \pmod{p_1} \\ b+1 & \equiv 0 \pmod{p_2} \\ \cdots \\ b+99 & \equiv 0 \pmod{p_{100}}. \end{cases}$$

We find that repeating this process with letting $a+1 \equiv 0 \left(\bmod \prod_{i=101}^{200} p_i\right)$

and defining similarly

$$\begin{cases} b \equiv 0 \pmod{p_{101}} \\ b+1 \equiv 0 \pmod{p_{102}} \\ \cdots \\ b+99 \equiv 0 \pmod{p_{200}} \end{cases}$$

gives us the following:

$$\begin{cases} a & \equiv 0 \left(\bmod \prod_{i=1}^{100} p_i\right) \\ a+1 & \equiv 0 \left(\bmod \prod_{i=101}^{200} p_i\right) \\ \cdots \\ a+99 & \equiv 0 \left(\bmod \prod_{i=9901}^{10000} p_i\right) \end{cases} \quad \text{and} \quad \begin{cases} b & \equiv 0 \left(\bmod \prod_{i=0}^{99} p_{100i+1}\right) \\ b+1 & \equiv 0 \left(\bmod \prod_{i=0}^{99} p_{100i+2}\right) \\ \cdots \\ b+99 & \equiv 0 \left(\bmod \prod_{i=1}^{100} p_{100i}\right) \end{cases}.$$

This notation looks quite intimidating; take a moment to realize what it is saying. It is letting each $a+k$ be divisible by 100 distinct primes, then letting b be divisible by the first of these primes, $b+1$ be divisible by the second of these primes and so forth. This is precisely what we did in our first two examples above. By CRT we know that a solution exists, therefore we have proven the existence of a 100×100 grid.

□

Motivation. This problem requires a great deal of insight. When I solved this problem, my first step was to think about completing a 1×100 square as we did above. Then you have to think of how to extend this method to a 2×100 square and then generalizing the method all the way up to a 100×100 square. Notice that our construction is not special for 100, we can generalize this method to a $x \times x$ square! □

2.3 Euler's Totient Theorem and Fermat's Little Theorem

Theorem 2.3.1 (Euler's Totient Theorem)**.** *For a relatively prime to m, we have $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Proof. Using Theorem 2.1.1 the sets $\{a_1, a_2, \cdots, a_{\phi(m)}\}$ and $\{aa_1, aa_2, \cdots, aa_{\phi(m)}\}$ are the same mod m. Therefore, the products of each set must be the same mod m

$$a^{\phi(m)}a_1a_2\cdots a_{\phi(m)} \equiv a_1a_2\cdots a_{\phi(m)} \pmod{m} \implies a^{\phi(m)} \equiv 1 \pmod{m}.$$

□

Corollary 2.3.1 (Fermat's Little Theorem)**.** For a relatively prime to a prime p, we have $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Trivial. □

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

We do this problem in two different ways.

Solution. Notice that we may not directly use Fermats Little Theorem because 33 is not prime. However, we may use Fermats little theorem in a neat way: Notice that $2^2 \equiv 1 \pmod{3}$ and $2^{10} \equiv 1 \pmod{11}$ from Fermats Little Theorem. We will find $2^{98} \pmod{3}$ and $2^{98} \pmod{11}$ then combine the results to find $2^{98} \pmod{33}$.

$$2^{98} \equiv (2^2)^{49} \equiv 1^{49} \equiv 1 \pmod{3},$$

$$2^{98} \equiv \left[(2^{10})^9\right]\left(2^8\right) \equiv 2^8 \equiv 256 \equiv 3 \pmod{11}.$$

Let $x = 2^{98}$. Therefore, $x \equiv 1 \pmod{3}$ and $x \equiv 3 \pmod{11}$. Inspection gives us $x \equiv \boxed{25} \pmod{33}$. □

OR

Solution. We will use Euler's Totient Theorem. Notice that $\phi(33) = 33(1-\frac{1}{3})(1-\frac{1}{11}) = 20$, therefore $2^{20} \equiv 1 \pmod{33}$. Now, notice that

$$x = 2^{98} = (2^{20})^5 2^{-2} \equiv 4^{-1} \pmod{33}.$$

Therefore, since $x \equiv 4^{-1} \pmod{33} \implies 4x \equiv 1 \pmod{33}$. Using quick analysis, $x \equiv 25 \pmod{33}$ solves this hence $2^{98} \equiv \boxed{25} \pmod{33}$. Our answer matches our answer above so we feel fairly confident in it. □

Example 2.3.1 (Brilliant.org)**.** *For how many integer values of i, $1 \leq i \leq 1000$, does there exist an integer j, $1 \leq j \leq 1000$, such that i is a divisor of $2^j - 1$?*

Solution. For i even it is clear that we can't have $i|(2^j - 1)$. For i odd let $j = \phi(i)$ to give us $2^{\phi(i)} - 1 \equiv 0 \pmod{i}$. Since $\phi(i) < 1000$ it follows that for i odd there is always a value of j and hence the answer is $\frac{1000}{2} = \boxed{500}$. □

Example 2.3.2 (Brilliant.org)**.** *How many prime numbers p are there such that $29^p + 1$ is a multiple of p?*

Solution. When $p = 29$ we have $29 \nmid 29^p + 1$. Therefore we have $\gcd(p, 29) = 1$. By Fermat's Little Theorem

$$29^p + 1 \equiv 29 + 1 \equiv 0 \pmod{p}.$$

Therefore it follows that $p \mid 30$ and hence $p = 2, 3, 5$ for a total of $\boxed{3}$ numbers. □

Example 2.3.3 (AIME 1983)**.** *Let $a_n = 6^n + 8^n$. Determine the remainder on dividing a_{83} by 49.*

Solution. Notice that $\phi(49) = 42$. Therefore, $6^{84} \equiv 1 \pmod{49}$ and $8^{84} \equiv 1 \pmod{49}$.

$$\begin{aligned} 6^{83} + 8^{83} &\equiv (6^{84})(6^{-1}) + (8^{84})(8^{-1}) \pmod{49} \\ &\equiv 6^{-1} + 8^{-1} \pmod{49} \end{aligned}$$

Via expanding both sides out we find:

$$\begin{aligned} 6^{-1} + 8^{-1} &\equiv (6 + 8)6^{-1}8^{-1} \pmod{49} \\ &\equiv (14)\, 48^{-1} \pmod{49} \\ &\equiv (14)\, (-1) \pmod{49} \\ &\equiv 35 \pmod{49} \end{aligned}$$

□

Tip 2.3.1. When dealing with $a^{\phi n-1} \pmod{n}$ it is often easier to compute $a^{-1} \pmod{n}$ then to compute $a^{\phi n-1} \pmod{n}$ directly.

Comment. There exists a solution to this problem that uses solely the Binomial Theorem. Try to find it! □

Example 2.3.4 (All Russian MO 2000)**.** *Evaluate the sum*

$$\left\lfloor \frac{2^0}{3} \right\rfloor + \left\lfloor \frac{2^1}{3} \right\rfloor + \left\lfloor \frac{2^2}{3} \right\rfloor + \cdots + \left\lfloor \frac{2^{1000}}{3} \right\rfloor.$$

Solution. Note that we have

$$2^x \equiv \begin{cases} 1 \pmod{3} & \text{when } x \text{ is even,} \\ 2 \pmod{3} & \text{when } x \text{ is odd.} \end{cases}$$

Therefore

$$\sum_{n=0}^{1000} \left\lfloor \frac{2^n}{3} \right\rfloor = 0 + \sum_{n=1}^{500} \left(\left\lfloor \frac{2^{2n-1}}{3} \right\rfloor + \left\lfloor \frac{2^{2n}}{3} \right\rfloor \right) = \sum_{n=1}^{500} \left(\frac{2^{2n-1}-2}{3} + \frac{2^{2n}-1}{3} \right)$$
$$= \frac{1}{3} \sum_{n=1}^{500} (2^{2n-1} + 2^{2n} - 1) = \frac{1}{3} \sum_{n=1}^{1000} 2^n - 500 = \boxed{\frac{1}{3}(2^{1001}-2) - 500}.$$

□

Tip 2.3.2. When working with floor functions, try to find a way to make the fractions turn into integers.

Example 2.3.5 (HMMT 2009)**.** *Find the last two digits of* 1032^{1032}. *Express your answer as a two-digit number.*

Solution. $\begin{cases} 1032^{1032} \equiv 0 \pmod{4} \\ 1032^{1032} \equiv 7^{1032} \equiv (-1)^{516} \equiv 1 \pmod{25} \end{cases} \implies 1032^{1032} \equiv \boxed{76} \pmod{100}$ □

Tip 2.3.3. When we have to calculuate $a \pmod{100}$ it is often more helpful to find $\begin{cases} a \pmod{4} \\ a \pmod{25} \end{cases}$ and then using the Chinese Remainder Theorem to find $a \pmod{100}$. We can do similar methods when dealing with $a \pmod{1000}$.

Example 2.3.6 (Senior Hanoi Open MO 2006)**.** *Calculuate the last three digits of* $2005^{11} + 2005^{12} + \cdots + 2005^{2006}$*.*

Solution. By reducing the expression modulo 1000, it remains to find the last three digits of the somewhat-less-daunting expression

$$2005^{11} + 2005^{12} + \cdots + 2005^{2006} \equiv 5^{11} + 5^{12} + \cdots + 5^{2006} \pmod{1000}.$$

Notice that $5^{11} + 5^{12} + \cdots + 5^{2006} \equiv 0 \pmod{125}$.

Next, we want $5^{11} + 5^{12} + \cdots + 5^{2006} \pmod{8}$. Notice that $5^2 \equiv 1 \pmod{8}$ and therefore $5^{2k} \equiv 1 \pmod{8}$ and $5^{2k+1} \equiv 5 \pmod{8}$. Henceforth

$$5^{11} + 5^{12} + \cdots + 5^{2006} \equiv \frac{1996}{2}(1+5) \equiv 4 \pmod{8}$$

.

Therefore $5^{11} + 5^{12} + \cdots + 5^{2006} \equiv \boxed{500} \pmod{1000}$.

□

Example 2.3.7 (PuMAC[a])**.** *Calculuate the last* 3 *digits of* $2008^{2007^{2006^{\cdots^{2^1}}}}$.

[a] Princeton University Mathematics Competition

Solution. To begin we notice $2008^{2007^{2006^{\cdots^{2^1}}}} \equiv 0 \pmod{8}$.

Next, we notice via Euler's Totient:

$$2008^{2007^{2006^{\cdots^{2^1}}}} \equiv 2008^{2007^{2006^{\cdots^{2^1}}} \pmod{\phi(125)}} \pmod{125}$$

Now notice

$$2007^{2006^{\cdots^{2^1}}} \equiv 7^{2006^{\cdots^{2^1}}} \pmod{100} \equiv 1 \pmod{100}$$

since $7^4 \equiv 1 \pmod{100}$. Therefore $2008^{2007^{2006^{\cdots^{2^1}}}} \equiv 2008^1 \equiv 8 \pmod{125}$. Henceforth

$$2008^{2007^{2006^{\cdots^{2^1}}}} \equiv \boxed{8} \pmod{1000}.$$

□

Tip 2.3.4. When a and n are relatively prime we have

$$a^b \equiv a^{b \pmod{\phi(n)}} \pmod{n}$$

It then suffices to calculate $b \pmod{\phi(n)}$.

Example 2.3.8 (PuMAC 2008)**.** *Define $f(x) = x^{x^{x^x}}$. Find the last two digits of $f(17) + f(18) + f(19) + f(20)$.*

Solution. We compute each individual term seperately.

- $f(20) \equiv 0 \pmod{100}$
- $\begin{cases} f(19) \equiv (-1)^{19^{19^{19}}} \equiv -1[4] \\ f(19) \equiv 19^{19^{19^{19}} \pmod{\phi 25}} \equiv 19^{-1} \equiv 4[25] \end{cases} \implies f(19) \equiv 79[100]$
- $\begin{cases} 18^{18^{18^{18}}} \equiv 0[4] \\ 18^4 \equiv 1[25] \implies 18^{18^{18^{18}}} \equiv 1 \pmod{25} \end{cases} \implies f(18) \equiv 76[100]$

- $$\begin{cases} f(17) \equiv 1 \pmod{4} \end{cases}$$
  $$\begin{cases} f(17) \equiv 17^{17^{17^{17}} \pmod{20}} \pmod{25} \\ \phi(20) = 8 \implies 17^{17^{17}} \equiv 17 \pmod{20} \\ f(17) \equiv 17^{17} \pmod{25} \\ 17^{16} \equiv (17^2)^8 \equiv \left((14)^2\right)^4 \equiv \left((-4)^2\right)^2 \equiv 16^2 \equiv 6 \pmod{25} \\ \implies f(17) \equiv (17)(6) \equiv 2 \pmod{25} \end{cases}$$

  $$\longrightarrow f(17) \equiv 77 \pmod{100}$$

  Therefore

  $$f(17)+f(18)+f(19)+f(20) \equiv 77+76+79+0 \equiv 232 \equiv \boxed{32} \pmod{100}$$

□

Comment. We pooled together all of our tips so far. □

Example 2.3.9 (AoPS)**.** *Show that for $c \in \mathbb{Z}$ and a prime p, the congruence $x^x \equiv c \pmod{p}$ has a solution.*

Solution. Suppose that x satisfies the congruences

$$\begin{cases} x & \equiv c \pmod{p}, \\ x & \equiv 1 \pmod{p-1}. \end{cases}$$

Then by Fermat's Little Theorem we have

$$x^x \equiv x^{x \pmod{p-1}} \equiv x^1 \equiv c \pmod{p}.$$

All that remains is to show that there actually exists a number with these properties, but since $(p, p-1) = 1$, there must exist such a solution by Chinese Remainder Theorem. ■ □

Example 2.3.10 (Balkan). *Let n be a positive integer with $n \geq 3$. Show that*

$$n^{n^{n^n}} - n^{n^n}$$

is divisible by 1989.

Solution. Note that $1989 = 3^2 \times 13 \times 17$. Therefore, we handle each case separately.

- First, we prove that

  $$n^{n^{n^n}} \equiv n^{n^n} \pmod{9}$$

  for all n. If $3|n$ then we are done. Otherwise, since $\phi(9) = 6$, the problem reduces itself to proving that

  $$n^{n^n} \equiv n^n \pmod{6}$$

  This is not hard to show true. It is obvious that $n^{n^n} \equiv n^n \pmod{2}$, and (as long as n is not divisible by 3) showing the congruence modulo 3 is equivalent to showing that $n^n \equiv n \pmod{\phi(3)}$, which is trivial since n and n^n have the same parity.

- Next, we prove that

  $$n^{n^{n^n}} \equiv n^{n^n} \pmod{13}$$

  This is a very similar process. If $13|n$ we are done; otherwise, the problem is equivalent to showing that

  $$n^{n^n} \equiv n^n \pmod{12}$$

  We have already shown that these two expressions are congruent modulo 3, and showing that they are equivalent modulo 4 is equivalent to showing that $n^n \equiv n \pmod{\phi(4)}$, and since $\phi(4) = 2$ this is trivial. Therefore they are congruent modulo 12 and this second case is complete.

- Finally, we prove that

  $$n^{n^{n^n}} \equiv n^{n^n} \pmod{17}$$

, which once again is quite similar. If $17|n$ we are done, otherwise the problem reduces itself to proving that

$$n^{n^n} \equiv n^n \pmod{16}$$

If $2|n$ in this case then the problem is solved; otherwise, it reduces itself again to proving that $n^n \equiv n \pmod{8}$. This is the most difficult case of this problem, but it is still not hard. Note that since n is odd, $n^2 \equiv 1 \pmod{8}$. Therefore $n^{n-1} \equiv 1 \pmod{8}$ and $n^n \equiv n \pmod{8}$. Through this, we have covered all possibilities, and so we are done with the third case.

We have shown that the two quantities are equivalent modulo 9, 13, and 17, so by Chinese Remainder Theorem they must be equivalent modulo $9 \times 13 \times 17 = 1989$, as desired. □

Example 2.3.11 (Canada 2003)**.** *Find the last* 3 *digits of* $2003^{2002^{2001}}$.

Solution. Taking the number directly mod 1000 doesn't give much (try it out and see!) Therefore we are going to do it in two different parts: Find the value mod 8 and find the value mod 125 then combine the two values. First off note that $\phi(8) = 4$ and $\phi(125) = 100$.

$$\begin{cases} 2003^{2002^{2001}} & \equiv 3^{2002^{2001}} \pmod{8} \\ 2002^{2001} & \equiv 0 \pmod{\phi(8)} \end{cases} \implies 3^{2002^{2001}} \equiv 3^0 \equiv 1 \pmod{8}$$

Now notice that $2003^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod{125}$. To find this we must find $2002^{2001} \equiv 2^{2001} \pmod{\phi(125) = 100}$. We split this up into finding $2^{2001} \pmod{4}$ and $2^{2001} \pmod{25}$:

$$\begin{cases} 2^{2001} & \equiv 0 \pmod{4} \\ 2^{2001} = 2^1(2^{20})^{100} = 2^1(2^{\phi(25)})^{100} & \equiv 2 \pmod{25} \end{cases} \implies x \equiv 52 \pmod{100}$$

Therefore we have $3^{2002^{2001}} \equiv 3^{52} \pmod{125}$. It is a tedious work but as this problem appeared on a mathematical olympiad stage it should be done by hand.

$$\begin{aligned}3^{52} &\equiv (3^5)^{10}(3^2) \pmod{125}\\ &\equiv (-7)^{10}(9) \pmod{125} \equiv (49)^5(9) \pmod{125}\\ &\equiv \left(49^2\right)^2(49)(9) \pmod{125} \equiv (26^2)(49)(9) \pmod{125}\\ &\equiv (51)(49)(9) \pmod{125} \equiv -9 \equiv 116 \pmod{125}\end{aligned}$$

Let $x = 2003^{2002^{2001}}$.

$$\begin{cases} x \equiv 1 \pmod 8 & \implies x = 8k+1\\ x \equiv 116 \pmod{125} & \implies x = 125m + 116\end{cases}.$$

Therefore, $x = 125m + 116 = 8k + 1$. Taking mod 8 of this equation we arrive at $5m + 4 \equiv 1 \pmod 8$ or $5m \equiv 5 \pmod 8$ hence $m \equiv 1 \pmod 8$. Henceforth we have $m = 8m_1 + 1$ or

$$x = 125(8m_1 + 1) + 116 = 1000m_1 + 241.$$

Therefore $x \equiv \boxed{241} \pmod{1000}$.

Comment. This is a nice problem to finish up our exponentation section. We calculate the number mod 8 and mod 125. However, in doing so we must find $2002^{2001} \pmod{\phi(125)}$ and after a lot of calculations we get back to our Chinese Remainder Theorem problem. □

Comment. There are much nicer solutions online for this problem (one can be found at [13]). □

□

Tips. *These are very helpful tips for dealing with problems involving exponentation.*

- *When dealing with* $a^{\phi n-1} \pmod n$ *it is often easier to compute* $a^{-1} \pmod n$ *then to compute* $a^{\phi n-1} \pmod n$ *directly.*
- *When we have to calculuate* $a \pmod{100}$ *it is often more helpful to find* $\begin{cases} a \pmod 4\\ a \pmod{25}\end{cases}$ *and then using the Chinese Remainder Theorem to find* $a \pmod{100}$*. We can do similar methods when dealing with* $a \pmod{1000}$.

