Number Theory - Chapter N Section T

Dennis Chen, Jet Chung, David Zhao, and Aadi Karthik

March 26, 2018

Preface

This handout covers a larger range of topics than my [Dennis Chen's] Algebra Inequalities and Telescoping handouts. As such, there may be some sections which are trivial for you and some sections you do not understand. Do not be surprised or discouraged if this is the case; if you need more solutions to learn from after trying the Exercises, do not hesitate to look up the solution. However, do not use the solutions as a way to get out of thinking of the problem; only use it after you have exhausted all possible methods you can think of. Similarly, check the solution after solving a problem; there may be other methods which will help you, or your solution could be wrong.

The organization of this handout is similar to those of my other handouts – the main sections will be Theory, Results, Examples, Exercises, and Hints. The Results section will contain some rules which stem from the concepts of the Theory. This time, however, the topics will build off of each other – we will start with basic divisibility rules and modular arithmetic which will then lead naturally into Fermat's Little Theorem, Euler's Totient Theorem, Wilson's Theorem, and even problems involving methods of proof such as induction and the pigeonhole principle.

1 GCF, LCM, and Divisibility

1.1 Divisibility Rules

Divisibility seems like such a simple idea – if a divides b (which is denoted as $a \mid b$ in this handout) then $\frac{b}{a}$ must be an integer. However, this falls apart when a or b is equivalent to 0. For the purposes of this handout we shall say that for integers a, b that $a \mid b$ if and only if there is some integer c such that $ac = b$. This means that 0 divides no integer except for 0, and that all integers divide 0.

Extending the definition of divisibility further gives us a rigorous definition of gcf and lcm. We state that $gcf(a_1, a_2 \ldots_n) = c$ such that $c|a_1, a_2 \ldots$ and that there is no d such that $d|a_1, a_2 \ldots a_n$and $d > c$. We also state that $lcm(a_1, a_2 \ldots a_n) = x$ such that $a_1, a_2 \ldots a_n|x$ and that there is no y such that $y|a_1, a_2 \ldots a_n$ and $y < x$. However, since we can always find an arbitrarily large negative number x, for the lcm, we require $x, y > 0$.

1.2 Results

Our rigorous definition of divisibility, gcf, and lcm leave us with some results that we can prove which we would not have obtained using the "intuitive" method.

1. If $a|b$ and $b|c$ then $a|c$. (This may be referred to as the chain rule of divisibility.)
2. If $a|b$, then $a|bc$.
3. If $a|b$ and $a|c$, then $a|b + c$.
4. The two values $gcf(a, b) \cdot lcm(a, b)$ and ab are equivalent.

1.3 Examples

1. Find the value of $gcf(0, 8)$.

Solution: Since all integers divide 0, we look at the largest one of them that evenly divides 8, which is 8 itself. Since 8|0 and 8|8 and no other integer c exists such that c|0,8 and c>8, the value

of gcf(0,8) is 8.

2. Find the value of $gcf(3, 6)$.

Solution: We claim that the answer is 3. We see that $3|3$ and that $3|6$. Now assume there is some integer a such that $a|3, 6$ and $a > 3$. Obviously, if $x > y$ then xy, so there is no a such that $a|3$ and $a > 3$, so $gcf(3, 6) = 3$.

3. Find the value of $gcf(0, 4, 10)$.

Solution: All numbers divide 0, so $gcf(0, 4, 10) = gcf(4, 10)$. We claim that $gcf(4, 10) = 2$. Since $gcf(2, 5) = 1$ (in other words, 2 and 5 are relatively prime), then multiplying both values by 2 only gives us a common factor of 2, so our answer is 2.

4. Find the value of lcm(4,6,10).

Solution: We claim that lcm(4,6,10)=2lcm(2,3,5)=60. Since (2,3,5) are pairwise relatively prime, lcm(2,3,5)=a must satisfy 2,3,5|a. The smallest number which does this is 235=30. If all the terms are multiplied by 2, there is only one more factor of 2 to account for, so our answer is (235)2=60.

1.4 Exercises

1.4.1 Easy

1. Is $\gcd(0, 0)$ defined? If so, what is its value? If not, what makes it undefined?

2. Is $\text{lcm}(0, 0)$ defined? If so, what is its value? If not, what makes it undefined?

3. Find the smallest number k such that $5, 6, 9|k$.

4. Find the largest number j such that $j|8, 10, 12$.

1.4.2 Medium

1. Let n be a 5-digit number, and let q and r be the quotient and the remainder, respectively, when n is divided by 100. For how many values of n is $q + r$ divisible by 11? (AMC)

1.4.3 Hard

1. How many ordered pairs of integers (a, b) satisfy $gcf(a, b) = 8$ and $lcm(a, b) = 120$?

2. Twenty bored students take turns walking down a hall that contains a row of closed lockers, numbered 1 to 20. The first student opens all the lockers; the second student closes all the lockers numbered $2, 4, 6, 8, 10, 12, 14, 16, 18, 20$; the third student operates on the lockers numbered $3, 6, 9, 12, 15, 18$: if a locker was closed, he opens it, and if a locker was open, he closes it; and so on. For the ith student, he works on the lockers numbered by multiples of i: if a locker was closed, he opens it, and if a locker was open, he closes it. What is the number of the lockers that remain open after all the students finish their walks? (104 NT)

2 Euclidean Algorithm

2.1 The Euclidean Algorithm

Imagine that we want to find the gcf of 102 and 78. We could factor both numbers, and find the factors they share, but there is a much more efficient method. Image that our gcf is n. Then $102 = kn$ and $78 = mn$. Thus, since they are both multiples of n, so will their difference, by a

combination of Result 2 and 3 in the Divisibility section. Thus, we can subtract the two and find the gcf of those - $gcf(36, 78)$. We can perform the above operations as many times as we want, until we get two numbers that are multiples of each other. We can subtract $2 \cdot 36$ from 78 to get $gcf(78 - 2 \cdot 36, 36) = gcf(6, 36)$. Since 36 is a multiple of 6, we can stop, and our gcf is 6.

An extension of the Euclidean Algorithm appropriately named the Extended Euclidean Algorithm can be used to solve Diophantine Equations of the form $ax + by = c$, more specifically, $ax + by = \gcd(a, b)$. This will be touched on in both this section and the section on Diophantine Equations. Since the Extended Euclidean Algorithm is more of a technique than a theorem, we shall be teaching through examples.

2.2 Bezout's Identity

Bezout's Identity states the following:
1. $ax + by = \gcd(a, b)$ has solutions.
2. The smallest positive value of c such that $ax + by = c$ has integer solutions is $\gcd(a, b)$.
3. All integers c such that $ax + by = c$ has solutions is divisible by $\gcd(a, b)$.

