Senior Math Circles  
October 8, 2008  
Number Theory I

Opening Problem
Suppose that you are given a row consisting of three O’s followed by three X’s:

O O O X X X

Your task is to obtain a row in which the O’s and X’s alternate:

O X O X O X  or  X O X O X O

Here are the rules:

• You make a succession of moves.
  
• Each move takes a consecutive pair of letters and moves them to either end of
  the row or into a pair of adjacent vacant slots.

• The final row does not need to occupy the same slots as the beginning row, but
  there must be no gaps between adjacent letters.

Find a solution.

Next, find a solution that uses the fewest possible number of moves.

Is it possible to find a solution that ends with O X O X O X?

Repeat this process starting with O O O O X X X.

Repeat again starting with O O O O O X X X X.

Can you determine a general process when starting with 4m X’s and 4m O’s?
Number Theory

Number theory is the study of the properties of numbers.

For integers $a$ and $b$, with $a < b$, there exist integers $q$ and $r$ with $0 \leq r < a$ such that $b = qa + r$.
The integer $q$ is called the quotient, and $r$ is the remainder.

Divisibility:

Definition:
For integers $a$ and $b$, if there exists an integer $q$ such that $b = qa$, then we say $a$ divides $b$, and we write $a|b$.
Note that $x|0$ for all integers $x$, since if we let $q = 0$, then $qx = 0x = 0$.

Properties of Divisibility:

1. If $a|b$ and $b|c$, then $a|c$.
2. If $a|b$ and $a|c$, then $a|bx + cy$ for all integers $x$ and $y$.

Proof of (1):
If $a|b$ and $b|c$, then by definition of divisibility, there exists an integer $q_1$ such that $b = q_1a$, and another integer $q_2$ such that $c = q_2b = q_2(q_1a) = (q_2q_1)a$.
Since $q_2q_1$ is an integer, therefore $a|c$.

Important Formulae:

1. $(a - b)|a^n - b^n$ for all positive integers $n$.
2. $(a + b)|a^n + b^n$ if $n$ is odd.
3. $(a + b)|a^n - b^n$ if $n$ is even.

Problems:

1. Prove $3|n^3 - n$.
2. Prove $35|3^{6n} - 2^{6n}$.
3. Prove $n^2 + 3n + 5$ is never divisible by 121.
Greatest Common Divisor:

Definition:
Let \(a\) and \(b\) be integers. Then the gcd of \(a\) and \(b\), written \(\gcd(a, b)\), is the non-negative integer \(d\) such that:

i) \(d|a\) and \(d|b\).

ii) For all integers \(c\) such that \(c|a\) and \(c|b\), then \(c|d\).

If \(\gcd(a, b) = 1\), then \(a\) and \(b\) are called relatively prime, or coprime.

Theorem:
\(\gcd(a, b) = \gcd(a, a + b)\)

Proof:
Let \(d = \gcd(a, b)\). We know \(d|a\) and \(d|b\), so \(d|(a + b)\). Now, let \(c\) be any integer such that \(c|a\) and \(c|(a + b)\). Therefore, we have that \(c|(a + b) - a = b\). Since \(c|a\), \(c|b\), and \(\gcd(a, b) = d\), by definition \(c|d\). Therefore, \(d = \gcd(a, a + b)\), and so \(\gcd(a, b) = \gcd(a, a + b)\).

Example: Find gcd(24, 162).
Solution:
We have \(\gcd(a, b) = \gcd(a, a + b)\). Let \(c = a + b\), so \(c - a = b\).
Now, \(\gcd(a, c - a) = \gcd(a, c)\).
So, \(\gcd(24, 162) = \gcd(24, 162 - 24)\)
\[= \gcd(24, 138)\]
\[= \gcd(24, 138 - 24)\]
\[= \gcd(24, 114)\]
\[= \gcd(24, 90)\]
\[= \gcd(24, 66)\]
\[= \gcd(24, 42)\]
\[= \gcd(24, 18)\]
\[= \gcd(6, 18)\]
\[= \gcd(6, 12)\]
\[= \gcd(6, 6)\]
\[= 6\]
Euclidean Algorithm:
If we have two integers \( a \) and \( b \) with \( a < b \), we know \( \gcd(a, b-a) = \gcd(a, b) \) and \( b = qa + r \), so by repeated subtraction of \( a \) from \( b \) we get \( \gcd(a, b) = \gcd(a, r) \).

Example: Find \( \gcd(54, 315) \)
Solution:
\[ 315 = 5(54) + 45, \text{ so } \gcd(54, 315) = \gcd(54, 45). \]
Now, \( 54 = 1(45) + 9, \text{ so } \gcd(54, 45) = \gcd(9, 45). \)
Now, \( 45 = 5(9) + 0, \text{ so } \gcd(9, 45) = \gcd(9, 0) = 9. \)
Therefore \( \gcd(54, 315) = 9. \)

Theorem:
Let \( d | a \) and \( d | b \), then \( \gcd(a, b) = d \) if and only if there exist integers \( x \) and \( y \) such that \( ax + by = d. \)

Example:
\( \gcd(2, 3) = 1, \text{ since } 1|2, 1|3, \text{ and } 3(1) + 2(-1) = 1. \)

Prime Numbers:
A positive integer with exactly 2 positive divisors is called a prime number.
1 is not prime.

Sophie Germain Formula:
\[ a^4 + 4b^4 = (a^2 + 2b^2 - 2ab)(a^2 + 2b^2 + 2ab) \]

Example: Determine if \( 4^{545} + 5^{400} \) is prime.
Solution:
We have
\[ 4^{545} + 5^{400} = (5^{100})^4 + 4 \cdot (4^{136})^4 \]
\[ = [(5^{100})^2 + 2(4^{136})^2 - 2(5^{100})(4^{136})][(5^{100})^2 + 2(4^{136})^2 + 2(5^{100})(4^{136})] \]
Therefore \( 4^{545} + 5^{400} \) is not prime.
The Euler Phi(\(\phi\)) Function:

Definition:
\(\phi(n)\) is defined as the number of integers \(x\) with \(1 \leq x < n\) such that \(\gcd(n, x) = 1\). That is, \(n\) and \(x\) are relatively prime.

Some examples are \(\phi(2) = 1\), \(\phi(6) = 2\) and \(\phi(97) = 96\).

Problem:
What is \(\phi(96059601)\)?
Problem Set

1. For what integers $n$ does $97|2^{4n} + 3^{4n}$?

2. Prove that $n^5 - 5n^3 + 4n$ is divisible by 120, for every integer $n$.

3. Let $aabb$ be a 4-digit perfect square. Find $a$ and $b$.

4. Prove that any two consecutive positive integers are relatively prime.

5. Prove that if $\gcd(a, c) = 1$, then $\gcd(ab, c) = \gcd(b, c)$.

6. Determine if $1000 \cdots 0001$ with 1961 0’s is prime or composite.

7. Prove that if $N$ is any positive integer and $a$ is relatively prime to $N$, then $N|a^{\phi(N)} - 1$.

8. Prove that $1^k + 2^k + \cdots + n^k$, where $n$ is any positive integer and $k$ is an odd integer, is divisible by $1 + 2 + \cdots + n$.

9. Prove that there exists an infinite number of prime numbers in the arithmetic sequence $3, 7, 11, 15, 19, \ldots$.