- *When a and n are relatively prime we have*

$$a^b \equiv a^{b \pmod{\phi(n)}} \pmod{n}$$

It then suffices to calculuate $b \pmod{\phi(n)}$.

Example 2.3.12 (Balkan MO 1999)**.** *Let $p > 2$ be a prime number such that $3|(p-2)$. Let*

$$S = \{y^2 - x^3 - 1 | 0 \leq x, y \leq p - 1 \cap x, y \in \mathbb{Z}\}$$

Prove that there are at most p elements of S divisible by p.

Solution. Despite the intimidiating notation, all that it is saying for S is that S is the set of $y^2 - x^3 - 1$ when x and y are positive integers and $0 \leq x, y \leq p - 1$ (essentially meaning x, y are reduced mod p).

Lemma. When $a \not\equiv b \pmod{p}$ we have $a^3 \not\equiv b^3 \pmod{p}$.

Proof. Assuming to the contrary that for some a, b with $a \not\equiv b \pmod{p}$ we have $a^3 \equiv b^3 \pmod{p}$. Since $\frac{p-2}{3}$ is an integer raising both sides to that power gives us

$$\begin{aligned}
(a^3)^{\frac{p-2}{3}} &\equiv (b^3)^{\frac{p-2}{3}} \pmod{p} \\
a^{p-2} &\equiv b^{p-2} \pmod{p} \\
a^{-1} &\equiv b^{-1} \pmod{p} \\
a &\equiv b \pmod{p}
\end{aligned}$$

With the last step following from the fact that every element has a unique inverse mod p.

□

We now count how many ways we have $y^2 - x^3 - 1 \equiv 0 \pmod{p}$. Notice that we must have $x^3 \equiv y^2 - 1 \pmod{p}$. For each value of y there is at most one value of x which corresponds to it. Since there are a total of p values of y there is at most p pairs (x, y) such that $y^2 - x^3 - 1 \equiv 0 \pmod{p}$. □

Motivation. The motivation behind this solution was trying a simple case. When $p = 5$ we notice that we have:

$x \pmod 5$	$x^2 \pmod 5$	$x^3 \pmod 5$
0	0	0
1	1	1
2	4	3
3	4	2
4	1	4

We need for the difference of an x^2 and y^3 to be 1. We notice that for each value of x^2 there can only be one value of y^3 that goes along with it. Then we go on to prove the general case. □

Example 2.3.13 (USAMO 1991)**.** *Show that, for any fixed integer* $n \geq 1$, *the sequence*

$$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}, \ldots \pmod n$$

is eventually constant.

[The tower of exponents is defined by $a_1 = 2$, $a_{i+1} = 2^{a_i}$. *Also* $a_i \pmod n$ *means the remainder which results from dividing* a_i *by* n*.]*

Solution. First, define the recursive sequence $\{a_k\}$ such that $a_1 = 2$ and $a_{i+1} = 2^{a_i}$ for each $i \geq 1$. It is clear that the sequence of a_i's maps to the sequence of integers described in the original problem.

In addition, for each positive integer n, consider a recursive sequence $\{b_k\}$ such that b_1 is the largest odd integer that evenly divides n and for each $i \geq 1$, b_{i+1} is the largest odd integer that evenly divides $\phi(b_i)$. For example, when $n = 62$, $b_1 = 31$, $b_2 = 15$, and $b_3 = 1$. Note that it is obvious that at some positive integer i we have $b_i = 1$, since the sequence of b_i's is monotonically decreasing.

Now consider a term of the sequence of towers of 2 with a sufficient number of 2s, say a_m. We wish to have for all sufficiently large m:

$$a_{m+1} \equiv a_m \pmod n$$

Note that we can write n in the form $2^{k_1}b_1$, where k_1 is a nonnegative integer. By Chinese Remainder Theorem, it suffices to check

$$\begin{cases} a_{m+1} \equiv a_m \pmod{2^{k_1}}, \\ a_{m+1} \equiv a_m \pmod{b_1}. \end{cases}$$

Since m is sufficiently large, $a_{m+1} \equiv a_m \equiv 0 \pmod{2^{k_1}}$. All that remains is to check if $a_{m+1} \equiv a_m \pmod{b_1}$. By Euler's Totient Theorem, since $\gcd(2, b_1) = 1$ we have $2^{\phi(b_1)} \equiv 1 \pmod{b_1}$, so

$$a_m = 2^{a_{m-1}} \equiv 2^{a_{m-1} \bmod \phi(b_1)} \pmod{b_1}.$$

Therefore, we now want $a_m \equiv a_{m-1} \pmod{\phi(b_1)}$. Since $\phi(b_1) = 2^{k_2}b_2$ we must check

$$\begin{cases} a_m \equiv a_{m-1} \pmod{2^{k_2}}, \\ a_m \equiv a_{m-1} \pmod{b_2}. \end{cases}$$

Because m is sufficiently large

$$a_m \equiv a_{m-1} \equiv 0 \pmod{2^{k_2}},$$

and so it suffices to check if $a_m \equiv a_{m-1} \pmod{b_2}$. We can continue this method all the way down to the integer i such that $b_i = 1$ at which point the equation $a_m \equiv a_{m-1} \equiv 0 \pmod{b_i}$ is clearly true so hence we have arrived at a true statement. Therefore $a_{m+1} \equiv a_m \pmod{n}$ for sufficiently large m and we are done. □

Motivation. The choice for the b_i sequence may be a bit confusing therefore I try my best to explain the motivation here.

When wishing to prove $a_{m+1} \equiv a_m \pmod{n}$ by Euler's Totient we try to see if we can have $a_m \equiv a_{m-1} \pmod{\phi(n)}$. If $\phi(n)$ was odd then we could continue on this method until we have $\phi\left(\phi(\cdots\phi(n))\right) = 1$ at which point since we have chosen m to be sufficiently large we would get a true statement.

Thankfully we patch the arugment by considering the largest odd divisor of $\phi(n)$ and using Chinese Remainder Theorem. That is where the idea for the b_i sequence comes from. □

Example 2.3.14 (ISL 2005 N6)**.** *Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that $a = b$.*

Solution. I desire to prove that for all primes $b \equiv a \pmod{p}$. Fix a to be a constant value and I construct a way to find the corresponding value of n which tells us that $b \equiv a \pmod{p}$. Notice that the following conditions are the same:

$$(a^n + n) \mid (b^n + n) \iff (a^n + n) \mid (b^n - a^n).$$

We set

$$\begin{cases} n \equiv -a \pmod{p}, \\ n \equiv 1 \pmod{p-1}. \end{cases}$$

Because $n \equiv 1 \pmod{p-1}$ we have $a^n \equiv a \pmod{p}$ via Fermat's Little Theorem. Also, because $n \equiv -a \pmod{p}$ we have $p|(a^n+n) \implies p|(b^n-a^n)$ However, $b^n \equiv b \pmod{p}$ and $a^n \equiv a \pmod{p}$ from $n \equiv 1 \pmod{p-1}$ therefore $b \equiv a \pmod{p}$ for all primes p hence $b = a$.

□

Motivation. The way I solved this problem was consider the case when $a = 1$ at first. In this case we must have $(n + 1) \mid b^n + n$. We desire to prove $b \equiv 1 \pmod{p}$ for all primes p. We notice that $b^n + n \equiv b^n - 1 \pmod{n+1}$. If we have $p|(n + 1)$ and $b^n \equiv b \pmod{p}$ then we would be done. The condition $b^n \equiv b \pmod{p}$ is satisfied when $n \equiv 1 \pmod{p-1}$ and the condition $p|(n + 1)$ is satisfied when $n \equiv -1 \pmod{p}$. Therefore we have proven the problem for $a = 1$. □

Comment. Notice how elementary techniques solves an IMO Shortlist N6 (a relatively difficult problem). □

2.3.1 Problems for the reader

Problem 2.3.1. (2003 Polish) Find all polynomials W with integer coefficients satisfying the following condition: for every natural number n, $2^n - 1$ is divisible by $W(n)$.

2.4 The equation $x^2 \equiv -1 \pmod{p}$

Theorem 2.4.1 (Wilson's)**.** *$(p-1)! \equiv -1 \pmod{p}$ for all odd primes p.*

Proof. Start out with looking at a few examples. $p = 5$ gives $4! = 24 \equiv -1 \pmod{5}$. However, another way to compute this is to note that

$$4! = (1 \cdot 4)(2 \cdot 3) \equiv (4)(6) \equiv (1)(4) \equiv -1 \pmod{5}.$$

We test $p = 7$ which gives $6! = 720 = 7(103) - 1 \equiv -1 \pmod{7}$ Also,

$$6! = (1 \cdot 6)(2 \cdot 4)(3 \cdot 5) = (6)(8)(15) \equiv (6)(1)(1) \equiv -1 \pmod{7}.$$

What we are doing is we are looking at all the terms in $(p-1)!$ and finding groups of two that multiply to 1 mod p. I will now prove that this method always works.

Notice that for all $x \in \{2, 3, \cdots, p-2\}$ there exists a $y \neq x$ such that $xy \equiv 1 \pmod{p}$ by Theorem 2 and the fact that $x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}$. Since p is odd, we can pair the inverses off into $\frac{p-3}{2}$ pairs. Let these pairs be $(x_1, y_1), (x_2, y_2), (x_3, y_3), \cdots (x_{(p-3)/2}, y_{(p-3)/2})$

Therefore,

$$\begin{aligned}(p-1)! &\equiv (1)(p-1)(x_1 y_1)(x_2 y_2) \cdots \left[x_{(p-3)/2} y_{(p-3)/2}\right] \pmod{p} \\ &\equiv (1)(p-1)(1)(1) \cdots (1) \pmod{p} \\ &\equiv -1 \pmod{p}.\end{aligned}$$ □

Theorem 2.4.2. *There exists an x with $x^2 \equiv -1 \pmod{p}$ if and only if $p \equiv 1 \pmod{4}$.*

Proof. For the first part notice that

$$\begin{aligned}x^2 &\equiv -1 \pmod{p} \\ (x^2)^{\frac{p-1}{2}} &\equiv (-1)^{\frac{p-1}{2}} \pmod{p} \\ x^{p-1} &\equiv (-1)^{\frac{p-1}{2}} \pmod{p} \\ 1 &\equiv (-1)^{\frac{p-1}{2}} \pmod{p},\end{aligned}$$

which happens only when $p \equiv 1 \pmod{4}$.

Now proving the other way requires a bit more work. First off from Wilsons theorem $(p-1)! \equiv -1 \pmod{p}$. Therefore our equation turns into $x^2 \equiv (p-1)! \pmod{p}$. Notice that

$$\begin{aligned}(p-1)! &= [(1)(p-1)]\,[(2)(p-2)]\cdots\left[\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\right]\\ &\equiv [(1)(-1)]\,[(2)(-2)]\left[\left(\frac{p-1}{2}\right)\left(-\frac{p-1}{2}\right)\right] \pmod{p}\\ &\equiv (-1)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}\\ &\equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}\end{aligned}$$

Therefore $x = \left(\frac{p-1}{2}\right)!$ solves the equation and we have proven the existence of x. □

Example 2.4.1. *Prove that there are no positive integers x, k and $n \geq 2$ such that $x^2 + 1 = k(2^n - 1)$.*

Solution. Notice that the condition is equivalent to $x^2+1 \equiv 0 \pmod{2^n-1}$. Since $2^n-1 \equiv 3 \pmod{4}$ it follows that there exists a prime divisor of 2^n-1 that is of the form $3 \pmod{4}$ (if not then $2^n-1 \equiv 1 \pmod{4}$). Label this prime divisor to be p. Therefore we have

$$x^2 + 1 \equiv 0 \pmod{p} \rightarrow\leftarrow$$

□

Example 2.4.2 (Korea 1999)**.** *Find all positive integers n such that $2^n - 1$ is a multiple of 3 and $(2^n-1)/3$ is a divisor of $4m^2+1$ for some integer m.*

Solution. Since $2^n - 1 \equiv 0 \pmod{3}$, we must have $n = 2k$. Therefore, our desired equation is $\frac{4^k-1}{3} | 4m^2+1$. I claim that $k = 2^m$ for $m \geq 0$ is a solution to this. To prove this requires using difference of squares and then the Chinese remainder theorem:

$$\begin{aligned}\frac{4^k-1}{3} &= \frac{4^{2^m}-1}{3} = \frac{(4^{2^{m-1}}+1)(4^{2^{m-2}}+1)\cdots(4+1)(4-1)}{3}\\ &= (4^{2^{m-1}}+1)(4^{2^{m-2}}+1)\cdots(4+1).\end{aligned}$$

We must have $4m^2 + 1 \equiv 0 \pmod{(4^{2^{m-1}} + 1)(4^{2^{m-2}} + 1) \cdots (4 + 1)}$. To use the Chinese Remainder Theorem to seperate this into different parts we must have all numbers in the product to be relatively prime. To prove this we notice that $4^{2^a} + 1 = 2^{2^{a+1}} + 1$ and then use the following lemma.

Lemma. Define $F_m = 2^{2^m} + 1$ to be a Fermat number. Prove that all Fermat numbers are pairwise relatively prime.

Proof. ([12])

Start out with noting that $F_m = F_{m-1}F_{m-2} \cdots F_0 + 2$. To prove this we use induction. Notice that for $m = 1$, we have $F_1 = F_0 + 2$ since $F_1 = 2^{2^1} + 1 = 5$ and $F_0 = 2^{2^0} + 1 = 3$. Assume this holds for $m = k$ and I prove it holds for $m = k + 1$.

$$\begin{array}{rcl} F_{m+1} & = & F_m F_{m-1} \cdots F_0 + 2 \\ \iff F_{m+1} & = & F_m(F_m - 2) + 2 \text{ from inductive hypothesis} \\ \iff F_{m+1} & = & F_m^2 - 2F_m + 2 \\ \iff F_{m+1} & = & (F_m - 1)^2 + 1 \\ \iff F_{m+1} & = & (2^{2^m})^2 + 1 \end{array}$$

The last step is true by definition therefore our induction is complete.

Now for $0 \le i \le m - 1$,

$$\gcd(F_m, F_i) = \gcd\left[F_{m-1}F_{m-2} \cdots F_0 + 2 - F_i(F_{m-1}F_{m-2} \cdots F_{i+1}F_{i-1} \cdots F_0), F_i\right] = \gcd(2, F_i) = 1.$$

When we range m over all possible non-negative integers we arrive at the conclusion that all pairs of Fermat numbers are relatively prime. □

Notice that each term in the mod is the same as a Fermat number as $4^{2^a} = 2^{2^{a+1}} = F_{a+1}$ for $a \ge 0$. Hence, by Chinese Remainder Theorem the condition

$$4m^2 + 1 \equiv 0 \pmod{(4^{2^{m-1}} + 1)(4^{2^{m-2}} + 1)(\cdots)(4 + 1)}$$

is the same as

$$\begin{cases} 4m^2 + 1 \equiv 0 \pmod{4^{2^{m-1}} + 1}, \\ 4m^2 + 1 \equiv 0 \pmod{4^{2^{m-2}} + 1}, \\ \cdots \\ 4m^2 + 1 \equiv 0 \pmod{4 + 1}. \end{cases}$$

Now, notice that $4^{2^a} + 1 = 4(4^{2^a - 1}) + 1 = 4\left(2^{2^a - 1}\right)^2 + 1$ for $a \ge 0$. Therefore, the solution to the equation $4m^2 + 1 \equiv 0 \pmod{4^{2^a} + 1}$ is $m \equiv$

$2^{2^a-1} \pmod{4^{2^a}+1}$. Therefore by Chinese Remainder Theorem there exists an m that satisfies all the above congruences and we have proved $k = 2^m$ for $m \geq 0$ works.

Assume that $k \neq 2^m$ and hence $k = p2^m$ for $m \geq 0$ and p being an odd integer that is not 1. Then

$$\frac{4^{2^m p}-1}{3} = \frac{(4^{2^{m-1}p}+1)(4^{2^{m-2}p}+1)\cdots(4^p+1)(4^p-1)}{3}.$$

Notice that we must have

$$4m^2+1 \equiv 0 \left(\bmod\ \frac{4^{2^m * p}-1}{3}\right) \implies 4m^2+1 \equiv 0 \left(\bmod\ \frac{4^p-1}{3}\right)$$

Notice that $\frac{4^p-1}{3} = \frac{(2^p-1)(2^p+1)}{3}$. However, since p is odd we have $3 \mid 2^p+1$ so

$$4m^2+1 \equiv 0 \left(\bmod\ \frac{4^p-1}{3}\right) \implies 4m^2+1 \equiv 0 \,(\bmod\, 2^p-1)$$

Since $p > 1$ we clearly have $2^p - 1 \equiv 3 \pmod 4$. Assume that all prime divisors of 2^p-1 are of the form $1 \pmod 4$. However, this would imply that $2^p-1 \equiv 1 \pmod 4$ a contradiction therefore there exists at least one prime divisor of 2^p-1 that is of the form $3 \pmod 4$. Label this prime divisor to be z.

$$(2m)^2 \equiv -1 \left(\bmod\ \frac{4^p-1}{3}\right) \equiv -1 \pmod z$$

but by Theorem 3 this is a contradiction. Henceforth the answer is $k = 2^m$ for $m \geq 0$; therefore $n = 2^r$ for $r \geq 1$. □

Comment. We notice that the condition $4m^2+1 \equiv 0 \left(\bmod\ \frac{2^n-1}{3}\right)$ is not satisfied when $\frac{2^n-1}{3}$ has a prime factor of the form $3 \pmod 4$. That is the main motivation behind the solution, the rest boils down to proving the case $n = 2^r$ for $r \geq 1$ satisfies the equation and proving that when $n = p2^r$ we can find a prime factor of the form $3 \pmod 4$.

The way that I came to the conclusion that $n = 2^r$ would satisfy the equation was by trying small examples for n. We notice that $n = 2, 4, 8$ all satisfy the equation however $n = 3, 5, 6, 7$ all cannot satisfy the equation. We find the reason that the values of n cannot satisfy the equation (which is by theorem 3), and we proceed to test our hypothesis. □

2.5 Order

Definition 2.5.1. The *order* of a mod m (with a and m relatively prime) is the smallest positive integer x such that $a^x \equiv 1 \pmod{m}$. We write this as $x = \text{ord}_m a$ or sometimes shorthanded to $o_m a$.

Example. The order of 2 mod 9 is 6 because $2^1 \equiv 2 \pmod 9, 2^2 \equiv 4 \pmod 9, 2^3 \equiv 8 \pmod 9, 2^4 \equiv 7 \pmod 9, 2^5 \equiv 5 \pmod 9, 2^6 \equiv 1 \pmod 9$.

Example. Prove that the order of a mod m (with a and m relatively prime) is less than or equal to $\phi(m)$.

Proof. By Euler's Totient theorem we have

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Since order is the smallest x such that $a^x \equiv 1 \pmod{m}$ it follows that $x \leq \phi(m)$. □

The following theorem is incredibly important and we will use it a lot throughout the document.