It should be obvious why 3 is true – If $\gcd(a, b)|ax + by$ but $\gcd(a, b) \not| c$ then $\gcd(a, b) \neq c$ because they do not share all of their divisors. So $\gcd(a, b)|c$. The proofs of Statements 1 and 2 are left as exercises.

Examples

1. Find two integer values (x, y) such that $5x + 7y = 1$.

Solution: By the Extended Euclidean Algorithm,
$7 = 5 + 2(1)$
$5 = 2(2) + 1$

This implies the following:
$1 = 5 - 2(2)$
Substituting in $2 = 7 - 5$ yields $1 = 5 - 2(2) = 5 - (7 - 5)(2) = 3 = 5(3) - 7(2)$. As thus, a pair of values is $(3, -2)$. It should be easy at this point to find the general form for the solutions – $(3+7n, 2-4n)$. (Plugging the general form in yields $5(3+7n)+7(-2-5n) = 15+35n-14-25n = 1$.)

2. Find all integer solutions (in general form) to $14x + 20y = 52$.

Solution: This implies that $7x + 10y = 26$ (dividing both side by 2).

By the Extended Euclidean Algorithm,
$10 = 7(1) + 3$
$7 = 3(2) + 1$
$3 = 1(3)$.

This implies the following:
$1 = 7 - 3(2)$
Substitute in $3 = 10 - 7$ to yield $1 = 7 - (10 - 7)(2) = 7(3) - 10(2)$. Multiplying both coefficients by 26 will give us a difference of 26. Therefore, one solution is $(78, -52)$.) It should be easy to see that the general form is $(8 + 10n, 3 - 7n)$. (Why can we jump from $(78, -52)$ to $(8, 3)$?)

2.3 Exercises

2.3.1 Easy

1. Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every natural number n. (1959 IMO #1)

2. Prove that the fraction $\frac{30n+1}{12n+1}$ is irreducible for every natural number n

2.3.2 Medium

1. 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.(1985 AIME #13) (The reader is encouraged to give some time to this problem.)

2.3.3 Hard

2.3.4 Problem 1

1. Prove Bezout's Identity, which states that for integers a and b there exists integers m and n such that $am + bn = \gcd(a, b)$
2. Find the GCD of $(2002 + 2, 2002^2 + 2, 2002^3 + 2 \cdots)$

3 Modular Arithmetic

3.1 An introduction

Imagine a clock. There are 12 different numbers. Time goes from 12-11:59 - there is no 13'O Clock, unless you are using military time, in which there is no 25'O Clock. Once you get an hour past 12 o clock, you don't have 13 o clock - you get back to one. This is the idea of modular arithmetic.

It can also be represented as a circle, like a clock. Imagine you have a circle that starts at 0 or 5, and goes around. You go 0, 1, 2, 3,4, but instead of going to 5, you go back to one. This shows the remainders when dividing by 5 - at first, the remainder is 0, 1, 2, 3, 4, but once you get to 5, the remainder is once again 0. The remainder when 6 is divided by 5 is 1, then 2, 3, 4, back to 0. Each different possible remainder is called a ***residue*** There are exactly n residues for mod n - $0, 1, \cdots n - 1$. Once you get to n, it wraps around back to 0.

3.2 Some Definitions

We say $a \equiv b \mod n$ if the remainder when a is divided by n is the same as when b is divided by n. Both a and b can be represented as $kn + x$ and $mn + x$ where x is the remainder, and m and n are integers. Thus, if we subtract both numbers, the number will be divisible by n. This can be formally represented as $a \equiv b \mod n$ if and only if $n|a - b$.

3.2.1 Results

If $a \equiv b \pmod n$, then the following must be true: 1. $a + nx \equiv b \pmod n$ 2. $a + x \equiv b + x \pmod n$ 3. $ax \equiv bx \pmod n$ 4. $\frac{a}{x} \equiv \frac{b}{x} \pmod{\frac{n}{gcf(n,x)}}$. 5. If $a \equiv b \pmod n$ and $c \equiv d \pmod n$ then $a + c \equiv b + d \pmod n$. 6. If $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$. (This is similar to the transitive property.) 7. $a^x \equiv b^x \pmod n$

We shall sketch a proof for 4 below – the rest of the proofs are left as exercises for the reader.

Proof for 4: Note that since $n|a - b$, that $a - b = nk$ for some arbitrary k. (Think of nk as the difference between a and b.) Then we note that $\frac{a-b}{x} = \frac{nk}{x}$. (Dividing the numbers by x divides the difference by x as well.)

3.3 Arithmetic with mods

If $a \equiv b \mod n$ and $c \equiv d \mod n$ Then $a + c \equiv b + d \mod n$ This can be shown by representing the numbers in the form $kn + x$ and will be left as an exercise for the reader to prove the above

for addition, subtraction, and multiplication $ac \equiv bd \mod n$

Finally, we can show if $a \equiv b \mod n$ then $a^m \equiv b^m \mod n$. This can again be shown by writing the numbers as $kn + x$ and then using binomial expansion.

Modular Inverses - there exists an a^{-1} such that $aa^{-1} \equiv 1 \mod n$ if and only if a and n are relatively prime. Proof - if they are not relatively prime, then we can write $ka = n$ where k is an integer. Then, $aa^{-1} - 1 \equiv 0 \mod ka$. Then we have $kma = aa^{-1} - 1$ Which is impossible because we have a multiple of a on the left, and a multiple of a-1 on the right, which cannot be equal as they are different mod a. The proof of the existence of the modular inverse is left as an exercise.

4 Divisibility with mods

4.1 Another introduction

What does it mean for a number to be divisible by another in terms of mods?

If a is a multiple of n, It means that $a \equiv 0 \mod n$ because if there is no remainder when a is divided by n, it is a multiple. Thus, we can use our knowledge of modular arithmetic to find out if a number is a multiple of another.

4.2 Divisibility by 2 and 5

Have our number x be represented as the sum of powers of ten, similar to how the base 10 expansion is written. With our digits $a_1, a_2 ... a_n$ we can represent x as $a_n 10^{n-1} + a_{n-1} 10^{n-2} + ... + a_1 10^0$. Taking this (mod 2) gives us $x \equiv a_1 10^0 \equiv a_1 \pmod 2$. This gives us our divisibility rule – if the last digit is divisible by 2, the whole number is.

The extension of this proof for divisibility by 5 is left as an exercise to the reader.

