ORMC AMC 10/12 Training Week 4
Number Theory

April 23, 2023

1 Warm-Up

These problems should be a review of basic concepts, or concepts we have previously discussed.

1. Let k be an even number. Is it possible to write 1 as the sum of the reciprocals of k odd integers?

2. Let n be a positive integer. Prove that $3^{2n} + 1$ is divisible by 2, but not by 4.

3. **(ARML 2003)** Find the largest divisor of 1001001001 that does not exceed 10000.

4. **(HMMT 2002)** If a positive integer multiple of 864 is chosen randomly, with each multiple having the same probability of being chosen, what is the probability that it is divisible by 1944?

5. Determine the number of ordered pairs of positive integers (a, b) such that the least common multiple of a and b is $2^3 5^7 11^{13}$.

6. Prove that there are infinitely many primes of the form $4k - 1$; that is, congruent to 3 modulo 4.

2 The Chicken McNugget Theorem

(More formally known as the Frobenius Coin Theorem)

Theorem 1. (Frobenius Coin Theorem)
Given any two relatively prime positive integers m, n, the largest integer that cannot be written in the form $am + bn$ for nonnegative integers a, b is $mn - m - n$.

2.1 Proof (Exercises)

Proof. Let N be an arbitrary positive integer.

1. Show that if (x_1, y_1) is a solution to $xm + yn = N$, and $m(x_1 - x_2) + n(y_1 - y_2) = 0$, then (x_2, y_2) is also a solution.

2. Show that if (x_1, y_1) and (x_2, y_2) are both solutions to $xm + yn = N$, then $m(x_1 - x_2) + n(y_1 - y_2) = 0$.

3. Let $S = \{0, 1, 2, \ldots, m-1\}$. Show that there exists exactly 1 solution (x_N, y_N) for $xm + yn = N$ such that $y \in S$.

4. Show that $x_N < 0$ in the previous problem if and only if there are no positive integers x, y which satisfy $xm + yn = N$.

5. Show that $mn - m - n$ is the largest N such that there are no positive integers x, y which satisfy $xm + yn = N$. This value N is called the **Frobenius Number** of m and n.

□

For more than 3 values, i.e. (m, n, k) with $\gcd(m, n, k) = 1$, the solution is much more complicated, and was originally solved using continued fractions. There are no known explicit solutions for 4 values in general, but there are some upper bounds.

As you will see in the following exercises, problems may not directly look like the Chicken McNugget Problem, but if you can reframe the problem in such a way that it involves exactly two relatively prime positive integers, then you can use the result we proved above.

2.2 Examples

1. At McDonalds, you can buy McNuggets in packs of 9 or 20. What is the largest number of McNuggets that you cannot buy in one order, with these packs?

2. **(2015 AMC 10B #15)** The town of Hamlet has 3 people for each horse, 4 sheep for each cow, and 3 ducks for each person. Which of the following could not possibly be the total number of people, horses, sheep, cows, and ducks in Hamlet?

2.3 Exercises

1. **(1994 AIME #11)** Ninety-four bricks, each measuring $4'' \times 10'' \times 19''$, are to stacked one on top of another to form a tower 94 bricks tall. Each brick can be oriented so it contributes $4''$ or $10''$ or $19''$ to the total height of the tower. How many different tower heights can be achieved using all ninety-four of the bricks?

2. **(Corollary to Chicken McNugget Theorem)** For any integer k, exactly one of k, $mn - m - n - k$ has no solution in $xm + yn$, where x, y are nonnegative integers. It follows that there are $\frac{mn-m-n}{2}$ positive integers with no nonnegative integer solutions in $xm + yn$.

3. **(2019 AIME #14)** Find the sum of all positive integers n such that, given an unlimited supply of stamps of denominations $5, n$, and $n + 1$ cents, 91 cents is the greatest postage that cannot be formed.

4. **(India TST)** On the real number line, paint red all points that correspond to integers of the form $81x + 100y$, where x and y are positive integers. Paint the remaining integer points blue. Find a point P on the line such that, for every integer point T, the reflection of T with respect to P is an integer point of a different colour than T.

3 Diophantine Equations

The equation we dealt with above is a special case of a more general class of equations, called **linear diophantine equations**. A linear diophantine equation is any equation of the form:

$$a_1x_1 + \cdots + a_nx_n = b,$$

where $a_1, \ldots, a_n, b$ are fixed integers, and we focus only on solutions where all of the x_i's are integers as well. Notice that with $n = 2$, and nonnegative x_i's, we have precisely the Chicken McNugget Problem.