Theorem 2.5.1. *For relatively prime positive integers a and m prove that $a^n \equiv 1 \pmod{m}$ if and only if*

$$ord_m a \mid n$$

Proof. If $\text{ord}_m a \mid n$ then we have $n = \text{ord}_m a q$ for some q. Therefore

$$a^n \equiv \left(a^{\text{ord}_m a}\right)^q \equiv 1 \pmod{m}$$

Now to prove the other direction. By the division algorithm we can write

$$n = (\text{ord}_m a)\, q + r \qquad 0 \leq r < \text{ord}_a m, q \in \mathbb{Z}$$

We now notice that

$$\begin{aligned} a^{(\text{ord}_m a)q+r} = a^n &\equiv 1 \pmod{m} \\ \implies a^{(\text{ord}_m a)q} a^r &\equiv 1 \pmod{m} \\ \implies a^r &\equiv 1 \pmod{m} \end{aligned}$$

However $r < \text{ord}_m a$ contradicting the minimality of $\text{ord}_m a$ if $r \neq 0$. Therefore $r = 0$ and we are done. □

Corollary 2.5.1. For relatively prime positive integers a and m

$$\text{ord}_m a \mid \phi(m)$$

Proof. Set $n = \phi(m)$ and use Euler's Totient theorem. □

Example 2.5.1. *For positive integers $a > 1$ and n find $\text{ord}_{a^n-1}(a)$*

Solution. We check that the order exists by noting $\gcd(a^n-1, a) = 1$. Notice that

$$\text{ord}_{a^n-1}(a) = x \iff a^x - 1 \equiv 0 \pmod{a^n - 1}$$

For $1 \le x < n$ we have $a^x - 1 < a^n - 1$ therefore $a^x - 1 \equiv 0 \pmod{a^n - 1}$ is impossible. For $x = n$ we have $a^n - 1 \equiv 0 \pmod{a^n - 1}$. Therefore $\text{ord}_{a^n-1}(a) = \boxed{n}$. □

Example 2.5.2 (AIME 2001)**.** *How many positive integer multiples of 1001 can be expressed in the form $10^j - 10^i$, where i and j are integers and $0 \le i < j \le 99$?*

Solution. We must have

$$\begin{aligned} 1001 &\mid 10^i \left(10^{j-i} - 1\right) \\ \implies 1001 &\mid 10^{j-i} - 1 \end{aligned}$$

Notice that $\text{ord}_{1001}(10) = 6$ since $10^3 \equiv -1 \pmod{1001}$ and $10^1, 10^2, 10^4, 10^5 \not\equiv 1 \pmod{1001}$. By theorem 8 we must now have $6 \mid j - i$.

We now relate this problem into a counting problem. In the case that $j \equiv i \equiv 0 \pmod 6$ there are 17 values between 0 and 99 inclusive that satisfy this. We notice that if we choice two different values out of these 17 values, then one must be j and the other must be i since $i < j$. Therefore there are $\binom{17}{2}$ solutions in this case.

Simiarly, when $j \equiv i \equiv 1 \pmod 6, j \equiv i \equiv 2 \pmod 6, j \equiv i \equiv 3 \pmod 6$ we get $\binom{17}{2}$ solutions. When $j \equiv i \equiv 4 \pmod 6$ and $j \equiv i \equiv 5 \pmod 6$ we get only 16 values between 0 and 99 henceforth we get $\binom{16}{2}$ solutions.

Our answer is $4\binom{17}{2} + 2\binom{16}{2} = \boxed{784}$. □

Example 2.5.3. *Prove that if p is prime, then every prime divisor of $2^p - 1$ is greater than p.*

Solution. Let q be a prime divisor of $2^p - 1$. Therefore we have $\text{ord}_q(2) \mid p$ by Theorem 8. Since p is prime we have

$$\text{ord}_q(2) \in \{1, p\}$$

However, $\text{ord}_q(2) = 1$ implies that $2 \equiv 1 \pmod{q}$ absurd. Therefore $\text{ord}_q(2) = p$.

We also have

$$\text{ord}_q(2) \mid \phi(q) \implies p \mid q - 1$$

Therefore $q \geq p + 1$ and hence $q > p$ and we are done. □

Example 2.5.4. *Let p be an odd prime, and let q and r be primes such that p divides $q^r + 1$. Prove that either $2r \mid p - 1$ or $p \mid q^2 - 1$.*

Solution. Because p is odd and $p \mid q^r + 1$ we have $p \nmid q^r - 1$. Also we have $p \mid q^{2r} - 1$. Henceforth by Theorem 8

$$\text{ord}_p(q) \mid 2r$$

However since $\text{ord}_p(q) \neq r$ we have $\text{ord}_p(q) \in \{1, 2, 2r\}$.

When $\text{ord}_p(q) = 2r$ we have $\text{ord}_p(q) \mid \phi(p) = p - 1$ we have $2r \mid p - 1$.

When $\text{ord}_p(q) \in \{1, 2\}$ in the first case we get $p \mid q - 1$ and in the second we get $p \mid q^2 - 1$. In conclusion we get $p \mid q^2 - 1$.

Therefore $2r \mid p - 1$ *or* $p \mid q^2 - 1$ □

Example 2.5.5. *Let $a > 1$ and n be given positive integers. If p is an odd prime divisor of $a^{2^n} + 1$, prove that $p - 1$ is divisible by 2^{n+1}.*

Solution. Since p is odd we have $p \nmid a^{2^n} - 1$. We also have $p \mid \left(a^{2^n} - 1\right)\left(a^{2^n} + 1\right) = a^{2^{n+1}} - 1$. Therefore

$$\text{ord}_p(a) \mid 2^{n+1}$$

However $\text{ord}_p(a) \nmid 2^n$ (since if it did then we would have $p \mid a^{2^n} - 1$) hence

$$\text{ord}_p(a) = 2^{n+1}$$

We know that $\text{ord}_p(a) \mid p - 1$ hence $2^{n+1} \mid p - 1$. □

Example 2.5.6 (Classical)**.** *Let n be an integer with $n \geq 2$. Prove that n doesn't divide $2^n - 1$.*

Solution. Let p be the smallest prime divisor of n. We have

$$p \mid n \mid 2^n - 1$$

By theorem 8 it follows that $\text{ord}_p(2) \mid n$. However notice that $\text{ord}_p(2) \leq \phi(p) < p$ contradicting p being the smallest prime divisor of n. □

Example 2.5.7. *Prove that for all positive integers $a > 1$ and n we have $n \mid \phi(a^n - 1)$.*

Solution. Since $\gcd(a^n - 1, a) = 1$ we consider $\text{ord}_{a^n-1}(a)$. From above, we have $\text{ord}_{a^n-1}(a) = n$

Now by theorem 8 we have $\text{ord}_{a^n-1}(a) \mid \phi(a^n - 1)$ hence $n \mid \phi(a^n - 1)$ as desired. □

Motivation. The motivation to work mod $a^n - 1$ stems from the fact that we want a value to divide $\phi(a^n - 1)$ so hence we will likely use order mod $a^n - 1$. After a bit of thought we think to look at $\text{ord}_a(a^n - 1)$. □

Example 2.5.8. *If a and b are positive integers relatively prime to m with $a^x \equiv b^x \pmod{m}$ and $a^y \equiv b^y \pmod{m}$ prove that*

$$a^{\gcd(x,y)} \equiv b^{\gcd(x,y)} \pmod{m}.$$

Solution. We have that

$$\begin{aligned} a^x &\equiv b^x \pmod{m} \\ b^x \left[\left(a \cdot b^{-1}\right)^x - 1\right] &\equiv 0 \pmod{m} \\ \left(a \cdot b^{-1}\right)^x &\equiv 1 \pmod{m} \end{aligned}$$

Set $z \equiv a \cdot b^{-1} \pmod{m}$. From $z^x \equiv 1 \pmod{m}$ we have $\operatorname{ord}_m(z) \mid x$. Simiarly we have $\operatorname{ord}_m(z) \mid y$ therefore

$$\operatorname{ord}_m(z) \mid \gcd(x, y)$$

From this we arrive at

$$\begin{aligned} z^{\gcd(x,y)} &\equiv 1 \pmod{m} \\ \left(a \cdot b^{-1}\right)^{\gcd(x,y)} &\equiv 1 \pmod{m} \\ a^{\gcd(x,y)} &\equiv b^{\gcd(x,y)} \pmod{m} \end{aligned}$$

□

Example 2.5.9. *Let a and b be relatively prime integers. Prove that any odd divisor of $a^{2^n} + b^{2^n}$ is of the form $2^{n+1}m + 1$.*

Solution. It suffices to prove that all prime divisors of $a^{2^n} + b^{2^n}$ are $1 \pmod{2^{n+1}}$. If we could do this, by multiplying the prime divisors together we get that all divisors are of the form $1 \pmod{2^{n+1}}$. We let q be an odd divisor of $a^{2^n} + b^{2^n}$. Since $\gcd(a, b) = 1$ it follows that $\gcd(q, a) = 1$ and $\gcd(q, b) = 1$.

$$\begin{aligned} q &\mid a^{2^n} + b^{2^n} \\ q &\mid a^{2^n}\left[1 + \left(b \cdot a^{-1}\right)^{2^n}\right] \\ q &\mid \left(b \cdot a^{-1}\right)^{2^n} + 1 \\ q &\mid \left(b \cdot a^{-1}\right)^{2^{n+1}} - 1 \end{aligned}$$

Let $z \equiv b \cdot a^{-1} \pmod{q}$. Therefore $\operatorname{ord}_q(z) \mid 2^{n+1}$. However since q is odd we have $q \nmid z^{2^n} - 1$ therefore

$$\operatorname{ord}_q(z) = 2^{n+1} \mid q - 1$$

□

Example 2.5.10 (Bulgaria 1996)**.** *Find all pairs of prime p, q such that $pq \mid (5^p - 2^p)(5^q - 2^q)$.*

Solution. We must either have $p \mid 5^p - 2^p$ or $p \mid 5^q - 2^q$. Assume $p \mid 5^p - 2^p$. By Fermat's Little Theorem we arrive at

$$5^p - 2^p \equiv 3 \equiv 0 \pmod{p} \implies p = 3$$

We must either have $q \mid (5^3 - 2^3) = 117$ or $q \mid (5^q - 2^q)$. By the same method, the second one produces $q = 3$ while the first renders $q = 13$. Using symettry we arrive at the solutions $(p, q) = (3, 3), (3, 13), (13, 3)$. Assume that $p, q \neq 3$ now.

We must have $p \mid 5^q - 2^q$ and $q \mid 5^p - 2^p$ then.

$$\begin{aligned} 5^q - 2^q &\equiv 0 \pmod{p} \\ 2^q \left[\left(5 \cdot 2^{-1}\right)^q - 1\right] &\equiv 0 \pmod{p} \\ \left(5 \cdot 2^{-1}\right)^q - 1 &\equiv 0 \pmod{p} \end{aligned}$$

Using this same logic we arrive at

$$\left(5 \cdot 2^{-1}\right)^p - 1 \equiv 0 \pmod{q}$$

Let $a \equiv 5 \cdot 2^{-1} \pmod{pq}$. We therefore have

$$\begin{cases} \text{ord}_p(a) \mid q \\ \text{ord}_q(a) \mid p \end{cases} \implies \begin{cases} \text{ord}_p(a) \in \{1, q\} \mid \phi(p) \\ \text{ord}_q(a) \in \{1, p\} \mid \phi(q) \end{cases}$$

If $\text{ord}_p(a) = q$ and $\text{ord}_q(a) = p$ then by Theorem 8 we would have

$$\begin{cases} q \mid p - 1 \\ p \mid q - 1 \end{cases} \implies \begin{cases} p \geq q + 1 \\ q \geq p + 1 \end{cases}$$

absurd. Therefore assume WLOG that $\text{ord}_p(a) = 1$ therefore $a - 1 \equiv 0 \pmod{p}$. Since $a \equiv 5 \cdot 2^{-1} \pmod{p}$ we have

$$2(a - 1) \equiv (2)(5)\left(2^{-1}\right) - 2 \equiv 3 \equiv 0 \pmod{p}$$

contradicting $p, q \neq 3$.

The solutions are hence $(p, q) = \boxed{(3, 3), (3, 13), (13, 3)}$. □

Example 2.5.11 (USA TST 2003)**.** *Find all ordered prime triples (p, q, r) such that $p \mid q^r + 1$, $q \mid r^p + 1$, and $r \mid p^q + 1$.*

Solution. We split this up into two cases.

Case 1: Assume that $p, q, r \neq 2$. We therefore have $p \nmid q^r - 1$ and similarly. Therefore we have

$$\begin{cases} p \mid q^{2r} - 1 \\ q \mid r^{2p} - 1 \\ r \mid p^{2q} - 1 \end{cases} \implies \begin{cases} \operatorname{ord}_p(q) \in \{1, 2, 2r\} \mid p - 1 \\ \operatorname{ord}_q(r) \in \{1, 2, 2p\} \mid q - 1 \\ \operatorname{ord}_r(p) \in \{1, 2, 2q\} \mid r - 1 \end{cases}$$

because $\operatorname{ord}_p(q) \mid 2r$ and $\operatorname{ord}_p(q) \neq r$ and similarly.

Assume that $\operatorname{ord}_p(q), \operatorname{ord}_q(r), \operatorname{ord}_r(p) \in \{1, 2\}$. $\operatorname{ord}_p(q) = 1$ implies $q \equiv 1 \pmod{p}$ and $\operatorname{ord}_p(q) = 2$ implies $q^2 \equiv 1 \pmod{p} \implies q \equiv -1 \pmod{p}$. Therefore we arrive at

$$\begin{cases} q \equiv \pm 1 \pmod{p} \\ r \equiv \pm 1 \pmod{q} \\ p \equiv \pm 1 \pmod{r} \end{cases} \implies \begin{cases} q \pm 1 \geq 2p \\ r \pm 1 \geq 2q \\ p \pm 1 \geq 2r \end{cases}$$

since $q \pm 1 \neq p$ from them all being odd. This inequality set is clearly impossible.

Therefore WLOG we set $\operatorname{ord}_p(q) = 2r$. We must have $2r \mid p - 1$ (Theorem 8) but since p and r are odd this reduces down to $r \mid p - 1$. However $r \mid p^q + 1$ but $p^q + 1 \equiv 2 \neq 0 \pmod{r}$ contradiction.

Case 2: We conclude there are no solutions when $p, q, r \neq 2$. Therefore WLOG let $p = 2$. From $p \mid q^r + 1$ we arrive at $q \equiv 1 \pmod{2}$. Also r is odd since $r \mid 2^q + 1$. Therefore we have $r \nmid 2p^q - 1$ and $q \nmid r^2 - 1$.

$$\begin{cases} q \mid r^4 - 1 \\ r \mid 2^{2q} - 1 \end{cases} \implies \begin{cases} \operatorname{ord}_q(r) \in \{1, 4\} \mid q - 1 \\ \operatorname{ord}_r(2) \in \{1, 2, 2q\} \mid r - 1 \end{cases}$$

If $\operatorname{ord}_r(2) = 1$ then we have $2 \equiv 1 \pmod{r}$ absurd. If $\operatorname{ord}_r(2) = 2$ then we have $2^2 \equiv 1 \pmod{r}$ or $r = 3$. We must have $q \mid 3^4 - 1 = 80$. Since $q \neq 2$, we check if $q = 5$ satisfies the equation. $(p, q, r) = (2, 5, 3)$ gives us $2 \mid 5^3 + 1, 5 \mid 3^2 + 1, 3 \mid 2^5 + 1$ which are all true. We arrive at the solutions $(p, q, r) = (2, 5, 3), (3, 2, 5), (5, 3, 2)$.

Now we must have $\operatorname{ord}_r(2) = 2q$. By theorem 8 we have $2q \mid r - 1$. Therefore since $q \neq 2$ we have $r \equiv 1 \pmod{q}$. However $q \mid r^p + 1$ but $r^p + 1 \equiv 2 \neq 0 \pmod{q}$.

In conclusion our solutions are $(p, q, r) = \boxed{(2, 5, 3), (3, 2, 5), (5, 3, 2)}$. □

Example 2.5.12. *Prove that for $n > 1$ we have $n \nmid 2^{n-1} + 1$.*

Proof. Let $p \mid n$. We arrive at

$$\begin{cases} p \mid 2^{p-1} - 1 \\ p \mid 2^{2n-2} - 1 \end{cases} \implies p \mid 2^{\gcd(p-1, 2n-2)} - 1$$

We must have $v_2(p-1) \geq v_2(2n-2)$ since $n \mid 2^{n-1} + 1$ and $p \neq 2$.. Let $n - 1 = 2^{v_2(n-1)}m$. We arrive at

$$p - 1 \equiv 0 \pmod{2^{v_2(n-1)+1}} \implies n \equiv \prod p \equiv 1 \pmod{2^{v_2(n-1)+1}}$$

However this implies $v_2(n-1) \geq v_2(n-1) + 1$ clearly absurd. □

Example 2.5.13. *(China 2009) Find all pairs of primes p, q such that*

$$pq \mid 5^p + 5^q$$

.

Solution. We divide this solution into two main cases.

Case 1: $p = q$

In this case we must have

$$p^2 \mid 2 \cdot 5^p \implies p = q = 5$$

Case 2: $p \neq q$. When $q = 5$ we arrive at $p \mid 5^p + 5^5$ or therefore

$$5^p + 5^5 \equiv 5 + 5^5 \equiv 0 \pmod{p} \implies p = 2, 5, 313$$

Hence we arrive at $(p, q) = (5, 2), (5, 313), (2, 5), (313, 5)$. Assume $p, q \neq 5$. We now have

$$\begin{aligned} 5^p + 5^q \equiv 5 + 5^q \equiv 0 \pmod{p} \implies 5^{q-1} + 1 \equiv 0 &\pmod{p} \\ 1 + 5^{p-1} \equiv 0 &\pmod{q} \\ \implies 5^{2q-2} \equiv 1 \pmod{p} \text{ and } 5^{2p-2} \equiv 1 &\pmod{q} \\ \implies \operatorname{ord}_p(5) \mid \gcd(2q-2, p-1) \text{ and } \operatorname{ord}_q(5) \mid \gcd(2p-2, q-1)& \end{aligned}$$

So long as $p, q \neq 2$ we arrive at

$v_2\left(\text{ord}_p 5\right) = v_2(2q-2) \le v_2(p-1)$ and $v_2\left(\text{ord}_q 5\right) = v_2(2p-2) \le v_2(q-1)$

Since $5^{q-1} \not\equiv 1 \pmod{p}$ and $5^{p-1} \not\equiv 1 \pmod{q}$. The two equations above are clearly a contradiction. Therefore p or q is 2. Let $p = 2$ for convenience. We then must have

$$5^2 + 5^q \equiv 5^2 + 5 \equiv 0 \pmod{q} \implies q = 2, 3, 5$$

We however know that $p \neq q$ therefore we rule out that solution. The solutions are hence $(p, q) = (2, 3), (2, 5), (3, 2), (5, 2)$.

In conclusion the solutions are

$$(p, q) = \boxed{(2, 3), (2, 5), (3, 2), (5, 2), (5, 5), (5, 313), (313, 5)}.$$

$\square$

3

p-adic Valuation

3.1 Definition and Basic Theorems

Important: *Unless otherwise stated p is assumed to be a prime.*

Definition 3.1.1. We define the **p-adic valuation** of m to be the highest power of p that divides m. The notation for this is $v_p(m)$.