4.3 Divisibility by 3, 9

Like above, we can represent our number x as the sum of powers of ten. Writing the same way gives us $x = a_n 10^{n-1} + a_{n-1} 10^{n-2} + ... + a_1 10^0$. Taking this all (mod 3) gives us $x \equiv a_n + a_{n-1} + ... + a_1$. This gives us our divisibility rule – if the sum of the digits of a number is divisible by 3, the whole number is.

The extension of this for 9 is also left as an exercise to the reader.

4.4 Divisibility by 11

Expanding, we can use the same trick as 3 and 9. Keep in mind that $10 \equiv -1 \mod 11$. What does this mean for our expansion of the number? What is the rule for divisibility by 11?

Problem: Let n be a 5-digit number, and let q and r be the quotient and the remainder, respectively, when n is divided by 100. For how many values of n is $q + r$ divisible by 11? (AMC)

4.5 Divisibility by Composite Numbers

A number will be divisible by numbers such as these if it is divisible by its prime factors. For example, a number is divisible by 6 if it is divisible by 2 and 3. The reader should come up with rules for 12, 20, 15, etc.

4.6 Examples

1. Consider a circle whose circumference has points labeled $1, 2, 3...100$. Any chord between two of these points is drawn – the chord is labeled with the product of the numbers its endpoints are labeled with. Find the remainder of the sum of all the numbers that label the chords when divided by 102.

5 Chinese Remainder Theorem

5.1 An Introduction

The Chinese Remainder Theorem(CRT) is a method of solving 2 or more linear congruencies. In this section, we will begin by stating and then proving CRT. Then we will show you two "versions" of CRT and as usual, we will end with a couple of exercises.

5.2 The Theorem

The Chinese Remainder Theorem states that 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(i.e. $\gcd(b_i, b_j) = 1 \iff i \neq j$)has one distinct solution for x modulo $b_1 b_2 \dots b_n$.

Proof: We will use induction. (See section 11) We will start by 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 $\pmod{b_1 b_2}$. To do so, consider the set of numbers

$$S = kb_1 + a_1, 0 \leq k \leq b_2 - 1.$$

From this we see 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 we will prove that there is a solution for $n = k + 1$. Let the following equation have solution $x \equiv z \mod b_1 b_2 \cdots b_k$ 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 $\gcd(b_k + 1, b_1 b_2 \cdots b_k) = 1$.

5.3 "Easy" CRT(How to Solve 2 Linear Congruences)

If m, n are co-prime integers then m^{-1} exists $\mod n$ and

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \iff x \equiv a + m \left[\frac{b-a}{m} \pmod{n} \right] \pmod{mn}$$

Exercise: Prove that "Easy" CRT works.

5.3.1 Examples

1. Solve $\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 7 \pmod{13} \end{cases}$.

   Solution: Because the GCD of 7 and 13 is 1, we can use easy CRT as shown below:

   $$x \equiv 2 + 7 \cdot \left(\frac{5}{7} \pmod{13} \right) \pmod{91}.$$

   $5 + 13k$ is divisible by 7 when $k = 5$, so $\frac{5}{7} \pmod{13}$ evaluates to $\frac{5 + 5 \cdot 13}{7} = 10$. Hence the final answer is $x \equiv 2 + 7 \cdot 10 = 72 \pmod{91}$

2. Solve $\begin{cases} x \equiv 11 \pmod{17} \\ x \equiv 20 \pmod{21} \end{cases}$.

   Solution: Because the GCD of 17 and 21 is 1, we can use easy CRT as shown below:

   $$x \equiv 11 + 17 \cdot \left(\frac{9}{17} \pmod{21} \right) \pmod{357}.$$

   $9 + 21k$ is divisible by 17 when $k = 2$, so $\frac{9}{17} \pmod{21}$ evaluates to $\frac{9 + 21 \cdot 2}{17} = 3$. Hence the final answer is $x \equiv 11 + 20 \cdot 3 = 62 \pmod{357}$

3. Solve $\begin{cases} x \equiv 15 \pmod{19} \\ x \equiv 22 \pmod{23} \end{cases}$.

   Solution: Because the GCD of 19 and 23 is 1, we can use easy CRT as shown below:

   $$x \equiv 15 + 19 \cdot \left(\frac{7}{19} \pmod{23} \right) \pmod{437}.$$

   $7 + 23k$ is divisible by 19 when $k = 3$, so $\frac{7}{19} \pmod{21}$ evaluates to $\frac{7 + 23 \cdot 3}{19} = 4$. Hence the final answer is $x \equiv 15 + 19 \cdot 4 = 91 \pmod{437}$

5.4 "Hard" CRT(How to Solve Linear Congruences the "Real" Way)

For a system of congruences with co-prime moduli, the process is as follows:

1. Begin with the congruence with the largest modulus, $x \equiv a_n \pmod{b_n}$. Re-write this modulus as an equation $x = b_n k + a_n$, for some positive integer k.
2. Substitute the expression for x into the congruence with the next largest modulus, $x \equiv a_n \pmod{b_n} \implies b_n + a_n \equiv a_{k-1}$.
3. Solve this congruence for k.
4. Write the solved congruence as an equation, and then substitute this expression for into the equation for x.
5. Continue substituting and solving congruences until the equation for x implies the solution to the system of congruence.

5.4.1 Examples

1. Solve $\begin{cases} x \equiv 7 \pmod 9 \\ x \equiv 9 \pmod{11} \\ x \equiv 13 \pmod{17}. \end{cases}$

   Solution: We don't want to do more work than we have to. Note that $x \equiv -2 \pmod 9$ and $x \equiv -2 \pmod{11}$, so $x \equiv -2 \equiv 97 \pmod{99}$. Then we can use "Hard CRT" and we see that $97 + 99n \equiv 12 + 15n \equiv 13 \pmod{17}$ implying $15n \equiv 1 \pmod{17}$. It should be easy to see at this point that $n \equiv 8 \pmod{17}$. Plugging in $n = 8$ yields $x \equiv 97 + 99 \cdot 8 \equiv 889 \pmod{1683}$ which is our solution.

2. Solve $\begin{cases} x \equiv 7 \pmod{13} \\ x \equiv 9 \pmod{19} \\ x \equiv 19 \pmod{23}. \end{cases}$

   Solution: Will add in later.

3. Solve $\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod 9. \end{cases}$

   Solution: We want to reduce our workload – $x \equiv -1 \pmod 4$ and $x \equiv -1 \pmod 5$ so $x \equiv -1 \pmod{20}$ and $x \equiv -2 \pmod 7$ and $x \equiv -2 \pmod 9$ so $x \equiv -2 \pmod{63}$. Now bigger numbers seem awfully annoying so let's solve for $-x$. So have $63n + 2 \equiv 1 \pmod{20}$. Clearly this implies $3n \equiv 1 \pmod{20}$, or $n \equiv 7 \pmod{20}$. Plugging this in gives us $-x \equiv 63 \cdot 7 + 2 \pmod{1260}$ or $x \equiv 817 \pmod{1260}$.