Theorem 2. A linear diophantine equation is solvable if and only if $\gcd(a_1, \ldots, a_n) \mid b$.

3.1 Proof (Exercises)

Proof. Let $d = \gcd(a_1, \ldots, a_n)$.

1. Show by a simple argument that if $d \nmid b$, then there are no solutions.

2. Note that if $d \mid b$, then we can WLOG consider only equations with $\gcd(a_1, \ldots, a_n) = 1$. Show that for $n = 1$, such an equation is always solvable.

3. Let $n \geq 2$, and assume, for induction, that the theorem holds for $n - 1$. Let $d' = \gcd(a_1, \ldots, a_{n-1})$. Show that if $d' = 1$, then we have a solution where $x_n = 0$.

4. WLOG, we may assume $d' > 1$. Show that there exists an x_n which solves the equation modulo d'.

Note that by the existence of such an x_n, it follows inductively that the theorem holds for n, since

$$a_nx_n \equiv b \pmod{d'} \implies b - a_nx_n \equiv 0 \pmod{d'} \implies d' \mid (b - a_nx_n).$$

□

If you are familiar with **Bezout's Identity**, note that it is the special case of this theorem, where $n = 2$.

For solving general Diophantine equations, remember the following:

- A common, powerful strategy for solving general Diophantine equations is to consider the equation modulo m. The point is that if there are no solutions modulo m, then there will be no solutions at all.
- Usually, there will be only a few small solutions, if any. So, you can usually find the solutions by testing some small values. The rest of your work will be to show that no other solutions exist for larger values.
- If there happens to be a large number of solutions, they will most often come in one or more regular pattern(s)/families. So, you can use induction to generate the family of solutions, starting with any smaller solutions that you find manually.

3.2 Examples

1. Prove that the equation

$$(x+1)^2 + (x+2)^2 + \cdots + (x+2001)^2 = y^2$$

is not solvable.

2. Find all pairs (p, q) of prime numbers such that

$$p^3 - q^5 = (p+q)^2$$

3.3 Exercises

1. Solve the equation

$$6x + 10y - 15z = 1.$$

2. Prove that the equation $x^5 - y^2 = 4$ has no solutions in integers.

3. Show that there are no integers a, b, c for which $a^2 + b^2 - 8c = 6$.

4. Solve in the integers the Diophantine equation $x^4 - 6x^2 + 1 = 7 \cdot 2^y$.

5. Determine all triples (x, y, z) of integers satisfying the equation

$$3x + 4y + 5z = 6.$$

6. Let n be a positive integer. Suppose that there are 666 ordered triples (x, y, z) of positive integers satisfying the equation

$$x + 8y + 8z = n.$$

Find the maximum value of n.

4 Advanced Problems

(General Number Theory)

1. **(China 2017)** Let $m \geq n > 1$ be integers. Let $a_1, a_2, \ldots, a_n$ be n distinct and relatively prime numbers not exceeding m. Show that for any real x, there exists an i for which
$$||a_i x|| \geq \frac{2}{m(m+1)}||x||$$
where $||x||$ denotes the distance between x and the nearest integer to x .

2. **(IMO 2017)** An ordered pair (x, y) of integers is a primitive point if the greatest common divisor of x and y is 1. Given a finite set S of primitive points, prove that there exist a positive integer n and integers $a_0, a_1, \ldots, a_n$ such that, for each (x, y) in S, we have:
$$a_0x^n + a_1x^{n-1}y + a_2x^{n-2}y^2 + \cdots + a_{n-1}xy^{n-1} + a_ny^n = 1.$$

3. **(Putnam 2022)** Let p be a prime number greater than 5. Let $f(p)$ denote the number of infinite sequences $a_1, a_2, a_3, \ldots$ such that $a_n \in \{1, 2, \ldots, p-1\}$ and $a_n a_{n+2} \equiv 1 + a_{n+1} \pmod{p}$ for all $n \geq 1$. Prove that $f(p)$ is congruent to 0 or 2 (mod 5).

4. **(USAMO 2023)** Let $n \geq 3$ be an integer. We say that an arrangement of the numbers $1, 2, \cdots, n^2$ in a $n \times n$ table is row-valid if the numbers in each row can be permuted to form an arithmetic progression, and column-valid if the numbers in each column can be permuted to form an arithmetic progression. For what values of n is it possible to transform any row-valid arrangement into a column-valid arrangement by permuting the numbers in each row?