Example. Since $20 = 2^2 \cdot 5$ we have $v_2(20) = 2$ and $v_5(20) = 1$. Since $360 = 2^3 \cdot 3^2 \cdot 5^1$ we have $v_2(120) = 3, v_3(360) = 2, v_5(360) = 1$. m can be a fraction, in this case we have $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.

Theorem 3.1.1. *$v_p(ab) = v_p(a) + v_p(b)$.*

Proof. Set $v_p(a) = e_1$ and $v_p(b) = e_2$. Therefore $a = p^{e_1}a_1$ and $b = p^{e_2}b_1$ where a_1 and b_1 are relatively prime to p. We then get

$$ab = p^{e_1+e_2}a_1b_1 \implies v_p(ab) = e_1 + e_2 = v_p(a) + v_p(b)$$

□

Theorem 3.1.2. *If $v_p(a) > v_p(b)$ then $v_p(a+b) = v_p(b)$.*

Proof. Again write $v_p(a) = e_1$ and $v_p(b) = e_2$. We therefore have $a = p^{e_1}a_1$ and $b = p^{e_2}b_1$. Notice that

$$a + b = p^{e_1}a_1 + p^{e_2}b_1 = (p^{e_2})\left(p^{e_1-e_2}a_1 + b_2\right)$$

Since $e_1 \geq e_2 + 1$ we have $p^{e_1 - e_2} a_1 + b_2 \equiv b_2 \neq 0 \pmod{p}$ therefore $v_p(a+b) = e_2 = b$ as desired. □

At this point the reader is likely pondering "these seem interesting but I do not see use for them". Hopefully the next example proves otherwise (we've split it into two parts).

Example 3.1.1. *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 $v_2\left(\sum_{i=1}^{n} \frac{n!}{i}\right)$. From 3.1.2 we get

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

We then get $v_2\left(\frac{n!}{4i-2} + \frac{n!}{4i}\right) = v_2\left(\frac{n!}{4i}\right)$ 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 $\sum_{i=1}^{n} \left(\frac{1}{i}\right)$ to be an integer we need

$$v_2\left(\sum_{i=1}^{n} \frac{n!}{i}\right) \geq v_2(n!)$$
$$v_2\left(\frac{n!}{2^{\lfloor \log_2 n \rfloor}}\right) \geq v_2(n!)$$
$$0 \geq \lfloor \log_2 n \rfloor,$$

which is a contradiction since $n \geq 2$. □

Example 3.1.2. *Prove that* $\displaystyle\sum_{i=0}^{n} \frac{1}{2i+1}$ *is not an integer for* $n \geq 1$.

Solution.

Definition 3.1.2. We define $(2i+1)!!$ to be the product of all odd numbers less than or equal to $2i+1$. Therefore $(2i+1)!! = (2i+1)(2i-1)\cdots 3 \cdot 1$. For example $(5)!! = 5 \cdot 3 \cdot 1 = 15$.

Similarly to what was done in the previous problem, we can rewrite the summation as

$$\sum_{i=0}^{n} \frac{1}{2i+1} = \sum_{i=0}^{n} \frac{\frac{(2n+1)!!}{2i+1}}{(2n+1)!!}.$$

Notice that

$$v_3\left(\frac{(2n+1)!!}{3i-2} + \frac{(2n+1)!!}{3i} + \frac{(2n+1)!!}{3i+2}\right) = v_3\left(\frac{(2n+1)!!}{3i}\right).$$

Since $v_3\left(\frac{(2n+1)!!}{3i-2} + \frac{(2n+1)!!}{3i+2}\right) > v_3\left(\frac{(2n+1)!!}{3i}\right)$. Repeating to sum all terms up in groups of three as this, we arrive at

$$v_3\left(\sum_{i=0}^{n} \frac{(2n+1)!!}{2i+1}\right) \geq v_3\left(\frac{(2n+1)!!}{3^{\lfloor \log_3(2n+1) \rfloor}}\right).$$

However we must have

$$\begin{aligned} v_3\left(\frac{(2n+1)!!}{3^{\lfloor \log_3(2n+1) \rfloor}}\right) &\geq v_3\left[(2n+1)!!\right] \\ 0 &\geq \lfloor \log_3(2n+1) \rfloor \end{aligned}$$

which is a contradiction since $n \geq 1$.

□

Example 3.1.3 (ISL 2007 N2)**.** *Let* $b, n > 1$ *be integers. For all* $k > 1$*, there exists an integer* a_k *so that* $k \mid (b - a_k^n)$*. Prove that* $b = m^n$ *for some integer* m*.*

Solution. Assume to the contrary and that there exists a prime p that divides into b such that $v_p(b) \not\equiv 0 \pmod{n}$. Therefore we set

$$b = p^{e_1 n + f_1} b_1, \qquad 1 \le f_1 \le n - 1$$

where $\gcd(b_1, p) = 1$ and p is a prime. Now let $k = p^{n(e_1+1)}$. We must have $v_p(b - a_k^n) \ge v_p(k) = n(e_1 + 1)$.

- If $v_p(a_k) \le e_1$ then we have

  $$v_p(b) > v_p(a_k^n) \implies v_p(b - a_k^n) = v_p(a_k^n) \le ne_1$$

  contradiction!

- If $v_p(a_k) \ge e_1 + 1$ then we have

  $$v_p(a_k^n) > v_p(b) \implies v_p(b - a_k^n) = v_p(b) < n(e_1 + 1)$$

  contradiction!

Both cases lead to a contradiction, therefore $f_1 \equiv 0 \pmod{n}$ and we have $b = m^n$. □

3.2 p-adic Valuation of Factorials

Factorials are special cases that really lend themselves to p-adic valuations, as the following examples show.

Example. Find $v_3(17!)$.

Solution. We consider the set $\{1, 2, \cdots, 17\}$. We count 1 power of 3 for each element with $v_p(x) = 1$ and we count two powers of 3 for each element with $v_p(x) = 2$.

- We begin by counting how many numbers have at least one power of 3 which is simply $\lfloor \frac{17}{3} \rfloor$.
- We have already accounted for the numbers with two powers of 3, however they must be counted twice so we add $\lfloor \frac{17}{9} \rfloor$ to account for them the second time.

Our answer is hence $\lfloor \frac{17}{3} \rfloor + \lfloor \frac{17}{9} \rfloor = \boxed{6}$. □

Theorem 3.2.1 (Legendre). *For all positive integers n and positive primes p, we have*

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

Outline. We consider the power of p that divides into $n!$.

- The number of occurences that the factor p^1 occurs in the set $\{1, 2, \cdots, n\}$. We notice that it occurs $\lfloor \frac{n}{p} \rfloor$ times.
- The number of occurences that the factor p^2 occur in the set $\{1, 2, \cdots, n\}$ is going to be $\lfloor \frac{n}{p^2} \rfloor$. We have added these once already when we added $\lfloor \frac{n}{p} \rfloor$, but since we need this to be added 2 times (since it is p^2), we add $\lfloor \frac{n}{p^2} \rfloor$ once.

Repeating this process as many times as necessary gives the desired $v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$. □

Theorem 3.2.2 (Legendre). *For all positive integers n and positive primes p, we have*

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

where $s_p(n)$ denotes the sum of the digits of n in base p.

Proof. In base n write

$$n = \sum_{i=0}^{k} \left(a_i \cdot p^i\right) \quad p-1 \geq a_k \geq 1 \text{ and } p-1 \geq a_i \geq 0 \text{ for } 0 \leq i \leq k-1$$

From 3.2.1 we arrive at

$$\begin{aligned} v_p(n!) &= \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{j=1}^{k} a_j \left(p^{j-1} + p^{j-2} + \cdots + 1\right) \\ &= \sum_{j=1}^{k} a_j \left(\frac{p^j - 1}{p-1}\right) \end{aligned}$$

where our steps were motivated by examining $\sum_{i=1}^{\infty}\left\lfloor \frac{a_j p^j}{p^i} \right\rfloor$.[1]

Now we evaluate $\frac{n-s_p(n)}{p-1}$. We notice that $s_p(n)=\sum_{i=0}^{k} a_i$, which implies that

$$\begin{aligned}\frac{n-s_p(n)}{p-1} &= \frac{1}{p-1}\left[\sum_{i=0}^{k}\left(a_i\cdot p^i\right)-\sum_{i=0}^{k}\left(a_i\right)\right]\\ &= \frac{1}{p-1}\sum_{i=0}^{k}\left[a_i\left(p^i-1\right)\right].\end{aligned}$$

Therefore $v_p\left(n!\right)=\frac{n-s_p(n)}{p-1}$ as desired. □

Example 3.2.1 (Canada)**.** *Find all positive integers n such that $2^{n-1} \mid n!$.*

Solution. From 3.2.2 we have

$$v_2\left(n!\right)=n-s_2\left(n\right)\geq n-1 \implies 1\geq s_2\left(n\right)$$

This happens only when n is a power of 2. □

Example 3.2.2. *Find all positive integers n such that $n \mid (n-1)!$.*

Solution. Set $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ be the prime factorization of n. If $k\geq 2$ then write $n=(p_1^{e_1})\,(p_2^{e_2}\cdots p_k^{e_k})$. From Chinese Remainder Theorem we must prove that

$$(p_1^{e_1})\mid(n-1)!\text{ and }(p_2^{e_2}\cdots p_k^{e_k})\mid(n-1)!$$

However since $n-1>p_1^{e_1}$ and $n-1>p_2^{e_2}\cdots p_k^{e_k}$ this is true.

[1] To make this more rigorous we would use the double summation notation. I avoided this notation to make the proof more easier to follow.

Therefore we now consider $k = 1$ or $n = p_1^{e_1}$. Using Legendre's formula we have

$$v_{p_1}\left(p_1^{e_1} - 1\right)! = \sum_{i=1}^{\infty} \left\lfloor \frac{p_1^{e_1} - 1}{p_1^i} \right\rfloor \geq e_1.$$

For $e_1 = 1$ this statement is obviously false (which correlates to n being prime). For $e_1 = 2$ we must have

$$\left\lfloor \frac{p_1^2 - 1}{p_1} \right\rfloor \geq e_1 \implies p_1 - 1 \geq e_1$$

Therefore since $e_1 = 2$ we have $p_1 = 2$ giving the only counterexample (which correlates to $n = 4$). Now for $e_1 \geq 3$ we have

$$\sum_{i=1}^{\infty} \left\lfloor \frac{p_1^{e_1} - 1}{p_1^i} \right\rfloor \geq p_1^{e_1 - 1} - 1 \geq 2^{e_1 - 1} - 1 \geq e_1.$$

Therefore the anwer is $\boxed{\text{all composite } n \text{ not equal to } 4}$.

□

Example 3.2.3. *Prove that for any positive integer n, the quantity $\frac{1}{n+1}\binom{2n}{n}$ is an integer.* ***Do not use binomial identities.***

Solution. For $n + 1 = p$ prime the problem claim is true by looking at the sets $\{n + 1, n + 2, \cdots, 2n\}$ and $\{1, 2, \cdots, n\}$ and noticing that factors of p only occur in the first set. Otherwise let p be a prime divisor of $n + 1$ less than $n + 1$. We must prove that

$$v_p\left[\binom{2n}{n}\right] \geq v_p\left(n + 1\right)$$

Let $v_p\left(n + 1\right) = k$. Therefore write $n + 1 = p^k n_1$ where $\gcd(n_1, p) = 1$. By Legendre's we have

$$v_p\left[\binom{2n}{n}\right] = \sum_{i=1}^{\infty} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Lemma. When $n + 1 = p^k n_1$ and $k \geq m$ we have

$$\left\lfloor \frac{2n}{p^m} \right\rfloor - 2\left\lfloor \frac{n}{p^m} \right\rfloor = 1.$$

Proof. We notice that $2n = 2n_1p^k - 2$. Therefore for $p \neq 2$ we have

$$\left\lfloor \frac{2n}{p^m} \right\rfloor = 2n_1p^{k-m} - 1 \quad \text{and} \quad 2\left\lfloor \frac{n}{p^m} \right\rfloor = 2\left(p^{k-m}n_1 - 1\right)$$

For $p = 2$, we arrive at the same formula unless $m = 1$, which then gives

$$\left\lfloor \frac{2n}{2} \right\rfloor = 2^kn_1 - 1 \quad \text{and} \quad \left\lfloor \frac{n}{2} \right\rfloor = 2^{k-1}n_1 - 1.$$

The calculations in both cases are left to the reader to verify (simple exercise). □

Therefore using our lemma we have

$$v_p\left[\binom{2n}{n}\right] \geq k,$$

which is what we wanted. □

Example 3.2.4 (Putnam 2003)**.** *Show that for each positive integer n,*

$$n! = \prod_{i=1}^{n} lcm\ \left\{1, 2, \ldots, \left\lfloor \frac{n}{i} \right\rfloor\right\}$$

(Here lcm denotes the least common multiple, and $\lfloor x \rfloor$ denotes the greatest integer $\leq x$.)

Solution. If we have $v_p(a) = v_p(b)$ for all primes p then in conclusion we would have $a = b$ since the prime factorizations would be the same. Assume that for this case $p \leq n$ because otherwise it is clear that $v_p(n!) = v_p\left(\prod_{i=1}^{n} \text{lcm}\ \left\{1, 2, \ldots, \left\lfloor \frac{n}{i} \right\rfloor\right\}\right) = 0$

By theorem 7 we have $v_p(n!) = \sum_{i=1}^{\infty} \left(\frac{n}{p^i}\right)$. I claim that this is the same as

$$v_p\left(\prod_{i=1}^{n} \text{lcm}\ \left\{1, 2, \ldots, \left\lfloor \frac{n}{i} \right\rfloor\right\}\right).$$

- When $i \in \{1, 2, \cdots, \lfloor \frac{n}{p} \rfloor\}$ we have at least one power of p in lcm $\{1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\}$. Therefore we add $\lfloor \frac{n}{p} \rfloor$.
- When $i \in \{1, 2, \cdots, \lfloor \frac{n}{p^2} \rfloor\}$ we have at least two powers of p in lcm $\{1, 2, \ldots, \lfloor \frac{n}{i} \rfloor\}$. However, since we need to count the power of p^2 a total of 2 times and it has already been counted once, we just add it once.

Repeating this process we arrive at $v_p\left(\prod_{i=1}^{n} \text{lcm } \left\{1, 2, \ldots, \left\lfloor \frac{n}{i} \right\rfloor\right\}\right) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$ as desired. □

Example 3.2.5. *Prove that for all positive integers n, $n!$ divides*

$$\prod_{k=0}^{n-1}(2^n - 2^k).$$

Solution. Notice that

$$\begin{aligned}\prod_{k=0}^{n-1}(2^n - 2^k) &= \prod_{k=0}^{n-1} 2^k\left(2^{n-k} - 1\right) \\ &= 2^{1+2+\cdots+n-1}\prod_{k=1}^{n-1}(2^k - 1).\end{aligned}$$

The number of occurences of 2 in the prime factorization of $n!$ is quite obviously more in $\prod_{k=1}^{n-1}(2^n - 2^k)$ then in $n!$ using the theorem 7. Therefore we consider all odd primes p and look at how many times it divides into both expressions.

Lemma.

$$v_p\left(\prod_{k=1}^{n-1}(2^k - 1)\right) \geq \sum_{i=0}^{\infty}\left\lfloor \frac{n-1}{(p-1)p^i} \right\rfloor = \sum_{i=1}^{\infty}\left\lfloor \frac{n-1}{(p-1)p^{i-1}} \right\rfloor.$$

Outline. We consider the set $\{2^1 - 1, 2^2 - 1, \cdots, 2^{n-1} - 1\}$ and consider how many times the exponent p^i divides into each term. We consider the worst case scenario situation when the smallest value of x such that $2^x \equiv 1 \pmod{p^j}$ is $x = \phi(p^j)$ via Euler's Totient.

- When p^1 divides into members of this set, we have

  $$p|(2^k - 1) \implies k \equiv 0 \pmod{p-1}.$$

  This results in giving us a total of $\lfloor \frac{n-1}{p-1} \rfloor$ solutions.

- When p^2 divides into members of this set, we have

  $$p^2|(2^k - 1) \implies k \equiv 0 \pmod{p(p-1)}.$$

  We only account for this once using similar logic as to the proof of Legendre's theorem therefore we add this a total of $\lfloor \frac{n-1}{p(p-1)} \rfloor$ times.

Repeating this process in general gives us

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

and keeping in mind that it is a lower bound, we have proven the lemma. □

We desire to have $v_p\left(\prod_{k=1}^{n-1}(2^k - 1)\right) \geq v_p(n!)$ which would in turn give us $n!$ divides $\prod_{k=1}^{n-1}(2^k - 1)$. Quite obviously $n \geq p$ or else $v_p(n!) = 0$ and there is nothing to consider. Because of this,

$$\frac{n-1}{p-1} \geq \frac{n}{p} \implies \frac{n-1}{(p-1)p^{i-1}} \geq \frac{n}{p^i}.$$

Therefore, we arrive at

$$\sum_{i=1}^{\infty} \left\lfloor \frac{n-1}{(p-1)p^{i-1}} \right\rfloor \geq \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

As a result,

$$v_p\left[\prod_{k=1}^{n-1}(2^k - 1)\right] \geq v_p(n!)$$

and we are done. □

Motivation. The motivation behind the solution was looking at small cases. We take out the factors of 2 because we believe that there are more in the product we are interested in then in $n!$. For $n = 3$ we want $3 \mid (2^3-1)(2^2-1)(2-1)$. Obviously $3 \mid (2^2-1)$.

Similarly, for $n = 5$ we want $(5 \times 3) \mid (2^5-1)(2^4-1)(2^3-1)(2^2-1)(2^1-1)$. Notice that $5 | (2^4-1)$ and $3 | (2^2-1)$.

At this point the motivation to use Fermat's Little Theorem to find which terms are divisible by p hit me. From here, the idea to use Legendre's formula and Euler's Totient for p^k hit me and the rest was groundwork. □

3.2.1 Problems

Problem 3.2.1. (1968 IMO 6) For every natural number n, evaluate the sum

$$\sum_{k=0}^{\infty}\lfloor\frac{n+2^k}{2^{k+1}}\rfloor = \lfloor\frac{n+1}{2}\rfloor + \lfloor[\frac{n+2}{4}\rfloor] + \cdots + \lfloor[\frac{n+2^k}{2^{k+1}}\rfloor] + \cdots$$

Problem 3.2.2. (1975 USAMO 1) Prove that

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

is integral for all positive integral m and n.

3.3 Lifting the Exponent

Theorem 3.3.1. *For p being an odd prime relatively prime to integers a and b with $p \mid a-b$ then*

$$v_p\left(a^n-b^n\right) = v_p\left(a-b\right) + v_p\left(n\right).$$

Proof. ([?])

We use induction on $v_p\left(n\right)$.