5.5 How to Solve Linear Congruences If the Moduli Aren't Coprime

Let's try to solve the congruence

$$\begin{cases} x \equiv a \pmod i \\ x \equiv b \pmod j \end{cases}$$

such that the $\gcd(i, j) = k$.

The first thing that must be true is $a \equiv b \pmod k$. For example, in the modular system

$$\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 4 \pmod 6, \end{cases}$$

there will be a solution. Both imply that x is even, which leads to no contradiction.

However, in the modular system

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 6, \end{cases}$$

the first congruence implies x is odd, while the second one implies x is even, which leads to a contradiction.

IF AND ONLY IF there is no contradiction, you can use CRT. The one thing that is different with non-coprime moduli is that you have to divide the smaller modulus by the gcd of the two moduli in order to apply CRT correctly.

5.5.1 Examples

1. Solve $\begin{cases} x \equiv 8 \pmod 9 \\ x \equiv 10 \pmod{11} \end{cases}$

   Solution: Note that $n \equiv -1 \pmod 9$ and $n \equiv -1 \pmod{11}$. This implies $n \equiv -1 \equiv 98 \pmod{99}$, which is our answer.

2. Solve $\begin{cases} x \equiv 7 \pmod 9 \\ x \equiv 6 \pmod{11} \end{cases}$

   Solution: Using Hard CRT we see that $9x + 7 \equiv 6 \pmod{11}$ or $9x \equiv 1 \pmod{11}$. At this point it is quite obvious $x \equiv 5 \pmod{11}$. Plugging this in gives us $x \equiv 9 \cdot 5 + 7 \equiv 61 \pmod{99}$.

3. Solve $\begin{cases} x \equiv 8 \pmod{10} \\ x \equiv 5 \pmod{15} \end{cases}$

   Solution: The first congruence implies x is not divisible by 5 and the second one implies that x is divisible by 5. Since this is a contradiction, we have no solutions.

5.6 Exercises

5.6.1 Easy

1. Solve $\begin{cases} x \equiv 7 \pmod{19} \\ x \equiv 13 \pmod{23} \end{cases}$ using both methods.

2. Solve $\begin{cases} x \equiv 6 \pmod{12} \\ x \equiv 14 \pmod{16} \end{cases}$ using both methods.

3. Solve $\begin{cases} x \equiv 6 \pmod{12} \\ x \equiv 14 \pmod{16} \end{cases}$ using both methods.

4. Solve $\begin{cases} x \equiv 20 \pmod{31} \\ x \equiv 28 \pmod{32} \end{cases}$ using both methods.

5. Solve $\begin{cases} x \equiv 19 \pmod{27} \\ x \equiv 28 \pmod{108} \end{cases}$ using both methods.

5.6.2 Medium

1. Solve $\begin{cases} x \equiv 33 \pmod{37} \\ x \equiv 39 \pmod{42} \\ x \equiv 43 \pmod{47}. \end{cases}$

2. Solve $\begin{cases} x \equiv 7 \pmod{17} \\ x \equiv 9 \pmod{18} \\ x \equiv 10 \pmod{19} \\ x \equiv 39 \pmod{42}. \end{cases}$

3. Solve $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 6 \pmod 9 \\ x \equiv 10 \pmod{12}. \end{cases}$

5.6.3 Hard

1. Let $N = 123456789101112\ldots4344$ be the 79-digit number obtained that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45?(Source: AMC 10)

2. Last year Isabella took 7 math tests and received 7 different scores between 91 and 100, inclusive. After each test she noticed that the average of her test scores was an integer. Her score on the seventh test was 95. What was her score on the sixth test? (Source: AMC 10)

6 Diophantine Equations

6.1 An Introduction

Diophantine Equations are polynomials that require integer solutions. There are a few methods for solving Diophantine's:

6.2 Factoring with one variable

We know how to solve quadratic equations by factoring: for example, if we have $x^2 - 3x + 2 = 0$, we can factor this as $(x-2)(x-1)$. But what about if we have $x^2 - 3x + 2 = 6$? It is a blessing that in number theory that there are only integer solutions, thus only a finite number of solutions to this equation. We can factor $x^2 - 3x + 2 = 6$ as $(x-2)(x-1) = 6$, and then find the factors of 6: $1, 6; 2, 3$ and the negatives of all of these. Note that $(x-2)$ and $(x-1)$ may only be the values of $(-3, -2)$ and $(2, 3)$. The values of x given these values of $(x-2, x-1)$ are left as an exercise to the reader.

6.2.1 Examples

1. A point whose coordinates are both integers is called a lattice point. How many lattice points lie on the hyperbola $x^2 - y^2 = 2000^2$? (AIME)

Solution: We can factor $(x+y)(x-y) = 2000^2.2000^2 = 2^8 \cdot 5^6$, and $x+y$ and $x-y$ must have the same parity (even or odd), so they must both be even. Thus, we are splitting up $2^6 \cdot 5^6$. We know that there are $(6+1)(6+1)$ factors, or 49. Since there are 49 factors, there are 49 factor pairs. However, we can multiply by 2 because both numbers can be negative, which yields our final answer of $2 \cdot 49 = 98$.

2. How many lattice points does the line $4x + 6y = 7$ intersect in the region $0 \leq x \leq 100$?

Solution: Note that we desire solutions to the Diophantine Equation $4x + 6y = 7$. However, this has no solutions, because $2|4x + 6y = 2(2x + 3y)$ but the statement $2|7$ is not true. For two values to be equivalent, they must have the same divisors, so this Diophantine Equation has no solutions, giving us our answer of 0.

When we complete the square, we can think of it as finding the area of a square with side length $x + 3$ in the case of $x^2 + 6x = 16$. We can add 9 to both sides, and we have $x^2 + 6x + 9 = 25$. Thus, the area of the square is 25, the length is 5, and x is 2.

6.3 Completing the Rectangle/SFFT

What if we want to factor a problem such as $xy + 5x - 6y = 0$? We can do something called completing the rectangle. It is very similar to completing the square, but it is now finding the area of a rectangle. If we have $xy + 5x - 6y = 9$, we can think of this as the area of a rectangle with sides $x - 6$ and $y + 5$ (insert diagram here). Thus, the last term that is missing on the LHS is 30. Adding 30 to both sides, we get $(x+5)(y-6) = 39$. Thus, we know that $(x+5)$ and $(y-6)$ are either $13, 3, 3, 13, 1, 39$, or $39, 1$. Of course, we can solve for x and y, for which there are many pairs.