Base case: We begin with the base case of $v_p\left(n\right) = 0$. We have

$$v_p\left(a^n-b^n\right) = v_p\left(a-b\right) + v_p\left(a^{n-1} + a^{n-2}\cdot b + \cdots + b^{n-1}\right)$$

Now notice that

$$a^{n-1} + a^{n-2} \cdot b + \cdots + b^{n-1} \equiv n \cdot a^{n-1} \pmod{p}$$

from $a \equiv b \pmod{p}$ therefore since $\gcd(a, p) = 1$ we have

$$v_p\left(a^n - b^n\right) = v_p\left(a - b\right)$$

as desired.

Second base case: It is not necessary to do two base cases, however it will help us down the road so we do it here. We prove that when $v_p\left(n\right) = 1$ we have $v_p\left(a^n - b^n\right) = v_p\left(n\right) + v_p\left(a - b\right)$. Let $n = pn_1$ where $\gcd(n_1, p) = 1$. We arrive at

$$v_p\left(a^{pn_1} - b^{pn_1}\right) = v_p\left[(a^p)^{n_1} - (b^p)^{n_1}\right] = v_p\left(a^p - b^p\right)$$

Now let $a = b + kp$ since we know $p \mid a - b$. We arrive at

$$(b + kp)^p - b^p = \binom{p}{1}(kp) + \binom{p}{2}(kp)^2 + \cdots + \binom{p}{p}(kp)^p$$

Using the fact that $p \mid \binom{p}{i}$ for all $1 \le i \le p - 1$ we arrive at

$$v_p\left[(b + kp)^p - b^p\right] = v_p\left(\binom{p}{1}p\right) + v_p\left(k\right) = 2 + v_p(a - b) - 1$$

as desired.

Inductive hypothesis: Assume the statement holds for $v_p\left(n\right) = k$ and I prove it holds for $v_p\left(n\right) = k + 1$. Set $n = p^{k+1}n_1$. Then we have

$$v_p\left[\left(a^{p^k}\right)^{pn_1} - \left(b^{p^k}\right)^{pn_1}\right] = v_p\left(a^{p^k} - b^{p^k}\right) + 1 = v_p\left(a - b\right) + k + 1$$

Via our second base case and inductive hypothesis. □

Corollary 3.3.1. For p being an odd prime relatively prime to a and b with $p \mid a - b$ and n is a **odd** positive integer than

$$v_p\left(a^n + b^n\right) = v_p\left(a + b\right) + v_p\left(n\right)$$

.

Theorem 3.3.2. *If $p = 2$ and n is even, and*

- $4 \mid x - y$ *then* $v_2(x^n - y^n) = v_2(x - y) + v_2(n)$
- $4 \mid x + y$ *then* $v_2(x^n - y^n) = v_2(x + y) + v_2(n)$

Proof. This is left to the reader, advising that they follow along the same lines as the above proof. □

Example 3.3.1 (AoPS). *Let $p > 2013$ be a prime. Also, let a and b be positive integers such that $p|(a+b)$ but $p^2 \nmid (a+b)$. If $p^2|(a^{2013}+b^{2013})$ then find the number of positive integer $n \leq 2013$ such that $p^n|(a^{2013} + b^{2013})$*

Solution. The first condition is equivalent to $v_p(a+b) = 1$. We also must have $v_p(a^{2013} + b^{2013}) \geq 2$. However if $p \nmid a, b$ then we have

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

Therefore $p \mid a, b$ which in turn gives $p^{2013} \mid a^{2013} + b^{2013}$. Therefore the answer is all positive integers n less than or equal to 2013 or $\boxed{2013}$. □

Example 3.3.2 (AMM). *Let a, b, c be positive integers such that $c \mid a^c - b^c$. Prove that $c \mid \frac{a^c-b^c}{a-b}$.*

Solution. Let

$$p \mid c, v_p(c) = x$$

If $p \nmid a - b$ then we obviously have

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

Therefore consider $p \mid a - b$. Using lifting the exponent so long as $p \neq 2$, we arrive at

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

When $p = 2$ we arrive at

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

□

Example 3.3.3 (IMO 1999)**.** *Find all pairs of positive integers (x, p) such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$.*

Solution. Assume that $p \neq 2$ for the time being (we will see why later). We trivially have $x = 1$ always giving a solution. Now, let q be the minimal prime divisor of x. We notice that:

$$\begin{aligned} q &\mid \left[(p-1)^2\right]^x - 1 \\ \implies \operatorname{ord}_q \left[(p-1)^2\right] &\mid \gcd(x, q-1) = 1 \\ \implies (p-1)^2 - 1 &\equiv 0 \pmod{q} \\ \implies (p-2)(p) &\equiv 0 \pmod{q} \end{aligned}$$

We know that $(p-1)^x + 1 \equiv 0 \pmod{q}$. However, if $p - 2 \equiv 0 \pmod{q}$ then we have

$$(p-1)^x + 1 \equiv 2 \neq 0 \pmod{q}$$

Since $p - 1$ is odd. Therefore we must have $p \equiv 0 \pmod{q}$ or therefore $p = q$. Now, by lifting the exponent [2] we have:

$$\begin{aligned} v_p \left[(p-1)^x + 1\right] = 1 + v_p(x) &\geq p - 1 \\ x \geq p^{p-2} &\geq 2p \text{ for } p > 3 \end{aligned}$$

However we have $x \leq 2p$. We now account for $p \in \{2, 3\}$.

$p = 2$ gives $x \mid 2$ or $x = 1, 2$. $p = 3$ gives $x^2 \mid 2^x + 1$ where $x \leq 6$. Therefore we have $x = 1, 3$. The solutions are hence $(x, p) = (1, p), (2, 2), (3, 3)$. □

Example 3.3.4 (Bulgaria)**.** *For some positive integers n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.*

Solution. Say $n = p_1 p_2 \cdots p_k$ where $p_1 \leq p_2 \leq \cdots \leq p_k$ and $k \geq 2$.

We have $3^{p_i} - 2^{p_i} \mid 3^n - 2^n$. Let $p \mid 3^{p_i} - 2^{p_i}$ for all p_i. We have $p \mid z^{p_i} - 1$ where $z \equiv 3 \cdot 2^{-1} \pmod{p}$ since $p \neq 2$. Therefore

$$\operatorname{ord}_p(z) \mid p_i \implies \operatorname{ord}_p(z) \mid \gcd(p_1, p_2, \cdots, p_i)$$

[2] lifting the exponent is not the same for $p = 2$

However $\gcd(p_1, p_2, \cdots, p_i) \in \{1, p_i\}$ with it being p_i when $p_1 = p_2 = \cdots = p_k$. But if $\gcd(p_1, p_2, \cdots, p_i) = 1$ then we have $p \mid z - 1$. However

$$2(z-1) \equiv 1 \equiv 0 \pmod{p} \rightarrow\leftarrow$$

Therefore $p_1 = p_2 = \cdots = p_k$. We must therefore consider $n = p^k$.

Let $3^{p^k} - 2^{p^k} = q^z$. Therefore $3^{p^{k-1}} - 2^{p^{k-1}} = q^{z_1}$. Therefore $\text{ord}_q(z) \mid p^{k-1}$ if $k \geq 2$. Let $\text{ord}_q(z) = p^m$. Therefore $3^{p^m} - 2^{p^m} \equiv 0 \pmod{q}$. Now we use lifting the exponent to give us

$$v_q\left[\left(3^{p^m}\right)^{p^{k-m}} - \left(2^{p^m}\right)^{p^{k-m}}\right] = v_q\left(3^{p^m} - 2^{p^m}\right) + v_q(p)$$

However if $q = p$ then we have $\text{ord}_p(z) \mid \gcd(p^k, p-1) = 1$ giving the same $p = 1$ contradiction. Therefore $v_q(p) = 0$. Hence we must have $v_q\left(3^{p^m} - 2^{p^m}\right) \geq z$. Therefore

$$3^{p^k} - 2^{p^k} > 3^{p^m} - 2^{p^m} \geq q^z$$

since $m \leq k - 1$. Therefore $k = 1$ implying that p is prime. □

Comment. When we do Zsigmondy's theorem you will notice there is a lot easier solution to this. □

Example 3.3.5 (IMO 1990). *Find all natural n such that $\frac{2^n+1}{n^2}$ is an integer.*

Solution. Trivially $n = 1$ is a solution. Now assume $n \neq 1$ and define $\pi(n)$ to be the smallest prime divisor of n. Let $\pi(n) = p \neq 2$. Then we have:

$$\begin{aligned} p \mid 2^n + 1 \mid 2^{2n} - 1 &\text{ and } p \mid 2^{p-1} - 1 \\ &\implies p \mid 2^{\gcd(2n, p-1)} - 1 \end{aligned}$$

Now if $r \neq 2 \mid n$ then we can't have $r \mid p - 1$ because then $r \leq p - 1$ contradiction. Therefore $r = 2$ and since n is odd $\gcd(2n, p-1) = 2$. Hence

$$p \mid 2^2 - 1 \implies p = 3$$

Let $v_3(n) = k$. By lifting the exponent we must have

$$v_3(2^n + 1) = 1 + k \geq v_3(n^2) = 2k \implies k = 1$$

Let $n = 3n_1$. $n_1 = 1$ is a solution ($2^3 + 1 = 3^2 = 9$). Assume $n_1 \neq 1$ and let $\pi(n_1) = q \neq 3$. By Chinese Remainder Theorem since $q \neq 3$ we have:

$$\begin{aligned} q \mid 8^{n_1} + 1 \mid 8^{2n_1} - 1 \text{ and } q \mid 8^{q-1} - 1 \\ \implies q \mid 8^{\gcd(2n_1, q-1)} - 1 = 63 \text{ so } q = 7 \end{aligned}$$

However $2^n + 1 \equiv 8^{n_1} + 1 \equiv 2 \pmod 7$ contradiction.

The solutions are henceforth $n = 1, 3$. □

Example 3.3.6 (China TST 2009). *Let $a > b > 1$ be positive integers and b be an odd number, let n be a positive integer. If $b^n \mid a^n - 1$ prove that $a^b > \frac{3^n}{n}$.*

Solution. We fix b. I claim that the problem reduces down to b prime. Assume that we have shown the problem statement for b prime (which we will do later). Now let b be composite and say $q \mid b$ where q is prime. Then we would have $q^n \mid b^n \mid a^n - 1$. However, by our assumption $q^n \mid a^n - 1$ gives us $a^q > \frac{3^n}{n}$ therefore we have $a^b > a^q > \frac{3^n}{n}$. Therefore the problem reduces down to b prime. Let $b = p$ be prime.

We have $p^n \mid a^n - 1$. Since $p \mid a^n - 1$ we have $\text{ord}_p a \mid n$. Also by Fermat's Little Theorem we have $\text{ord}_p a \mid p - 1$. Let

$$\text{ord}_p a = x \leq p - 1$$

We now have $a^x \equiv 1 \pmod p$. Therefore $x \mid n$ and set $n = xn_1$.

Now we must have $p^n \mid (a^x)^{n_1} - 1$. By lifting the exponent we have

$$v_p\left[(a^x)^{n_1} - 1\right] = v_p(a^x - 1) + v_p(n_1) \geq n$$

Lemma. $\log_p n \geq v_p(n)$

Proof. Let $n = p^r s$. Therefore $v_p(n) = r$. We also have $\log_p n = r + \log_p s \geq r$. □

Therefore we now have

$$\begin{aligned} v_p(a^x - 1) \geq n - v_p(n_1) \geq n - \log_p n_1 \\ v_p(a^x - 1) \geq \log_p \left(\frac{p^n}{n_1}\right) \\ a^b > a^x - 1 \geq p^{v_p(a^x - 1)} \geq \frac{p^n}{n_1} = \frac{x \cdot p^n}{n} \geq \frac{3^n}{n} \end{aligned}$$

We use the fact that p is odd in the last step since we have $p^n \geq 3^n$. □

3.4 General Problems for the Reader

Problem 3.4.1 (Turkey)**.** Let b_m be numbers of factors 2 of the number $m!$ (that is, $2^{b_m}|m!$ and $2^{b_m+1} \nmid m!$). Find the least m such that $m - b_m = 1990$.

4

Diophantine equations

4.1 Bounding

Example 4.1.1. *(Russia) Find all natural pairs of integers (x, y) such that $x^3 - y^3 = xy + 61$.*

Solution.

$$x^3 - y^3 = (x - y)\left(x^2 + xy + y^2\right) = xy + 61$$

Notice that $x > y$. Therefore we have to consider $x^2 + xy + y^2 \leq xy + 61$ or $x^2 + y^2 \leq 61$. Since $x > y$, we have

$$61 \geq x^2 + y^2 \geq 2y^2 \implies y \in \{1, 2, 3, 4, 5\}$$

$$\begin{cases} y = 1 & x^3 - x - 62 = 0 \\ y = 2 & x^3 - 2x - 69 \\ y = 3 & x^3 - 3x - 89 \\ y = 4 & x^3 - 4x - 125 \\ y = 5 & x^3 - 5x - 186 = 0 \end{cases}$$

Of these equations, we see the only working value for x is when $x = 6, y = 5$ so the only natural pair of solutions is $(x, y) = (6, 5)$. □

4.2 The Modular Contradiction Method

Example 4.2.1. *Find all pairs of integers (x, y) that satisfy the equation*

$$x^2 - y! = 2001.$$

Solution. We consider what happens modulo 7. When $y \geq 7$, $y! \equiv 0 \pmod{7}$, so $x^2 \equiv 2001 \equiv -1 \pmod{7}$. Therefore if an x is to satisfy this equation, $x^2 \equiv 6 \pmod{7}$. But by analyzing the table shown below, we can see that there are no solutions to that equation.

x	$x^2 \pmod{7}$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Therefore $y < 7$.

Now we must check cases. Note that the smallest perfect square greater than 2001 is $2025 = 45^2$, and this (surprisingly) gives two valid solutions: $(x, y) = (45, 4)$ and $(x, y) = (-45, 4)$. This covers all cases with $y \leq 4$. If $y = 5$, then $x^2 = 2001 + 5! = 2121$, but this equation has no integer solutions since 2121 is divisible by 3 but not 9. If $y = 6$, then $x^2 = 2001 + 6! = 2721$, which once again has no solutions for the same reasons as above. Therefore our only solutions are $(x, y) = \boxed{(45, 4), (-45, 4)}$.

□

Tip 4.2.1. When dealing with factorials, it is often advantageous to take advantage of the fact that $m! \equiv 0 \pmod{p}$ for all positive integers $m \geq p$. By finding the right mod, we can reduce the number of cases significantly.

Example 4.2.2 (USAMTS). *Prove that if m and n are natural numbers that*

$$3^m + 3^n + 1$$

cannot be a perfect square.

Solution. We look mod 8. Notice that we have

$$3^{2k} \equiv 1 \pmod 8 \text{ and } 3^{2k+1} \equiv 3 \pmod 8$$

Therefore we have $3^m \equiv \{1,3\} \pmod 8$. Henceforth the possible values of $3^m + 3^n + 1$ mod 8 are $1+1+1, 3+1+1, 3+3+1$ which gives $3, 5, 7$.

Notice that when x is even we have $x^2 \equiv 0, 4 \pmod 8$. When $x = 2k+1$ we get $x^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 8$ since $k^2 + k \equiv 0 \pmod 2$. Therefore the possible values of $x^2 \pmod 8$ are $0, 1, 4$. None of these match the values of $3^m + 3^n + 1 \pmod 8$ therefore we have a contradiction. □

Motivation. The motivation for looking mod 8 stems from trying mod 4 at first. Trying mod 4 eliminates the case m and n are both even (since then $3^m + 3^n + 1 \equiv 3 \pmod 4$) and the case when m and n are both odd (since then $3^m + 3^n + 1 \equiv 7 \equiv 3 \pmod 4$). Since we notice how close this gets us, we try mod 8. □

Example 4.2.3. *Prove that* 19^{19} *cannot be written as the sum of a perfect cube and a perfect fourth power.*

Solution. We look $\pmod{13}$. Notice that when $\gcd(x, 13) = 1$ we have

$$\left(x^3\right)^4 \equiv 1 \pmod{13}$$

hence substituting $y \equiv x^3 \pmod{13}$ we arrive at $y^4 \equiv 1 \pmod{13}$. The solutions to this equation are $y \equiv 1, 5, 8, 12 \pmod{13}$. Therefore $x^3 \equiv 0, 1, 5, 8, 12 \pmod{13}$.

Next when $\gcd(x, 13) = 1$ we have

$$\left(x^4\right)^3 \equiv 1 \pmod{13}$$

therefore substituting $x^4 \equiv y \pmod{13}$ gives us the equation $y^3 \equiv 1 \pmod{13}$. The solutions to this are $y \equiv 1, 3, 9$ henceforth $x^4 \equiv 0, 1, 3, 9 \pmod{13}$.

Lastly, notice that

$$19^{19} \equiv \left(6^{12}\right)\left(6^7\right) \equiv \left(6^2\right)^3(6) \equiv (-3)^3(6) \equiv 7 \pmod{13}$$

$x^3 \pmod{13}$	$y^4 \pmod{13}$
0	0
1	1
5	3
8	9
12	

It is clear that the sum of no two elements above will be 7 (mod 13) therefore we are done. □

Tip 4.2.2. When a problem says to prove a diophantine equation has no solutions it usually has a modular solution. Finding the right mod is quite an important trick. Find the modulo which reduces the cases to as small as possible and this will likely be the right mod to work with. If not, try many different mods and see which ones work.

Comment. In this case since when z is relatively prime to 13 we have $z^{12} \equiv 1 \pmod{13}$ and $3 \cdot 4 = 12$, we suspect mod 13 may be a good idea. If mod 13 doesn't work, try other mods that seem helpful (such as maybe mod 5 to limit the values of $y^4 \pmod{5}$). □

Example 4.2.4. *Find all solutions to the equation $x^5 = y^2 + 4$ in positive integers.*

Solution. We look $\pmod{11}$. The motivation behind this is noting that when $\gcd(x, 11) = 1$ we have $x^{10} \equiv 1 \pmod{11}$.

Notice that when $\gcd(x, 11) = 1$ we have

$$\left(x^5\right)^2 \equiv 1 \pmod{11}.$$

Therefore substituting $y \equiv x^5 \pmod{11}$ we arrive at $y^2 \equiv 1 \pmod{11}$ or $y \equiv \pm 1 \pmod{11}$ therefore $x^5 \equiv 0, 1, 10 \pmod{11}$.

The possible squares mod 11 are $0^2 \equiv 0 \pmod{11}, 1^2 \equiv 1 \pmod{11}, 2^2 \equiv 4 \pmod{11}, 3^2 \equiv 9 \pmod{11}, 4^2 \equiv 5 \pmod{11}, 5^2 \equiv 3 \pmod{11}$ since $x^2 \equiv (11 - x)^2 \pmod{11}$. Therefore $x^2 \equiv 0, 1, 3, 4, 5, 9 \pmod{11}$.

Henceforth we have:

$x^5 \pmod{11}$	$y^2 \pmod{11}$
0	0
1	1
10	3
	4
	5
	9

Therefore $x^5 - y^2 \equiv 4 \pmod{11}$ is impossible and we have concluded that there are no solutions.