6.4 Linear Combinations

Linear combinations is the name given to any Diophantine Equation of the form $ax + by = c$. Let's take a look at a few properties of these equations.

(PLEASE NOTE: This paragraph is important for the Linear Combinations subsection – do not

Table 1: Solutions to $5x + 7y = 700$

7x	5y
0	140
5	133
10	126
...	...
100	0

skim over this.)

First off, $gcf(a, b)|c$ must be true for there to be solutions x, y. Here's how we can prove this – have $gcf(a, b) = n$. Then we have $a = a'n$ and $b = b'n$. This implies also that $gcf(a', b') = 1$. We want to find the values of (x, y) such that $n(a'x + b'y) = c$. Note that if two values (i, j) are equivalent then either both $n|i$ and $n|j$ or $n \not| i$ and $n \not| j$. Clearly, $n|n(a'x + b'y)$, so $n|c$, by the first property in the last sentence.

6.4.1 Examples

1. You want to fill a 700 gallon pool with water using buckets that can hold 5 gallons and 7 gallons. How many ways are there to do this?

We can express this situation as $5x + 7y = 700$. The key is to start from one solution and then see how we can find the others. Since 700 is divisible by both 7 and 5, we can start out with one solution being 0, and go from there.
We can see a pattern: on the left column, the numbers go up by 5, while they go up by 7 on the right. This is because each new solution has to add and then subtract a 35. This should make intuitive sense. We can count this: $0, 5, 10 \ldots 100$ leaves 21 solutions to this equation.

2. Find the ordered pair (x, y) such that $x > 0$, x is minimized, (x, y) are integers, and $89x - 55y = 1$.

Solution: The following implies $89x \equiv 1 \pmod{55}$. Since $gcf(55, 89) = 1$, there is a modular inverse. Using the Extended Euclidean Algorithm, we can find the modular inverse. We shall do this in an organized manner using a table.

89 = 55(1)+34	34=89-55(1)
55 = 34(1)+21	21=55-34(1)
34=21(1)+13	13=34-21(1)
21=13(1)+8	8=21-13(1)
13=8(1)+5	5=13-8(1)
8=5(1)+3	3=8-5(1)
5=3(1)+2	2=5-3(1)
3=2(1)+1	1=3-2(1)
2=1(2)	

Using the right hand side of the table we get the following.

$$
\begin{aligned}
1 &= 3 - 2(1) \\
1 &= 3 - (5 - 3(1)) = 3(2) - 5 \\
1 &= (8 - 5)(2) - 5 = 8(2) - 5(3) \\
1 &= 8(2) - (13 - 8)(3) = 8(5) - 13(3) \\
1 &= (21 - 13)(5) - 13(3) = 21(5) - 13(8) \\
1 &= 21(5) - (34 - 21)(8) = 21(13) - 34(8) \\
1 &= (55 - 34)(13) - 34(8) = 55(13) - 34(21) \\
1 &= 55(13) - (89 - 55)(21) = 55(34) - 89(21)
\end{aligned}
$$

As thus, $89(21) - 55(34) = -1$. Even though this is a -1, we can remedy the problem. Note that $54(89(21) - 55(34) = 55 + 54(-1) = 1$, which means $(54 \cdot 21, 54 \cdot 34)$ is a solution. Then note that we may decrease x by 55 and decrease y by 89 and still obtain a solution. We see that $54 \cdot 21 \equiv -1 \cdot 21 \equiv 34 \pmod{55}$, so the smallest possible value of x is 34. Plugging this in gives us $89(34) - 55y = 1$, implying $y = 55$. As thus, our ordered pair is $(34, 55)$.

6.5 Exercises

1. How many lattice points are contained in the segment from $(19, -4)$ to $(1243, 356)$ (including the endpoints)? (Mathynomial)

2. How many right triangles have integer leg lengths a and b and a hypotenuse of length $b + 1$, where $b < 100$? (AMC)

3. In how many ways can 345 be written as the sum of an increasing sequence of two or more consecutive positive integers? (AMC)

4. Find the number of ordered pairs of positive integer solutions (m, n) to the equation $20m+12n = 2012$. (AIME)

5. Let x and y be two-digit integers such that y is obtained by reversing the digits of x. The integers x and y satisfy $x^2 - y^2 = m^2$ for some positive integer m. What is $x + y + m$? (AMC)

6. Let $N = 123456789101112 \ldots 4344$ be the 79-digit number obtained that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45? (AMC 10)

7. Let m be the number of solutions in positive integers to the equation $4x + 3y + 2z = 2009$, and let n be the number of solutions in positive integers to the equation $4x + 3y + 2z = 2000$. Find the remainder when $m - n$ is divided by 1000. (AIME)

8. How many lattice points does a circle with area 144π centered at the origin intersect?

9. Find all solutions (x, y) to $15x + 10y = 6$.

7 Results of Euler and Fermat

7.1 Euler's Totient Function

How many numbers less than a number n are coprime to n? For example, for $n = 10$, the numbers $3, 7, 9$ are coprime to n, and thus there are 3. This leads us to the totient function:

Definition: We define $\phi(n)$ to be the number of integers k such that $k < n$ and satisfying $gcd(n, k) = 1$.

It may be useful to calculate some values of $\phi(n)$ for some values of n. Of course, this function is only defined over the Naturals. As you may wonder, how are we going to calculate the value for $\phi(n)$? Well, before asking that question, it will be useful to look at an easier case, a subset of the naturals: the primes. For any prime p, it is easy to see that $\phi(p) = p-1$, but we can do better.

Let's say that we want to calculate $\phi(n)$ for $n = p_1^{e_1} p_2^{e_2} ... p_n^{e_n}$. We can see that $\frac{1}{p_n}$ of these numbers will be divisible by p_n. Thus, $1 - \frac{1}{p_n}$ of these numbers will not be divisible by p_n. We want this for every p_i, so we can multiply n by $(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots$

Thus, we end with $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \cdots (1 - \frac{1}{p_n})$.

Make sure you understand why this works.

7.2 Fermat's Little Theorem

Consider a prime p and the set of numbers $1, 2, 3 \dots p-1$. Now, multiply these numbers by a number n. We are left with $n, 2n, 3n \dots n(p-1)$.

These numbers are all different mod p because if they were not, then there are integers $kn \equiv jn \mod p$ and we can divide by n because p and n are co-prime. Thus, we have $k \equiv j \mod p$.