□

Comment. The same trick we used last time works beautifully. □

Example 4.2.5 (USAJMO 2013)**.** *Are there integers a, b such that a^5b+3 and ab^5+3 are perfect cubes?*

Solution. The cubic residues mod 9 are $-1, 0, 1$. Therefore we think to take mod 9. Assume that we can find a, b such that a^5b+3 and ab^5+3 are perfect cubes. Therefore we must have

$$\begin{cases} a^5b+3 \equiv -1,0,1 \pmod{9} \\ ab^5+3 \equiv -1,0,1 \pmod{9} \end{cases} \Longrightarrow \begin{cases} a^5b \equiv 5,6,7 \pmod{9} \\ ab^5 \equiv 5,6,7 \pmod{9} \end{cases}$$

If $3 \mid a$ we would have $a^5b \equiv 0 \pmod{9}$ so hence $\gcd(a,3) = 1$ and similarly $\gcd(b,3) = 1$. We notice that via Euler's Totient Theorem

$$x^6 \equiv 0,1 \pmod{9}$$

Therefore we must have a^5b and ab^5 to multiply to either 0 or 1 when reduced mod 9. However, $5 \cdot 5 \equiv 7 \pmod{9}, 5 \cdot 7 \equiv 8 \pmod{9}, 7 \cdot 7 \equiv 4 \pmod{9}$ therefore we have arrived at a contradiction.

It is therefore impossibile to find a, b such that a^5b+3 and ab^5+3 are perfect cubes.

□

Motivation. The motivation behind this solution was to limit the values on the possibilities for a^5b+3 and ab^5+3 mod 9. The other key idea was that via Euler's Totient $\phi(9) = 6$ therefore $(a^5b)(ab^5) \equiv 0,1 \pmod{9}$. □

Example 4.2.6. *Find all solutions to the diophantine equation $7^x = 3^y + 4$ in positive integers (India)*

Solution.

Lemma. $\text{ord}_{3^n}(7) = 3^{n-1}$

Sketch. First off notice that $\text{ord}_{3^n}(11) = 3^i$ (prove it!) Via lifting the exponent we have

$$v_3\left(7^{3^i} - 1\right) = i + 1 \geq n$$

□

We note that $(x, y) = (1, 1)$ is a solution and there is no solution for $y = 2$. Now assume $y \geq 3$. Therefore we have

$$7^x \equiv 4 \pmod 9 \implies x \equiv 2 \pmod 3$$

I claim that $x \equiv 8 \pmod 9$. From $\text{ord}_{27}(7) = 9$ we have

$$7^x - 4 \equiv 7^{x \pmod 9} - 4 \equiv 0 \pmod{27}$$

After testing $x = 2, 5, 8$ we arrive at $x \equiv 8 \pmod 9$.

We wish to make 7^x constant mod p. Therefore we find p such that $\text{ord}_p(7) = 9$. Since $7^9 - 1 = (7^3 - 1)(7^6 + 7^3 + 1)$ and $7^6 + 7^3 + 1 = 3 \cdot 37 \cdot 1063$ we take $p = 37$. Since $37 \nmid 7^3 - 1$ we have $\text{ord}_{37}(7) = 9$.

Take the original equation mod 7 and use $\text{ord}_7(3) = 6$ to give $y \equiv 1 \pmod 6$. Therefore y is odd so we write $y = 2m + 1$ to give us $3^y = 3^{2m+1} = 3 \cdot 9^m$. Now $\text{ord}_{37}(9) = 9$ so hence $9^m \equiv 9^{m \pmod 9} \pmod{37}$.

We have $3^y \equiv 7^x - 4 \equiv 7^7 - 4 \equiv 12 \pmod{37}$

$m \pmod 9$	$3^{2m+1} \pmod{37}$
0	3
1	27
2	21
3	4
4	36
5	28
6	30
7	11
8	25

Contradicting $3^y = 3^{2m+1} \equiv 12 \pmod{37}$.

Therefore the only solution is $(x, y) = (1, 1)$. □

Example 4.2.7. *Solve the diophantine equation in positive integers:* $2^x + 3 = 11^y$

Solution.

Lemma. $\text{ord}_{2^n} 11 = 2^{n-2}$

Sketch. We must have $\text{ord}_{2^n} 11 \mid 2^{n-1}$. From lifting the exponent $v_2\left(11^{2^i} - 1\right) = i + 2$ Therefore we must have $i + 2 \geq n \implies i \geq n - 2$. □

$(x, y) = (3, 1)$ is a solution to this equation and $x = 4$ isn't. Assume $x \geq 5$ now. Take the original equation mod 16 to give us

$$11^y \equiv 3 \pmod{16}$$
$$11^y \equiv 11^3 \pmod{16}$$
$$\implies y \equiv 3 \pmod 4$$

using the lemma.

Therefore

$$11^y - 3 \equiv 11^{y \pmod 8} - 3 \equiv 0 \pmod{32}$$

From which $y \equiv 7 \pmod 8$

We take $p = 2^4 + 1 = 17$ since $\text{ord}_{17}(2) = 8$.

We also have $\text{ord}_{17}(11) = 16$. Take the equation mod 11 to give $x \equiv 3 \pmod{10} \implies x \equiv 1 \pmod 2$. [1] Notice that $11^y \equiv 11^7, 11^{15} \equiv 3, 14 \pmod{17}$. Also

$x \pmod 8$	$2^x + 3 \pmod{17}$
1	5
3	11
5	1
7	12

Contradicting $2^x + 3 \equiv 11^y \pmod{17}$. Therefore the only solution is $(x, y) = (3, 1)$.

□

[1] from $\text{ord}_{11}(2) = 10$

Example 4.2.8 (USAMO 2005)**.** *Prove that the system*

$$x^6 + x^3 + x^3y + y = 147^{157}$$
$$x^3 + x^3y + y^2 + y + z^9 = 157^{147}$$

has no solutions in integers x, y, and z.

Solution. ([16])

We wish to limit the possibilities for z^9; therefore we choose to look at the equation (mod 19). Notice that $147 \equiv 14 \pmod{19}$ and $157 \equiv 5 \pmod{19}$. By Fermat's Little Theorem we have

$$147^{157} \equiv 14^{157} \equiv 14^{13} \equiv 2 \quad (\text{mod } 19)^2$$
$$157^{147} \equiv 5^{147} \equiv 5^3 \equiv 11 \pmod{19}$$

Adding the two equations results in

$$\left[x^3\left(x^3+y+1\right)+y\right] + \left[y\left(x^3+y+1\right)+x^3+z^9\right] \equiv [9]+[4] \pmod{19}$$
$$\implies \left(x^3+y+1\right)\left(x^3+y\right) + \left(x^3+y+1\right) - 1 + z^9 \equiv 13 \pmod{19}$$
$$\implies \left(x^3+y+1\right)^2 + z^9 \equiv 14 \pmod{19}$$

When $\gcd(z, 19) = 1$ we have $\left(z^9\right)^2 \equiv 1 \pmod{19} \implies z^9 \equiv \pm 1 \pmod{19}$. Therefore $z^9 \equiv -1, 0, 1 \pmod{19}$ or henceforth

$$(x^3+y+1)^2 \equiv 13, 14, 15 \pmod{19}$$

By work of calculations we find that the quadratic residues mod 19 are $\{0, 1, 4, 5, 6, 7, 9, 11, 16, 17\}$ therefore we have arrived at a contradiction. □

Motivation. There isn't much motivation behind this solution. The one thing we have to notice is that z^9 is a floater and hence we likely want to limit the possibilities for it. To do so we take mod 19. □

4.3 General Problems for the Reader

Problem 4.3.1 (Hong Kong TST 2002)**.** Prove that if a, b, c, d are integers such that

$$(3a + 5b)(7b + 11c)(13c + 17d)(19d + 23a) = 2001^{2001}$$

then a is even.

5

Problem Solving Strategies

In this chapter, we explore three famous theorems in Number Theory, and end with some extremely challenging problems that highlight select problem solving techniques.

5.1 Chicken Mcnuggets anyone?

Mcdonalds once offered Chicken Mcnuggets in sets of 9 and 20 only. A question prompted from this is, assuming you only buy sets of 9 and 20 Chicken Mcnuggets and do not eat/add any during this process, what is the largest amount of Mcnuggets that is impossible to make? It turns out the answer is 151, which we will explore in this section.

Theorem 5.1.1 (Chicken Mcnugget Theorem)**.** *Prove that for relatively prime naturals m, n, the largest impossible sum of m, n (i.e. largest number not expressable in the form $mx + ny$ for x, y non-negative integers) is $mn - m - n$.*

Proof. (Experimenting)

First off, let's try a small case. Let $m = 7$ and $n = 5$. We then have to show that $5 \times 7 - 5 - 7 = 23$ is impossible to make, and every value above 23 is makable. Assume for sake of contradiction that $23 = 7x + 5y$. We then arrive at $x \in \{0, 1, 2, 3\}$ since when $x \geq 4$ this implies that $y < 0$.

$$\begin{cases} x = 0, 5y = 23 \\ x = 1, 5y = 16 \\ x = 2, 5y = 9 \\ x = 3, 5y = 2 \end{cases}$$

All of these result in contradictions. Next, notice that

$$\begin{cases} 24 = 5 \times 2 + 7 \times 2 \\ 25 = 5 \times 5 \\ 26 = 5 \times 1 + 7 \times 3 \\ 27 = 5 \times 4 + 7 \times 1 \\ 28 = 7 \times 4 \\ 29 = 5 \times 3 + 7 \times 2 \\ 30 = 5 \times 6 \\ 31 = 5 \times 2 + 7 \times 3 \\ 32 = 5 \times 5 + 7 \times 1 \\ \cdots \end{cases}$$

We notice that 29 and 24 are exactly the same, except for that the factor of 5 is increased by 1 in 29. Similarly, the same holds for 25 to 30, and 26 to 31, and so forth. In fact, once we have $24, 25, 26, 27, 28$, the rest of the numbers above 23 are makable by just repeatedly adding 5.

OBSERVATIONS:

- WLOG let $n \geq m$. Then, if we can show that $mn-m-n$ is unmakable and $mn - m - n + 1, mn - m - n + 2, \cdots, mn - m - n + m$, are all makable, we can just add m repeatedly to make all numbers above $mn - m - n$.
- There seems to be an inequality related with $mn - m - n$.

Let's take a look at our equation above to show that $mn - m - n$ is unmakable. We arrive at $23 = 7x + 5y$. We think to check both mod 5 and mod 7 to see if this gives us anything. Mod 5 gives us

$$7x \equiv 23 \pmod 5 \implies 2x \equiv 3 \pmod 5 \implies x \equiv -1 \pmod 5$$

Therefore, we arrive at $x \geq 4$, contradicting $x \in \{0, 1, 2, 3\}$. Taking mod 7 gives us

$$5y \equiv 23 \equiv -5 \pmod 7 \implies y \equiv -1 \pmod 7$$

Therefore, we get $y \geq 6$ again contradiction. Both of these methods give one of the variables equal to -1 mod m or mod n. This gives us the inspiration to try this for the general equation.

Set

$$mx + ny = mn - m - n.$$

Taking mod m of this equation results in $ny \equiv -n \pmod m$. Now, since $\gcd(n, m) = 1$, we must have $y \equiv -1 \pmod m$. Now, we try $y = m - 1$ to see what happens. This gives us

$$mx + n(m-1) = mn - m - n \implies mx = -m$$

Contradicting x, y non-negative. Obviously, for y more than $m - 1$ the left hand side is way bigger than the right hand side, so we have now proven that $mn - m - n$ is impossible.

Let's try to construct how would we find x, y such that $24 = 7x + 5y$. Notice that taking this equation mod 7, we arrive at

$$5y \equiv 3 \pmod 7 \implies y \equiv 2 \pmod 7$$

Therefore, set $y = 2$ and we arrive at $x = 2$ as well. Let's try to find 26 such that $26 = 7x + 5y$. Taking this equation mod 7, we arrive at

$$5y \equiv 5 \pmod 7 \implies y \equiv 1 \pmod 7$$

Take $y = 1$ and we get $x = 3$. It seems like modulos could do the trick for us. Set

$$mn - m - n + k = mx + ny \tag{5.1}$$

Since $mn - m - n$ is a **symmetric polynomial** (meaning the variables are interchangable), we can assume **without loss or generality** that $n \geq m$. If instead $m \geq n$, then replace m by n to get $n \geq m$ (Sidenote: If $m \geq n$, we would have taken the original equation mod n.) In light of observation 1 above, we only have to consider

$$k \in \{1, 2, 3, \cdots, m\} \tag{5.2}$$

Now, what exactly do we have to prove?

- For every $k \in \{1, 2, 3, \cdots, m\}$, there exists a y such that x is an integer.
- For every $k \in \{1, 2, 3, \cdots, m\}$, there exists a y such that x is a non-negative integer.

Let's knock off the first item by using the modulo idea. Taking mod m of (1) gives us

$$n(y+1) \equiv k \pmod{m} \implies y + 1 \equiv kn^{-1} \pmod{m}$$

For any k, we get $y \equiv kn^{-1} - 1 \pmod{m}(*)$, resulting in x being an integer. We now must prove that x is a positive integer. Notice that for We know that $n{-}1 \pmod{m}$ exists since $\gcd(m, n) = 1$. Now, we must prove that x is a non-negative integer. This is a bit harder to do, as we have no idea how to even begin. We know that we want $mn - m - n + k - ny$ to be positive for every $k \in \{1, 2, 3, \cdots, m\}$. For $y = m - 2$, we notice that we get

$$mn - m - n + k - ny = n - m + k > 0^{1}$$

Similarly, for $y = m - y_0$ for $m \geq y_1 \geq 2$, we get

$$mn - m - n - +k = (y_0 - 1)n - m + k > 0$$

However, for $y = m - 1$, we have no idea where to begin. We do notice that, however, from (*),

$$y \equiv -1 \pmod{m} \implies kn^{-1} - 1 \equiv -1 \pmod{m} \implies k \equiv 0 \pmod{m}$$

Therefore for $y = m - 1$, we have $k = m$ giving

$$mn - m - n + k - ny = 0 \implies x = 0$$

Our proof is complete.

□

This was another awesome problem to do, as it had many key steps involved in it.

- We first off played around with some small cases (i.e $m = 5, n = 7$ and noticed that taking mod m and mod n helped solve the equation). We also figured that inequalities would be helpful as they worked when noting $x \in \{0, 1, 2, 3\}$.

[1] using our WLOG

- We used the ideas of mods to reduce down to $y \equiv kn^{-1} - 1 \pmod{m}$. We know that there will exist a value of m due to this equation, however, we must use inequalities to figure out how.
- We assume without loss or generality that $n \geq m$ to aid in our use of inequalities (we do this before the inequalities).
- We show that the equation will always be positive for every $k \in \{1, 2, 3, \cdots, m\}$.

The full rigorous proof below is included again to show what a complete proof looks like. The above method is included to show the reader what the mathematical method is like as a problem solver. The reader may prefer the following rigorous proof, but hopefully understood how they would go about finding this proof as problem solvers.

Proof. (Rigorous) Because the equation is symettric, WLOG assume that $n \geq m$. Assume that $mn - m - n = mx + ny$. Taking the equation mod m, we arrive at

$$ny \equiv -n \pmod{m} \implies y \equiv -1 \pmod{m}^2$$

This implies that $y \geq m - 1$, however, this gives

$$mx + ny \geq mx + mn - m > mn - m - n$$

Contradiction. Now, I prove that

$$mn - m - n + k = mx + ny, k \in \{1, 2, 3, \cdots, m\}$$

The reason for this is that for $k = k_1 > m$, then we can repeatedly add m to the reduced value of k_1 mod m until we reach k_1. Our goal is to prove that for every k, there exists an x such that

- x is an integer.
- x is a non-negative integer.

Taking the equation mod m brings us to

$$n(y+1) \equiv k \pmod{m} \implies y \equiv kn^{-1} - 1 \pmod{m}(1)$$

[2] from $\gcd(m, n) = 1$

Using this value of y produces the first desired outcome. For the second, we must have $mn - m - n + k - ny \geq 0$. For $y = m - y_0$ and $m \geq y_0 \geq 2$, we get

$$mn - m - n + k - ny = (y_0 - 1)n - m + k > 0$$

For $y_0 = 1$, we have

$$y \equiv -1 \pmod{m} \implies kn^{-1} - 1 \equiv -1 \pmod{m} \implies k \equiv 0 \pmod{m}$$

Therefore, $k = m$, and we get

$$mn - m - n + k - ny = mn - m - n + m - n(m-1) = 0 \implies x = 0$$

Therefore, we have proven our desired statement, and we are done. □

Example 5.1.1. *(IMO 1983) Let a, b and c be positive integers, no two of which have a common divisor greater than 1. Show that $2abc - ab - bc - ca$ is the largest integer which cannot be expressed in the form $xbc + yca + zab$, where x, y, z are non-negative integers.*

5.2 Vieta Jumping

Example 5.2.1 (Putnam 1988)**.** *Prove that for every real number N, the equation*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

has a solution for which x_1, x_2, x_3, x_4 are all integers larger than N.

Solution. Notice that a trivial solution of this equation is $(x_1, x_2, x_3, x_4) = (1, 1, 1, 1)$. This is our generator of the other solutions, what we are about to do is find a form for another solution in terms of the other variables for x_1 to find a new value of x_1 that works. To do this, we have to isolate the variables to make a quadratic in terms of x_1. We arrive at the equation

$$x_1^2 - x_1(x_2x_3 + x_2x_4 + x_3x_4) + x_2^2 + x_3^2 + x_4^2 - x_2x_3x_4 = 0$$

Therefore, we notice that if the solutions for x_1 are $x_1 = r_1, r_2$, we have

$$r_1 + r_2 = x_2x_3 + x_2x_4 + x_3x_4$$

by Vietas formula. Assume that $(x_1, x_2, x_3, x_4) = (r_1, s_1, t_1, u_1)$ is a solution of the original equation with WLOG $u_1 \geq t_1 \geq s_1 \geq r_1$. Then by the above relationship $(x_1, x_2, x_3, x_4) = (s_1t_1 + s_1u_1 + t_1u_1 - r_1, s_1, t_1, u_1)$ is also a solution to the equation. We notice that $s_1t_1 + s_1u_1 + t_1u_1 - r_1 > u_1 \geq t_1 \geq s_1 \geq r_1$. Therefore, the new solution for x_1 is the new largest value. Repeating this procedure for the variables x_2, x_3, x_4 and so on we can always create a new largest value, hence our largest value tends to infinity and it is larger than N for all real N ■.

That was a mouthful! Go back and read this a few times through, walk away from your computer and walk around with it a bit, it's a confusing method but once you understand it you are golden!

□

Example 5.2.2 (IMO 2007). *Let a and b be positive integers. Show that if $4ab - 1$ divides $(4a^2 - 1)^2$, then $a = b$.*

Solution. Start out with noting that because $\gcd(b, 4ab - 1) = 1$, we have:

$$\begin{aligned}
& 4ab-1 \mid (4a^2-1)^2 \\
\iff & 4ab-1 \mid b^2(4a^2-1)^2 \\
\implies & 4ab-1 \mid 16a^4b^2 - 8a^2b^2 + b^2 \\
\implies & 4ab-1 \mid (16a^2b^2)(a^2) - (4ab)(2ab) + b^2 \\
\implies & 4ab-1 \mid (1)(a^2) - (1)(2ab) + b^2 \\
\implies & 4ab-1 \mid (a-b)^2
\end{aligned}$$

The last step follows from $16a^2b^2 \equiv (4ab)^2 \equiv 1 \pmod{4ab-1}$ and $4ab \equiv 1 \pmod{4ab-1}$.

Let $(a, b) = (a_1, b_1)$ be a solution to $4ab - 1|(a - b)^2$ with $a_1 > b_1$ contradicting $a = b$ where a_1 and b_1 are both positive integers. Assume $a_1 + b_1$ has the smallest sum among all pairs (a, b) with $a > b$, and I will prove this is absurd. To do so, I prove that there exists another solution $(a, b) = (a_2, b_1)$ with a smaller sum. Set $k = \frac{(a-b_1)^2}{4ab_1-1}$ be an equation in a. Expanding this we arrive at

$$\begin{aligned}
4ab_1k - k &= a^2 - 2ab_1 + b_1^2 \\
\implies a^2 - a(2b_1 + 4b_1k) + b_1^2 + k &= 0
\end{aligned}$$

This equation has roots $a = a_1, a_2$ so we can now use Vietas on the equation to attempt to prove that $a_1 > a_2$. First, we must prove a_2 is a positive integer. Notice that from $a_1 + a_2 = 2b_1 + 4b_1k$ via Vietas hence a_2 is an integer. Assume that a_2 is negative or zero. If a_2 is zero or negative, then we would have

$$a_1^2 - a_1(2b_1 + 4b_1k) + b_1^2 + k \quad = \quad 0 \geq b^2 + k$$

absurd. Therefore, a_2 is a positive integer and (a_2, b_1) is another pair that contradicts $a = b$. Now, $a_1a_2 = b_1^2 + k$ from Vieta's. Therefore, $a_2 = \frac{b^2+k}{a_1}$. We desire to show that $a_2 < a_1$.

$$\begin{aligned} a_2 &< a_1 \\ \iff \frac{b_1^2+k}{a_1} &< a_1 \\ \iff b_1^2 + \frac{(a_1-b_1)^2}{4a_1b_1-1} &< a_1^2 \\ \iff \frac{(a_1-b_1)^2}{4a_1b_1-1} &< (a_1-b_1)(a_1+b_1) \\ \iff \frac{(a_1-b_1)}{4a_1b_1-1} &< a_1+b_1 \end{aligned}$$

Notice that we can cancel $a_1 - b_1$ from both sides because we assumed that $a_1 > b_1$. The last inequality is true because $4a_1b_1 - 1 > 1$ henceforth we have arrived at the contradiction that $a_1 + b_1 > a_2 + b_1$. Henceforth, it is impossible to have $a > b$ (our original assumption) and by similar logic it is impossible to have $b > a$ forcing $a = b$ □. □

Example 5.2.3 (Classical). *Let x and y be positive integers such that xy divides $x^2 + y^2 + 1$. Prove that*

$$\frac{x^2+y^2+1}{xy} \quad = \quad 3.$$

Solution. Let $(x, y) = (x_1, y_1)$ be a solution such that $x + y$ is minimal and $\frac{x^2+y^2+1}{xy} = k \neq 3$. WLOG let $x_1 \geq y_1$ (because the equation is symmetric). However, if $x_1 = y_1$, then we must have $\frac{2x_1^2+1}{x_1^2} = 2 + \frac{1}{x_1^2} = k$ and since k is a positive integer, $x_1 = y_1 = 1$ which gives $k = 3$ but we are assuming $k \neq 3$ so hence $x_1 \neq y_1$ and $x_1 \geq y_1 + 1$ (we will use this later). I will prove that we are able to find another solution (x_2, y_1) with $x_2 + y_1 < x_1 + y_1$ forcing $k = 3$ since it contradicts the assumption that $x + y$ is minimal.

$$\begin{aligned} \frac{x^2 + y_1^2 + 1}{xy_1} &= k \\ \implies x^2 - x(ky_1) + y_1^2 + 1 &= 0 \end{aligned}$$

This equation is solved when $x = x_1, x_2$. We will now prove that x_2 is a positive integer. Notice that $x_1 + x_2 = ky_1$ therefore x_2 is an integer. Also from Vietas, $x_1 x_2 = y_1^2 + 1 > 0 \implies x_2 > 0$ from $x_1 > 0$. Therefore, x_2 is a positive integer and (x_2, y_1) is another pair that contradicts the $\frac{x^2+y^2+1}{xy} = 3$ statement. Using $x_1 x_2 = y_1^2 + 1$, we arrive at $x_2 = \frac{y_1^2+1}{x_1}$. We desire $x_2 < x_1$.

$$\begin{aligned} x_2 &< x_1 \\ \iff \frac{y_1^2 + 1}{x_1} &< x_1 \\ \iff y_1^2 + 1 &< x_1^2 \\ \text{but} x_1^2 \geq (y_1 + 1)^2 = y_1^2 + 2y + 1 &> y_1^2 + 1 \end{aligned}$$

Therefore, $x_2 < x_1$ and we have $y_1 + x_2 < y_1 + x_1$ contradicting our initial assumption, and hence $k = 3$ □. □

Example 5.2.4. *Let a, b be positive integers with $ab \neq 1$. Suppose that $ab - 1$ divides $a^2 + b^2$. Show that*

$$\frac{a^2 + b^2}{ab - 1} = 5$$

.

Solution. Let $(a, b) = (a_1, b_1)$ with WLOG $a_1 \geq b_1$ be the pair of integers such that

$$\frac{a^2 + b^2}{ab - 1} = k \neq 5$$

and $a + b$ is the smallest. If $a_1 = b_1$, then we would have $\frac{2a_1^2}{a_1^2 - 1} = k = 2 + \frac{2}{2a_1^2}$ which is only an integer when $a_1 = 1$ however $a_1 = b_1 = 1$ gives $a_1 b_1 = 1$ contradicting $ab \neq 1$ and giving zero in the denominator. Therefore $a_1 \neq b_1$

and $a_1 \geq b_1 + 1$ (we will use this later). I will show that there exist a pair $(a, b) = (a_2, b_1)$ such that $a_1 > a_2$ contradicting $a_1 + b_1$ being minimal.

$$\begin{aligned} \frac{a^2 + b_1^2}{ab_1 - 1} &= k \\ \implies a^2 + b_1^2 &= kab_1 - k \\ \implies a^2 - a(kb_1) + b_1^2 + k &= 0 \end{aligned}$$

We now have a quadratic in terms of a with roots $a = a_1, a_2$. I will now prove a_2 is a positive integer. Notice that $a_1 + a_2 = kb_1$ hence a_2 is an integer and $a_1 a_2 = b_1^2 + k$ gives us that a_2 is positive since $b_1^2 + k$ is positive and a_1 is positive.

We desire to prove that $a_2 < a_1$. From Vietas we have $a_1 a_2 = b_1^2 + k$ hence $a_2 = \frac{b_1^2 + k}{a_1}$

$$\begin{aligned} a_2 &< a_1 \\ \iff \frac{b_1^2 + k}{a_1} &< a_1 \\ \iff b_1^2 + k &< a_1^2 \\ \iff \frac{a_1^2 + b_1^2}{a_1 b_1 - 1} &< a_1^2 - b_1^2 \\ \iff \frac{a_1^2 + b_1^2}{a_1 b_1 - 1} &< a_1 + b_1 \text{from difference of squares and} a_1 - b_1 \geq 1 \\ \iff a_1^2 + b_1^2 &< a_1^2 b_1 + a_1 b_1^2 - a_1 - b_1 \\ \iff a_1 + b_1 &< a_1(a_1 b_1 - 1) + b_1(a_1 b_1 - b_1) \end{aligned}$$

If $a_1, b_1 \geq 2$ then this inequality is obviously true and $a_2 < a_1$ contradicting the minimal assumption and $k = 5$. If a_1 or b_1 are equal to 1 then we are not done however and we have to prove that $k = \frac{a_1^2 + b_1^2}{a_1 b_1 - 1} = 5$ in this situation. Since $a_1 \geq b_1 + 1$, let $b_1 = 1$. We therefore have $k = \frac{a_1^2 + 1}{a_1 - 1} = a_1 + 1 + \frac{2}{a_1 - 1}$. Therefore, we must have $a_1 - 1 | 2$ or $a_1 = 2, 3$. In both of these cases, we get $k = \frac{2^2 + 1}{2 - 1} = \frac{3^2 + 1}{3 - 1} = 5$. In both cases we have proved $k = 5$ hence we are done $\square$. $\square$

5.2.1 Exercises

Problem 5.2.1 (Crux)**.** If a, b, c are positive integers such that $0 < a^2 + b^2 - abc \leq c$ show that $a^2 + b^2 - abc$ is a perfect square.

Problem 5.2.2 (IMO 1988)**.** Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Prove that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

5.3 Wolstenholme's Theorem

We begin the number theory section with a problem that highlights a key problem solving technique throughout all of mathematics: experimenting.

Theorem 5.3.1 (Wolstenholme's)**.** *For prime p¿3, express* $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}$ *in the form* $\frac{m}{n}$ *for* m,n *relatively prime (meaning they share no common divisors). Prove that* p^2 *divides* m*.*

Proof. (Experimenting)

When solving this problem, a mathematician would first off try to simplify the problem. Instead of showing p^2 divides m, we first off try to show that p divides m. To do this, we start out with some small cases, say $p=5$. Notice that

$$\begin{aligned} 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4} &= 1+\frac{12}{24}+\frac{8}{24}+\frac{6}{24} \\ &= \frac{50}{24}=\frac{25}{12} \end{aligned}$$

We see quite clearly that $5^2 \mid 25$. We begin writing down some observations that could help us later in the problem.

- The product of the denominators $(2,3,4)$ is relatively prime to 5. In fact, the whole set $\{1,2,3,\cdots,p-1\}$ is relatively prime to p so it makes sense that there product is relatively prime to p as well.
- In the set of denominators $(1,2,3,4)$ we have $1+4=5, 2+3=5$.

We test out the second observation to see if it is of any use:

$$\left(1+\frac{1}{4}\right)+\left(\frac{1}{2}+\frac{1}{3}\right) = \frac{5}{4}+\frac{5}{6}=5\left(\frac{1}{4}+\frac{1}{6}\right)$$

We now invoke our first observation, and notice that since $\gcd(4\times 6,5)=1$, the numerator must be divisible by 5 because there are no factors of 5 in the denominator of $\frac{1}{4}+\frac{1}{6}$.

We try extending this grouping idea to the general case:

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1} \quad = \quad \left(1+\frac{1}{p-1}\right)+\left(\frac{1}{2}+\frac{1}{p-2}\right)+\cdots$$

Notice that

$$1+\frac{1}{p-1}=\frac{p}{p-1}, \qquad \frac{1}{2}+\frac{1}{p-2}=\frac{p}{2(p-2)}, \quad \cdots \quad \frac{1}{j}+\frac{1}{p-j}=\frac{p}{j(p-j)}$$

Therefore we can factor out a power of p and the resulting numerator will be divisible by p since there are no powers of p in the denominator.

Now that we've gotten that taken care of, let's move on to the p^2 problem. The first thought that we have at this point is to see what the remaining denominators are after we factor out this first power of p. Let's analyze what we had when $p=5$:

$$5\left(\frac{1}{4}+\frac{1}{6}\right)=5\left(\frac{10}{24}\right)=5\left(\frac{5}{12}\right)$$

Now, obviously $5^2 \mid m$ in this case. The question that puzzles us now is why is the numerator of $\frac{1}{4}+\frac{1}{6}$ likewise divisible by p? Let's try another example when $p=7$:

$$\begin{aligned}\left(1+\frac{1}{6}\right)+\left(\frac{1}{2}+\frac{1}{5}\right)+\left(\frac{1}{3}+\frac{1}{4}\right) &= 7\left(\frac{1}{6}+\frac{1}{10}+\frac{1}{12}\right)\\ &= 7\left(\frac{120+72+60}{6\times 10\times 12}\right)=7\left(\frac{252}{6\times 10\times 12}\right)\\ &= 7\times 7\times\left(\frac{36}{6\times 10\times 12}\right)\end{aligned}$$

Whatever the resulting expression is, it will not contribute any powers of 7 therefore the resulting numerator is divisible by 7^2. But why is 120+72+60 divisible by 7? Going through two base cases has not yielded anything yet. We could go through and try $p=11$, but I'll spear the reader this. When we hit a dead end in a math problem, we try a different technique. We go back to the general case and remember the equation

$$\frac{1}{j}+\frac{1}{p-j}=\frac{p}{j(p-j)}$$

After factoring out a p, we think "what if we consider the resulting expression mod p". Our study of inverses in the prerequisites tells us that we can indeed consider this expression mod p. Notice that

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

Whoah! This expression seems extremely useful. Since $\frac{1}{j}+\frac{1}{p-j}=\frac{p}{j(p-j)}$ uses up two terms, and we want for j to take on all the residues mod p, we must multiply the above expression by 2. For example, $\frac{p}{1(p-1)} \equiv -1^2$, but we want both the -1^2 and the $-(p-1)^2$ terms. Therefore, we now have

$$2\left[\left(\frac{1}{1}+\frac{1}{p-1}\right)+\left(\frac{1}{2}+\frac{1}{p-2}\right)+\cdots\right] \equiv -\left(\frac{1}{1^2}+\frac{1}{2^2}+\cdots+\frac{1}{(p-1)^2}\right) \pmod{p}$$

Since $\gcd(2,p)=1$, it is suficient to show that

$$-\left(\frac{1}{1^2}+\frac{1}{2^2}+\cdots+\frac{1}{(p-1)^2}\right) \equiv 0 \pmod{p}$$

Again, we don't know exactly how to proceed, but we think we have hit the right idea. Let's substitute $p=5$ into the new expression and see what results. What we desire to show is

$$-\left(\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}\right) \equiv 0 \pmod{5}$$

We think back to what frations mean modulo 5. Fractions are the same thing as inverses, so let's think about the set of inverses modulo 5. The set we are looking at is $\{1^{-1},2^{-1},3^{-1},4^{-1}\} \pmod{5}$. Notice that $1^{-1} \equiv 1 \pmod{5}, 2^{-1} \equiv 3 \pmod{5}, 3^{-1} \equiv 2 \pmod{5}, 4^{-1} \equiv 4 \pmod{5}$ therefore we have

$$\{1^{-1},2^{-1},3^{-1},4^{-1}\} \equiv \{1,3,2,4\} \pmod{5}$$

Notice that this is the same reordered set as $\{1,2,3,4\}$. Therefore, we arrive at

$$-\left(\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}\right) \equiv -\left(1^2+2^2+3^2+4^2\right) \pmod{5}$$

The resulting expression is divisible by 5 (check it yourself!) Now, we move onto the general case. We desire to show that

$$\{1^{-1},2^{-1},3^{-1},\cdots,(p-1)^{-1}\} \equiv \{1,2,\cdots,(p-1)\} \pmod{p}$$

Now, how would we do this? If we could show that no two numbers in the first set are the same, then the two sets will be congruent. This inspires us to use **proof by contradiction**, where we assume something is true, then show that this is actually a contradiction. Assume that

$$a^{-1} \equiv b^{-1} \pmod{p}, a \not\equiv b \pmod{p}$$

However, multiply both sides of the equation by ab to result in

$$\begin{aligned} aa^{-1}b &\equiv abb^{-1} \pmod{p} \\ a &\equiv b \pmod{p} \end{aligned}$$

Contradiction! Therefore, the two sets must be the same and in general we have

$$-\left(\frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2}\right) \equiv -\left(1^2 + 2^2 + 3^2 + \cdots + (p-1)^2\right) \pmod{p}$$

Now, we use the identity

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

To finally arrive at

$$-\left(1^2 + 2^2 + 3^2 + \cdots + (p-1)^2\right) = -\left(\frac{(p-1)(p)(2p-1)}{6}\right)$$

Since $\gcd(p, 6) = 1$ (since $p \geq 5$), the numerator of the expression is divisible by p implying that $p^2 \mid m$. □

That was a mouthful! Throughout this problem, we explored many useful problem solving strategies.

- **Weaken the problem:** When you have no idea how to attack a problem initially, try weakening the condition. In this case, we wanted to show that $p^2 \mid m$, so we tried tos how $p \mid m$, which provided motivation for grouping the sum.

- **Experimenting:** We analyzed simple cases such as $p = 5$ and $p = 7$ to see how would we would go about the weakened version of the problem. We wrote down some observations, and figured out how to solved the weakened problem.

- **Writing out the general form:** When our experimentation failed to solve the general case, we went back to the general form of the equation we found before. Doing so helped us relate the problem to the sum of the squares of inverses.
- **Back to the drawing board:** While the new expression looked more helpful, we had no idea how to deal with inverses. Therefore, we experimented with inverses a bit to make the key observation that the set of inverses mod p and the set of integers mod p (excluding 0) are the same.
- **Prove your lemmas:** While our observation looked extremely helpful, we had to rigorously proof our lemma. In mathematical proof writing, you cannot take statements for granted, you have to prove them. Thankfully the lemma was relatively simple to prove.

Here is a formal writeup of the above proof. The reason that I did not show this formal argument immediately, is many people are left scratching their heads thinking "I understand this, but how did the author come up with this?" Also, to be fully rigorous we must use sigma notation, which is likely confusing to some readers. You can read the following proof lightheartedly, it is included to show the reader how to write up a formal proof of their own once they solve an exciting math problem.

Proof. (Rigorous)

We group the terms as such:

$$\begin{aligned} 2\sum_{i=1}^{p-1}\frac{1}{i} &= \sum_{i=1}^{p-1}\left(\frac{1}{i}+\frac{1}{p-i}\right) \\ &= \sum_{i=1}^{p-1}\left(\frac{p}{i(p-i)}\right) \end{aligned}$$

Since $\gcd(2,p)=1$, we now desire to show that

$$\sum_{i=1}^{p-1}\frac{1}{i(p-i)} \equiv 0 \pmod{p}$$

Notice that $i(p-i)\equiv -i^2$, therefore

$$\sum_{i=1}^{p-1}\frac{1}{i(p-i)} \equiv -\sum_{i=1}^{p-1}\frac{1}{i^2} \pmod{p}.$$

Lemma. All inverses mod a prime are distinct, i.e. $a^{-1} \equiv b^{-1} \pmod{p} \iff a \equiv b \pmod{p}$

Proof.

$$\begin{aligned} a^{-1} &\equiv b^{-1} \pmod{p} \\ (ab)\, a^{-1} &\equiv (ab)\, b^{-1} \pmod{p} \\ a &\equiv b \pmod{p} \end{aligned}$$

□

Therefore

$$\{1^{-1}, 2^{-1}, 3^{-1}, \cdots, (p-1)^{-1}\} \equiv \{1, 2, 3, \cdots, (p-1)\} \pmod{p}$$

Therefore

$$\begin{aligned} -\sum_{i=1}^{p-1} \frac{1}{i^2} \pmod{p} &\equiv -\sum_{i=1}^{p-1} i^2 \\ &= \frac{(p-1)p(2p-1)}{6} \equiv 0 \pmod{p} \end{aligned}$$

Since $\gcd(p, 6) = 1$. We are now done. □

Notice how while the above proof is extremely concise, we have no motivation for why we broke the sum up as such, or how we would have thought of the above solution alltogether!

Here is a similar problem, which is much harder than this above theorem. We again include full motivation and a fully rigorous solution.