Because these are numbers ranging from 1 to $p-1$, there are no such k and j. Thus, we are assured all the numbers are different mod p

This means that $n, 2n, 3n \cdots n(p-1)$ is a rearrangement of $1, 2, 3 \dots p-1 \mod p$. If we multiply these numbers together, we get $n * 2n * 3n \dots (p-1)n \equiv 1 * 2 * 3 \dots (p-1) \mod p$ Dividing by $1 * 2 * 3 \dots (p-1)$, we get that $n^{p-1} \equiv 1 \mod p$

This theorem only works if $a \not\equiv 0 \mod p$ (can you find a counterexample?)

7.3 Euler's Theorem/Euler's Generalization of FLT

We have proven Fermat's Little Theorem (FLT), but what about if we want to take mod m instead of mod p, where m is not prime? Well, the last step of the proof of FLT, where we divide by $1 * 2 * 3 \dots (p-1)$ is only able to be done because all these numbers are coprime to p, and as we know, mods can only be divided if the number you are dividing by is coprime to the mod.

Well, what if we do just that? What if we line up the numbers that are coprime to m in a list like $1, a_1, a_2 \dots m-1$. We can multiply by n again, and we get $n, n(a_1, n(a_2) \dots n(m-1)$. We know there are $\phi(m)$ numbers in this list, because there are that many numbers coprime to m. The proof of Euler's Generalization of FLT is left as an exercise for the reader.

7.4 Exercises

7.4.1 Easy

1. Let a_n equal $6^n + 8^n$. Determine the remainder upon dividing a_{83} by 49. (AIME)

7.4.2 Medium

1. Finish the proof of Euler's Generalization and show how it relates to FLT (how can FLT be found from it?)

7.4.3 Hard

1. Prove that Euler's Totient function is multiplicative, and under which circumstances? $\phi(m) * \phi(m) = \phi(mn)$
2. Let R be the set of all possible remainders when a number of the form 2^n, n a nonnegative integer, is divided by 1000. Let S be the sum of the elements in R. Find the remainder when S is divided by 1000. (AIME)

8 Wilson's Theorem

Wilson's theorem can be really useful for solving many Number Theory Problems. When solving for a remainder, it is often used in conjunction with modular residues, as the problem would be trivial otherwise. As with the CRT section, we will first start by stating and then proving the theorem. Then we will give some example problems with solutions and as usual, we will end with some exercises.

8.1 The Theorem

Wilson's theorem states that a positive integer $n > 1$ is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Proof: At first glance, it seems that proving the conditional is a really difficult job, but proving the converse shouldn't be that hard. Surprisingly, the situation is exactly opposite. Proofs of the conditional and the converse are included separately below.

Conditional: Assuming n, a composite number, we show a contradiction. If n is a composite number then it has at least one divisor, d, less than n, that is $d \leq n-1$. But since $(n-1)!$ is the product of all positive integers from 1 to $n-1$, the product must contain d and thus be divisible by d. So we have $(n-1)! \equiv 0 \pmod{d}$. Also $(n-1) \equiv 0 \not\equiv -1 \pmod{d}$ since $d|n$, contradicting the hypothesis. So n can't be composite, hence prime.

Converse: Let p be a prime. Consider the field of integers modulo p. By Fermat's Little Theorem, every nonzero element of this field is a root of the polynomial

$$P(x) = x^{p-1} - 1.$$

Since this field has only $p-1$ nonzero elements, it follows that

$$x^{p-1} - 1 = \prod_{r=1}^{p-1}(x - r).$$

Now, either $p = 2$, in which case $a \equiv -a \pmod{2}$ for any integer a, or $p-1$ is even. In either case, $(-1)^{p-1} \equiv 1 \pmod{p}$, so that

$$x^{p-1} - 1 = \prod_{r=1}^{p-1}(x - r) = \prod_{r=1}^{p-1}(-x + r).$$

If we set x equal to 0, the theorem follows.

8.1.1 Examples

1. What is the residue of $\frac{1}{1\cdot 2} \cdot \frac{1}{2\cdot 3} \cdot ... \cdot \frac{1}{11\cdot 12} \pmod{13}$?

Solution: Have the following be congruent to x. Note that the following is equivalent to $x \equiv \frac{12}{(12!)^2} \pmod{13}$. Multiplying both sides by $(12!)^2$ yields $(12!)^2 x \equiv 12 \pmod{13}$. Then, by Wilson's Theorem, $(12!) \equiv -1 \pmod{13}$ so $(12!)^2 \equiv 1 \pmod{13}$. As thus, $(12!)^2 x \equiv (-1)^2 x \equiv x \equiv 12 \pmod{13}$, which gives us our answer.

2. Find the remainder of $(1^3)(1^3 + 2^3)(1^3 + 2^3 + 3^3)...(1^3 + 2^3 + ... + 99^3)$ when divided by 101.

Solution: Note that $(1 + 2 + ... + n)^2 = (1^3 + 2^3 + ... + n^3)$. Have this expression be congruent to x modulo 101. We can rewrite our expression as $\left(\frac{(1\cdot 2)(2\cdot 3)...(99\cdot 100)}{2^{99}}\right)^2 \equiv x \pmod{101}$, or $\frac{(100!)^4}{2^{198}\cdot 100^2} \equiv x \pmod{101}$. Then note that by Fermat's Little Theorem, $2^{100} \equiv 1 \pmod{101}$, so we can multiply both sides by 2^{200} to get $\frac{(100!)^4}{625} \equiv x \pmod{101}$. Applying Wilson's Theorem yields $\frac{1}{625} \equiv x \pmod{101}$, and multiplying by 625 yields $1 \equiv 625x \equiv 19x \pmod{101}$. As thus, we are trying to find a solution x such that $19x + 101y = 1$. We shall apply the extended Euclidean Algorithm.

101=19(5)+6	6=101-19(5)
19=6(3)+1	1=19-6(3)
6=1(6)	

Using the right hand side of the table, we can find (x, y). Note that

$$1 = 19 - (101 - 19(5))(3) = 19(16) - 101(3).$$

As thus, $19 \cdot 16 \equiv 1$, so $x \equiv 16$, which is our answer.

8.2 Exercises

1. Find the remainder of 97! when divided by 101.

2. Find the remainder of $(p-2)!$ when divided by p, provided that p is prime.

3. Find the greatest common factor of $(21!+20), (20!+20)$.

9 Miscellaneous Number Theory

9.1 Floor and Ceiling Functions in Number Theory

The floor of k is the greatest value of n such that $k \geq n$ and n is an integer. This is denoted as $\lfloor k \rfloor$. Similarly, the ceiling of k is the smallest value of m such that $m \geq k$ and m is an integer. This is denoted as $\lceil k \rceil$. Floors and ceilings can be used to express certain functions formally, or as a technique needed to solve a problem.