Example 5.3.1. *(IberoAmerican Olympiad) Let $p > 3$ be a prime. Prove that if*

$$\sum_{i=1}^{p-1} \frac{1}{i^p} = \frac{n}{m}$$

with $(n, m) = 1$ then p^3 divides n.

Proof. (Experminenting) Incomplete. □

Proof. (Rigorous) This is equivalent to wishing to prove that

$$2\sum_{i=1}^{p-1}\frac{1}{i^p}\equiv 0 \pmod{p^3}$$

treating each of the numbers as inverses and using $\gcd(p,2)=1$.

We now notice $\frac{1}{j^p}+\frac{1}{(p-j)^p}=\frac{(p-j)^p+j^p}{j^p(p-j)^p}$. Therefore

$$2\sum_{i=1}^{p-1}\frac{1}{i^p}=\sum_{i=1}^{p-1}\frac{(p-i)^p+i^p}{i^p(p-i)^p}$$

By lifting the exponent $v_p\left((p-i)^p+i^p\right)=v_p\left(p-i+i\right)+v_p(p)=2$. Therefore we can factor a p^2 out of the numerator to give us

$$\begin{aligned}\sum_{i=1}^{p-1}\frac{(p-i)^p+i^p}{i^p(p-i)^p}&=p^2\sum_{i=1}^{p-1}\frac{\frac{(p-i)^p+i^p}{p^2}}{i^p(p-i)^p}\equiv 0 \pmod{p^3}\\ &\iff \sum_{i=1}^{p-1}\frac{\frac{(p-i)^p+i^p}{p^2}}{i^p(p-i)^p}\equiv 0 \pmod{p}\end{aligned}$$

Notice that $i\equiv -\left(p-i\right) \pmod{p}$ so hence we now need

$$\sum_{i=1}^{p-1}\frac{\frac{(p-i)^p+i^p}{p^2}}{i^{2p}}\equiv 0 \pmod{p}$$

since we can take the negative out of the denominator.

We consider

$$\sum_{i=1}^{p-1}\frac{\frac{(\frac{p+1}{2})^p+(\frac{p-1}{2})^p}{p^2}}{i^{2p}}+\sum_{i=1}^{p-1}\frac{\frac{i^p+(p-i)^p-(\frac{(p+1)}{2})^p-(\frac{(p-1)}{2})^p}{p^2}}{i^{2p}}$$

We desire to show each part is divisible by p. For the first sum notice that we want $\sum_{i=1}^{p-1}\frac{1}{i^{2p}}\equiv\sum_{i=1}^{p-1}i^{2p} \pmod{p}$ since each element from 1 to $p-1$ has a distinct inverse including $1^{-1}\equiv 1 \pmod{p}$ and $(p-1)^{-1}\equiv(p-1) \pmod{p}$.

By Fermat's Little Theorem we have

$$\sum_{i=1}^{p-1}i^{2p}\equiv\sum_{i=1}^{p-1}i^2 \pmod{p}\equiv\frac{(p-1)(p)(2p-1)}{6}\equiv 0 \pmod{p}$$

since $p \neq 2, 3$.

Now we desire to prove that $\frac{i^p+(p-i)^p-\left(\frac{(p+1)}{2}\right)^p-\left(\frac{p-1}{2}\right)^p}{p^2} \equiv 0 \pmod{p}$. Since $\gcd(p, 2) = 1$ we want

$$\begin{aligned} 2^p i^p + 2^p(p-i)^p - (p+1)^p - (p-1)^p &\equiv 0 \pmod{p^3} \\ 2^p\left[i^p + \binom{p}{1}p(-i)^{p-1} + (-i)^p\right] - \left[p\binom{p}{1} + 1 + p\binom{p}{1}(-1)^{p-1} + (-1)^p\right] &\equiv 0 \pmod{p^3} \\ 2^p\left[p^2\right] - 2p^2 &\equiv 0 \pmod{p^3} \end{aligned}$$

The second step follows from the fact that $p^2\binom{p}{2} \equiv 0 \pmod{p^3}$ and every $i \geq 3$ we have $p^i\binom{p}{i} \equiv 0 \pmod{p^3}$, and the third step follows from p being odd.

Now, $p^2\left(2^p - 2\right) \equiv 0 \pmod{p^3}$ is true by Fermat's Little Theorem therefore we are done. □

5.4 Bonus Problems

Example 5.4.1 (IMO 1989)**.** *Prove that for all n we can find a set of n consecutive integers such that none of them is a power of a prime number.*

Solution. I claim that the set $\{(2n+2)!+2, (2n+2)!+3, \cdots, (2n+2)!+n+1\}$ satisfies the problem statement. Notice that

$$(2n+2)! + 2 = 2\left[1 + \frac{(2n+2)!}{2}\right].$$

Since $\frac{(2n+2)!}{2} \equiv 0 \pmod{2}$ it follows that $1 + \frac{(2n+2)!}{2} \equiv 1 \pmod{2}$; henceforth it is impossible for $(2n+2)!+2$ to be a power of a prime number because it has an even and an odd factor.

Next, notice that

$$(2n+2)! + k = k\left[1 + \frac{(2n+2)!}{k}\right].$$

Because $2 \leq k \leq n+1$ we must have $(2n+2)! \equiv 0 \pmod{k^2}$ or hence $\frac{(2n+2)!}{k} \equiv 0 \pmod{k}$. Therefore $1 + \frac{(2n+2)!}{k} \equiv 1 \pmod{k}$. However, since

$(2n+2)!+k$ is divisible by k it must be a perfect power of k, but since $1+\frac{(2n+2)!}{k}$ is not a perfect power of k it follows that $(2n+2)!+k$ is not a perfect power of a prime. □

Motivation. The way that we arrived at this set may be a bit confusing to the reader so I explain my motivation. When I see a problem like this I instantly think of factorials. The reason behind this is that if I asked to find a set of n consecutive integers none of which are prime, I would use the set

$$\{(n+1)!+2,(n+1)!+3,\cdots,(n+1)!+n+1\}$$

for $n \geq 1$. The reason behind this is we are looking for numbers that have two divisors.

In this case we are looking for numbers that have a divisor divisible by k and another that is not divisible by k. I noticed that looking in the prime factorization of $(2n)!$ that we can find two factors of any number k with $2 \leq k \leq n$. Therefore looking at $(2n!)+k$ we can find that this number is divisible by k but when we factorize it we are left with a term that is $1 \pmod{k}$. □

(Note: The following example includes some intense notation. For this reason we have included a table for $f_2(x)$ and $g_2(x)$ in the "motivation" section in hopes for the reader to better understand the notation.)

Example 5.4.2 (USA TSTST 2013). *Define a function $f:\mathbb{N}\to\mathbb{N}$ by $f(1)=1$, $f(n+1)=f(n)+2^{f(n)}$ for every positive integer n. Prove that $f(1),f(2),\ldots,f(3^{2013})$ leave distinct remainders when divided by 3^{2013}.*

Solution. Define $f(x)$ to be the same as in the problem. Define a function $f_n(x)$ such that $0 \leq f_n(x) \leq 3^n-1$ and $f_n(x) \equiv f(x) \pmod{3^n}$. Next, define $g_n(x)$ such that $0 \leq g_n(x) \leq \phi(3^n)-1$ and $g_n(x) \equiv f(x) \pmod{\phi(3^n)}$. We re-write the problem statement as if $x,y \in \{1,2,\cdots,3^n\}$ we have $f_n(x)=f_n(y) \iff x=y$ (i.e. $f_n(x)$ is distinct). A few nice properties of these:

1. By Chinese remainder theorem we have $f_{n-1}(x) \equiv f_n(x) \equiv g_n(x) \pmod{3^{n-1}}$.

2. By Euler's totient we have $f_n(x) \equiv 2^{g_n(x-1)} + f_n(x-1) \pmod{3^n}$.

3. From (1) and (2) along with Chinese Remainder Theorem we have $g_n(x) \equiv 2^{g_n(x-1)} + g_n(x-1) \pmod{\phi(3^n)}$

I claim that $f_n(x) = f_n(y) \iff x \equiv y \pmod{3^k}$. This is to say that the values of $f_n(x)$ are distinct when $x \in \{1, 2, \cdots, 3^n\}$ and we have $f_n(x)$ has a period of 3^n (i.e $f_n(x) = f_n(x + 3^n m)$ where m is a positive integer.

Base case: We have $f_1(1) = 1, f_1(2) = 0, f_1(3) = 2$ therefore the problem statement holds for $k = 1$. Notice that $g_1(x) = 1$ therefore $f_1(x) \equiv 2 + f_n(x-1) \pmod 3$ from proposition (2). Therefore it is clear that $f_1(x) = f_1(x + 3m)$.

Inductive hypothesis: $f_n(x) = f_n(y) \iff x \equiv y \pmod{3^n}$ holds for $n = k$. I claim it holds for $n = k + 1$.

From (1) we have $g_{k+1}(x) \equiv f_k(x) \pmod{3^k}$. Therefore we have

$$g_{k+1}(x) \equiv g_{k+1}(y) \pmod{3^k} \iff x \equiv y \pmod{3^k}$$

Since $\phi(3^{k+1}) = 2 \cdot 3^k$ and $g_{k+1}(x)$ is odd we have $g_{k+1}(x) = g_{k+1}(x + 3^k m)$ for positive integers m. This means that we can separate $g_{k+1}(x)$ into three "groups" that have length 3^k and are ordered $g_{k+1}(1), g_{k+1}(2), \cdots, g_{k+1}(3^k)$.

Because $f_k(x) \equiv g_{k+1}(x) \equiv f_{k+1}(x) \pmod{3^k}$ we can separate $f_{k+1}(x)$ into three groups all of whose elements correspond to $f_k(x)$ mod 3^k. We now have

$$f_{k+1}(x) \equiv f_{k+1}(y) \pmod{3^k} \iff x \equiv y \pmod{3^k}$$

We must now prove that

- $f_{k+1}(x) = f_{k+1}(x + 3^{k+1}m)$ where m is a positive integer.
- $f_{k+1}(x) \not\equiv f_{k+1}(x + 3^k) \pmod{3^{k+1}} \not\equiv f_{k+1}(x + 2 \cdot 3^k) \pmod{3^{k+1}}$.

Both of these two statements boil down to (2). We notice that we have

$$f_{k+1}(x + 3^k) \equiv 2^{g_{k+1}\left(x+3^k-1\right)} + f_{k+1}\left(x + 3^k - 1\right) \pmod{3^{k+1}}$$
$$\implies f_{k+1}(x + 3^k) \equiv 2^{g_{k+1}\left(x+3^k-1\right)} + 2^{g_{k+1}\left(x+3^k-2\right)} + \cdots + 2^{g_{k+1}(x)} + f_{k+1}(x) \pmod{3^{k+1}}$$

We now notice that $g_{k+1}(y)$ takes on all of the odd integers from 1 to $\phi\left(3^{k+1}\right) - 1$. This is exactly the number of elements we have above henceforth it happens that

$$f_{k+1}(x + 3^k) \equiv 2^1 + 2^3 + \cdots + 2^{\phi\left(3^{k+1}\right)-1} + f_{k+1}(x) \pmod{3^{k+1}}$$
$$f_{k+1}(x + 3^k) \equiv 2\left(\frac{2^{\phi(3^{k+1})} - 1}{3}\right) + f_{k+1}(x) \pmod{3^{k+1}}$$

.

Via lifting the exponent we have

$$v_3\left(2^{\phi(3^{k+1})}-1\right)=k+1$$

Therefore $v_3\left(\dfrac{2^{\phi(3^{k+1})}-1}{3}\right)=k$ henceforth $f_{k+1}(x+3^k)\equiv f_{k+1}(x)\pmod{3^k}$ but $f_{k+1}(x+3^k)\not\equiv f_{k+1}(x)\pmod{3^{k+1}}$. We write $f_{k+1}(x+3^k)-f_{k+1}(x)=z3^k$ where $\gcd(z,3)=1$. Notice that substituting $x=n3^k+x_1$ we arrive at

$$f_{k+1}(x_1+(n+1)\cdot 3^k)-f_{k+1}(x_1+n3^k)\equiv z3^k \pmod{3^{k+1}}$$

from which we can derive

$$f_{k+1}\left(x+a\cdot 3^k\right)-f_{k+1}\left(x+b\cdot 3^k\right)\equiv(a-b)3^k \pmod{3^{k+1}}$$

Now, notice that $f_{k+1}(x+3^k)-f_{k+1}(x)=z3^k$, $f_{k+1}(x+2\cdot 3^k)-f_{k+1}(x+3^k)=z3^k$ and $f_{k+1}(x+2\cdot 3^k)-f_{k+1}(x)=2z3^k$ therefore the first part of our list of necessary conditions is taken care of. Now, notice that substituting $a=3m, b=0$ into the second equation we arrive at the second condition.

Our induction is henceforth complete. Because the problem statement holds for all n it also holds for 2013 and we are done. □

Motivation. The main motivation I had when solving this problem was to look at the table of $f_2(x)$ and $g_2(x)$. This table was derived using properties (2) and (3). Notice how the other properties hold for this table.

x	$f_2(x)$	$g_2(x)$
1	1	1
2	3	3
3	5	2
4	1	7
5	3	9
6	5	8
7	1	4
8	3	6
9	5	5

□

Example 5.4.3 (IMO 2005)**.** *Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$*

Solution. [[2]]

I prove that for all primes p there exists a term in the sequence that is divisible by p. I claim that when $n = p-2$ we have $2^{p-2}+3^{p-2}+6^{p-2}-1 \equiv 0 \pmod{p}$.

$$\begin{aligned}
& 6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) \\
\equiv\ & 3(2^{p-1}) + 2(3^{p-1}) + 6^{p-1} - 6 \\
\equiv\ & 3(1) + 2(1) + 6(1) - 6 \equiv 0 \pmod{p}
\end{aligned}$$

Therefore when $p \neq 2, 3$ it follows that

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

When $p = 2$ we notice that $n = 1$ gives $2^1 + 3^1 + 6^1 - 1 = 10 \equiv 0 \pmod{2}$ and when $p = 3$ that $n = 2$ gives $2^2 + 3^2 + 6^2 - 1 = 48 \equiv 0 \pmod{3}$.

In conclusion notice that all primes divide a term in the sequence hence the only positive integer relatively prime to every term in the sequence is 1. □

Motivation. The motivation behind this problem is noticing that most likely every prime divides into at least one term and then trying to find which value of n generates this. The motivation fo rhte choice of n stems from noticing that $2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \equiv 0 \pmod{p}$. This is unfortunately not a fully rigorous proof as most olympiads do not accept working in fractions when we think about modulos (even though it is a fully legitimate method and is in fact necessary to prove some theorems). □

Example 5.4.4 (IMO 1971)**.** *Prove that we can find an infinite set of positive integers of the form $2^n - 3$ (such that n is a positive integer) every pair of which are relatively prime.*

Solution. [[15],[3]]

We use induction. Our base case is when a set has 2 elements and that is done by $\{5, 13\}$. Let a set have N elements and I prove it is always possible to construct a $N + 1$ element set with the new element larger than all the previous elements. Let all the distinct primes that divide the least common multiple of the N elements be $p_1, p_2, \cdots, p_k$. Denote the new element that we add to the set to be $2^x - 3$. We desire to have $2^x - 3 \not\equiv 0 \pmod{p_j}$ for $1 \le j \le k$. Since $\gcd(p_j, 2) = 1$ we have $2^{p_j - 1} \equiv 1 \pmod{p_j}$. Therefore letting

$$x = \prod_{i=1}^{k}(p_i - 1)$$

to give us $2^x - 3 \equiv -2 \pmod{p_j}$ and since $\gcd(p_j, 2) = 1$ we have $2^x - 3 \not\equiv 0 \pmod{p_j}$ as desired.

Notice that this process is always increasing the newest member of the set therefore we may do this process an infinite amount of times to give us an infinite set.

□

Motivation. The motivation behind using induction is to think of how you can construct an infinite set. It would be quite tough to build an infinite set without finding a way to construct a new term in the sequence which is essentially what we do here. □

Example 5.4.5. *(IMO Shortlist 1988) A positive integer is called a double number if its decimal representation consists of a block of digits, not commencing with 0, followed immediately by an identical block. So, for instance, 360360 is a double number, but 36036 is not. Show that there are infinitely many double numbers which are perfect squares.*

Solution. Let $C(n)$ be this function and notice that when $n = \sum_{i=0}^{k-1}(10^i a_i)$ where $0 \le a_m \le 9$ when $m \ne k-1$ and $1 \le a_{k-1} \le 9$, we have

$$C(n) = (10^k + 1)\sum_{i=0}^{k-1}(10^i a_i)$$

We set

- $10^k + 1 = 49p_1^{e_1} \cdots p_m^{e_m}$
- $\displaystyle\sum_{i=0}^{k-1}(10^i a_i) = 36p_1^{e_1} \cdots p_m^{e_m}$

Obviously $C(n)$ is a perfect square in this case. Also since

$$10^{k-1} < \sum_{i=0}^{k-1}(10^i a_i) = \frac{36}{49}(10^k + 1) < 10^k$$

it follows that $1 \le a_{k-1} \le 9$. It is left to prove that there are infinite k such that $49|(10^k + 1)$. Noticing that $\text{ord}_{49}(10) = 42$, we see that $k = 42x + 21$ satisfies the condition $10^k + 1 \equiv 0 \pmod{49}$ hence we have constructed infinitely many double numbers which are perfect squares. $\square$

Bibliography

[1] Burton, David M. Elementary Number Theory. Boston: Allyn and Bacon, 1976. Print.

[2] ”104 Number Theory Problems: From the Training of the USA IMO Team [Paperback].” Amazon.com: 104 Number Theory Problems: From the Training of the USA IMO Team (9780817645274): Titu Andreescu, Dorin Andrica, Zuming Feng: Books. N.p., n.d. Web. 01 Aug. 2013.

[3] Andreescu, Titu, and D. Andrica. Number Theory: Structures, Examples, and Problems. Boston, MA: Birkhuser, 2009. Print.

[4] Problems of Number Theory in Mathematial Competitions by Yu Hong-Bing

[5] `http://yufeizhao.com/olympiad/mod2.pdf`

[6] `http://aopswootblog.wordpress.com/2013/03/09/number-theory-4-using-appropriate-moduli-to-solve-exponential-diophantine-equa`

[7] `http://projectpen.files.wordpress.com/2008/10/pen-vol-i-no-1.pdf`

[8] `http://blogs.sch.gr/sotskot/files/2011/01/Vieta_Jumping.pdf`

[9] `http://www.uwyo.edu/moorhouse/courses/3200/division_algorithm.pdf`

[10] `http://math.stanford.edu/~paquin/Notes.pdf`

[11] Art of Problem Solving 2012-2013 WOOT Diophantine Equations Handout

[12] http://www.artofproblemsolving.com/Wiki/index.php/Fermat_number

[13] http://www.math-olympiad.com/35th-canadian-mathematical-olympiad-2003.htm#2

[14] http://www.artofproblemsolving.com/Forum/viewtopic.php?f=721&t=542072

[15] http://www.artofproblemsolving.com/Forum/viewtopic.php?t=42703

[16] http://www.artofproblemsolving.com/Wiki/index.php/2005_USAMO_Problems/Problem_2