9.1.1 Examples

1. What is the floor and ceiling of 4.5?

Solution: The largest integer smaller than 4.5 is 4, and the smallest integer larger than 4.5 is 5, so the floor and ceiling of 4.5 respectively are 4 and 5.

2. What is the floor of $1.01^2 - 0.02^2$?

Solution: By difference of squares $1.01^2 - 0.02^2 = (1.03)(0.99)$. Note that $(1.03)(0.99) = 1.03 - 1.03(0.01)$. By now, it should be quite obvious that $1 \leq 1.03 - 1.03(0.01)$, and it is self-explanatory that $2 \geq 1.03 - 1.03(0.01)$, so our floor is 1.

3. Express the largest odd number less than or equal to x as a function of x using ceiling and/or floor functions.

Solution: $f(x) = 2\lceil \frac{x}{2} \rceil - 1$.

Motivation: We want there to be no change from an odd to an even and there needs to be a change from an even to an odd. So we see that this is in terms of a fraction with denominator 2 – we want to have the change happen from even to odd, which sounds like ceiling. Then multiplying by 2 should be obvious, and plugging in values to get the difference yields -1.

9.2 Exercises

9.2.1 Easy

1. Find the value of $\lfloor 4.5 \rfloor + \lceil 6.7 \rceil$.
2. Find the value of $\lfloor 2.25^2 \rfloor - \lfloor 2.25 \rfloor^2$.

9.2.2 Medium

1. Express the largest even number less than or equal to x as a function of x using ceiling and/or floor functions.
2. Describe the set of reals $\{k_1, k_2 ...\}$ such that $\lfloor k_n \rfloor + 1 = \lceil k_n \rceil$.

9.2.3 Hard

1. What is the largest integer value of n such that $1.01^2 - \frac{n^2}{10000}$ is greater than or equal to 1?
2. Find the smallest integer value of n such that $\lfloor 0.3^2 + (0.1n)^2 \rfloor = 1$.
3. What is the smallest value of k such that there is no integer solution n to $\lfloor \frac{n^2}{36} \rfloor = k$?

10 The Pigeonhole Principle

The Pigeonhole Principle is a very simple postulate that has far-reaching applications. It states that, given n items (pigeons) and k slots (pigeonholes), if $n > k$, then there must be one slot with more than one item in it. In addition, there must be one slot with at least $\lceil \frac{n}{k} \rceil$ items and one slot with at most $\lfloor \frac{n}{k} \rfloor$ items.

This makes sense. Try plugging in some numbers. For example, say that $n = 5$ and $k = 2$. Then, we can see obviously that one of the six possibilities below must be satisfied:

Slot 1	Slot 2
5	0
4	1
3	2
2	3
1	4
0	5

Checking back with the principle, we see that all conditions are satisfied.

Please note that this section will be harder than previous sections in the book. This is because the Pigeonhole Principle is almost never used on AIME and never used on AMC, due to its nature. Thus, the practice questions, and examples, will be Olympiad level, or late AIME. The section starts easily, but escalates quickly.

Example 1: Prove that there are at least two people in New York City with the same number of hairs on their head.

At first, this problem seems crazy. How are we ever going to prove this?

But we look at the facts. There are approximately 9 million people in New York City. But the human head has only 75,000 to 175,000 hairs. There are very few people who have more or less than this range. (I'm counting hairs by the number of follicles, so bald people would still have hair.) That's only 100,000 "slots" for number of hairs. Thus, by Pigeonhole, we have that since $100,000 < 9,000,000$, there must be at least one hair slot with more than one person in it, and we are done.

Obviously, this proof is not very rigorous. But it serves as an intuitive example of the power of Pigeonhole. Now, we present a more rigorous example:

Example 2: Show that, if we select $n + 1$ random integers, at least two of them will have the same remainder when divided by n.

Basically, the problem is asking us to prove, that in a group of $n+1$ integers, at least two have the same residue modulo n. There are only n possible residues modulo n, so by Pigeonhole, at least two of those integers must have the same residue.

Extension to Example 2: Prove that for any natural number n, there is a natural number composed entirely of 5s and 0s that is divisible by n.

Until now, these problems have been simplistic and have made sense. Now, let's try working through an olympiad-level problem with Pigeonhole.

Example 3: (2012 USAMO Problem 2) A circle is divided into 432 congruent arcs by 432 points. The points are colored in four colors such that some 108 points are colored Red, some 108 points are colored Green, some 108 points are colored Blue, and the remaining 108 points are colored Yellow. Prove that one can choose three points of each color in such a way that the four triangles formed by the chosen points of the same color are congruent.

When we see congruent shapes and circles, we think of rotation. So let's rotate the circle by $\frac{\pi}{216}$ radians 431 times. Obviously, each red point will overlap every green point once. There are 108 red points overlapping 108 green points each. Thus, the average number of overlapped points per rotation is $\frac{108 \cdot 108}{431}$, which is slightly above 27. Thus, by Pigeonhole, on at least one of those

rotations, we'll have at least 28 overlapped points. So we have shown that we can choose 28 red points and 28 green points such that they form congruent convex 28-gons.

Let's rotate these 28 points $\frac{\pi}{216}$ radians 431 times again, looking at overlapped blue points. The average number of overlapped points per rotation is $\frac{28 \cdot 108}{431}$, which is slightly more than 7. So, by Pigeonhole, on one of those rotations, there will be at least 8 overlapping points. So we've shown that we can choose 8 each of red, green, and blue points such that they form congruent convex octagons.

Finally, we'll rotate these 8 points $\frac{\pi}{216}$ radians 431 times again, looking at overlapped yellow points this time. The average number of overlapped points per rotation this time is $\frac{8 \cdot 108}{431}$, which is slightly more than 2. Thus, using Pigeonhole one last time, we determine that on one of those rotations, there will be at least three overlapping points. So we've shown that we can choose 3 each of red, green, blue, and yellow points such that they form congruent triangles, and we are done.

That example was pretty tricky, and may have confused some readers. So, we'll go a little bit easier now, down to AIME level.

Example 4: (1986 AIME Problem 12, modified) Let S be a set of positive integers, none greater than 15. Suppose no two disjoint subsets of S have the same sum. What is the maximum number of elements that can be in set S?

It's obvious that all sets of 1 and 2 have this property. A little bit of work shows us that many 3 and 4 element sets have this property too. An example is the set $\{11, 13, 14, 15\}$ and its 3 element subsets. So the answer must be at least 4. Let's conjecture that the answer is 5.

Now, we can use Pigeonhole. We see that the maximum sum of a 4 element set is $15 + 14 + 13 + 12 = 54$. We're trying to prove that S cannot contain 6 or more elements. To show this, we can just show that it cannot contain 6 elements, as we can use our process on higher numbers too.

In a 6 element set, there are 6 subsets of size 1, $\binom{6}{2} = 15$ subsets of size 2, $\binom{6}{3} = 20$ subsets of size 3, and $\binom{6}{4} = 15$ subsets of size 4. There are 56 subsets of size 1, 2, 3, or 4. However, every subset of size 4 or lower must have sum ≤ 54 and ≥ 1. There are only 54 possible sums in this range, so by Pigeonhole, at least two must have the same sum.

Now, we have shown that the answer is either 4 or 5. We'll start building a set, then, and see if we can attain 5. We'll start with our example set, $\{11, 13, 14, 15\}$, and see if we can add another number. Working our way down, we see that neither 10 nor 9 work, as $10 + 15 = 11 + 14$ and $9 + 15 = 11 + 13$. Trying 8, though, gives us a valid set. Thus, the answer is 5.

10.1 Exercises

10.1.1 Easy

1. Prove the Extension to Example 2.
2. You have a 2 by 2 square. Prove that is impossible to place 10 dots on the square such that each dot is at least 1 unit away from the other
3. You flip a coin 10 times. What is the minimum number of times you must flip tails so that you will not have flipped heads twice in a row?
4. Prove that of any 52 integers, two can always be found such that the difference of their squares is divisible by 100.

10.1.2 Medium

1. What is the smallest number n, that in any arrangement of n points on the plane, there are three of them making an angle of at most $\frac{\pi}{10}$ radians?
2. Prove that you can't arrange 100 points inside a 13×18 rectangle so that the distance between any two points is at least 2.

10.1.3 Hard

1. Each of eight boxes contains six balls. Each ball has been colored with one of n colors, such that no two balls in the same box are the same color, and no two colors occur together in more than one box. Determine, with justification, the smallest integer n for which this is possible.

2. Two permutations $a_1, a_2, \ldots, a_{2010}$ and $b_1, b_2, \ldots, b_{2010}$ of the numbers $1, 2, \ldots, 2010$ are said to intersect if $a_k = b_k$ for some value of k in the range $1 \leq k \leq 2010$. Show that there exist 1006 permutations of the numbers $1, 2, \ldots, 2010$ such that any other such permutation is guaranteed to intersect at least one of these 1006 permutations.

10.1.4 Insanely Hard

1. Given a set M of 1985 distinct positive integers, none of which has a prime divisor greater than 23, prove that M contains a subset of 4 elements whose product is the 4th power of an integer.

11 Induction

11.1 Introduction to Induction

Induction is a method of proof that is used to show that a certain statement holds for positive integers. The classic analogy is a line of dominoes: If there is a line of dominoes, and one is tipped over, then the rest will fall. The same idea holds in induction: we prove it for a base case, often 1, then we prove that if it holds for k, then it holds for the next value. Thus, since it holds for 1, it holds for 2, and since it holds for 2, it holds for three, and so on to infinity. Induction is a very powerful method of proof that has applications to number theory.

11.1.1 Examples

1. Prove that for all positive integers n then the sum of the first n positive integers is $\frac{n(n+1)}{2}$.

   Solution: We can start at $n = 1$. The sum of the first 1 numbers is just 1. This is true based on our formula: $\frac{1(1+1)}{2} = 1$.
   Now we move to the case $n = k$ which we will assume is true for now. We use it to solve the next step, $n = k + 1$. The sum of the first k integers is $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$. The sum of the first $k + 1$ integers is $1 + 2 + \cdots + k + (k + 1) = \frac{k(k+1)}{2} + (k + 1)$. Simple algebraic manipulation tells us that $\frac{k(k+1}{2} + (k + 1) = \frac{(k+1)(k+2)}{2}$. Thus, given that $n = k$ holds, we know that $n = k+1$ holds. Starting at 1, we now know that 2 works, and from this 3 works, and so on until infinity. Thus, our proof holds. This is the power of induction and we will see how it can apply to Number Theory

11.2 Application to Number Theory

Prove that for every positive integer n there exists an n-digit number divisible by 5^n all of whose digits are odd. (2003 USAMO)

Solution: Since we see that this question is asking us to prove something for all positive integers, we can think of induction starting at 1.

$n = 1$: The only solution is 5
$n = 2$: We only have 75 (none other work)
$n = 3$: We have 375 (the reader is encouraged to prove a few other cases and find some patterns)

$n = k$: Let us assume this case works for now and our number is $B = 5^k * b$, where b is between 1 and 9 inclusive.

$n = k + 1$: If we take the previous number and append a new digit a to the left-hand side,

and the new number A is divisible by 5^{k+1}, then we know that proof holds. Now the challenge is to prove that such a digit exists in every case.

A can be represented as the sum of the new digit and the old number B or $10^k a + 5^k b$. We want this number to be divisible by 5^{k+1}. When we divide, we are left with $5|2a + b$. We can now make a table of values of a that work for values of b. We know that b is between 1 and 9, and that it is odd (otherwise the number will not have all even digits) and that it is not 5 (otherwise we have 5^{k+1} which is a different case)

b	a
1	7
3	1
7	9
9	3

Thus, for each possible value of b, there is a corresponding value of a. The reader is encouraged to play with these constructions of a and b as an exercise.

Here is an exercise for the reader to play with: Show that $\frac{1}{9}(10^n + 3 * 4^n + 5)$ is an integer for all $n \geq 1$ (AMSP)

12 Appendices

12.1 Factorizations Worth Memorizing

Difference of Squares: $x^2 - y^2 = (x + y)(x - y)$

Difference of Cubes: $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$

Sum of Cubes: $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$

Perfect-Square Trinomial: $(ax + b)^2 = a^2x^2 + 2abx + b^2$

Binomial Theorem: $(x + y)^n = \sum_{a=1}^{n} \binom{n}{a} x^a b^{n-x}$

SFFT: $(ax + b)(cy + d) = acxy + adx + bcy + bd$

Sum of Squares: $a^2 + b^2 = (a + bi)(a - bi)$

Sophie-Germaine: $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$

13 From here

If you've gotten through this handout and are looking for a new challenge, here are a few links:

https://artofproblemsolving.com/wiki/index.php?title=Category:Intermediate_Number_Theory_Problems

https://artofproblemsolving.com/school/course/intermediate-numbertheory

https://www.awesomemath.org/product/number-theory-concepts-and-problems/