Introduction to Number Theory

Walker Kroubalkian, Oshadha Gunasekara, Ricky Shapley

October 26, 2015

1 Primes

A prime is a number with two factors: 1 and itself. For example, 13 is a prime number because its factors are 1 and 13. There are infinitely many primes and only one even prime: 2.

Primes form the basis of all numbers. Every number can be written as the product of one or more primes. Commonly we denote this as $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \ldots \cdot p_n^{a_n}$, where $p_1, p_2, p_3, \ldots p_n$ are distinct primes and $a_1, a_2, a_3, \ldots a_n$ are their exponents.

Examples:

1. Prime factorize 642.
2. How many pairs of primes exist with sum 103?
3. Prove that there are infinitely many primes.

2 Divisibility

An integer a is considered divisible by another integer b if and only if b is a divisor of a. That is, $\frac{a}{b} = m$, for some integer m. We can denote this as $b|a$.

Divisibility Rules
2: If the units digit of n is even, then $2|n$.
3: If the sum of the digits of n is divisible by 3, then $3|n$.
4: If the last two digits of n are divisible by 4, then $4|n$.
5: If the units digit of n is 0 or 5, then $5|n$.
6: If n is divisible by 2 and 3, then $6|n$.
7: If $n - 2(n \pmod{10})$ is divisible by 7, then $7|n$.
8: If the last three digits of n are divisible by 8, then $8|n$.
9: If the sum of the digits of n is divisible by 9, then $9|n$.
10: If the units digit of n is 0, then $10|n$.
11: If the difference of the sum of the alternating digits is divisible by 11, then $11|n$.

Examples:

1. Find all a and b such that $11|a42b8$.
2. Find the sum of all $a + b$ such that $8|7485ba$.

3 Modular Arithmetic

3.1 Identities

We can define modular arithmetic in the following way: if $a = cx + b$ for some integers a, b, c, and x, then $a \equiv b \pmod{c}$. Inversely, if $a \equiv b \pmod{c}$ then a leaves a remainder of b when divided by c. With this definition, we are able to derive a few identities.

Theorem 1. *$a \equiv b \pmod{c}$ if and only if $c|a - b$. (Note: this can be seen in the Euclidean Algorithm).*

Theorem 2. *If $a \equiv b \pmod{e}$ and $c \equiv d \pmod{e}$, then $a\#c \equiv b\#d \pmod{e}$, where $\#$ denotes addition, subtraction, or multiplication.*

Theorem 3. *If $a \equiv b \pmod{c}$, then $a^n \equiv b^n \pmod{c}$ for integer exponents n.*

Theorem 4. *If $e|c$ and $a \equiv b \pmod{c}$, then $a \equiv b \pmod{e}$.*

Theorem 5. *If a and b satisfy $ab \equiv 1 \pmod{c}$, then $a^{-1} \equiv b \pmod{c}$. We consider b to be the modular inverse of a.*

Theorem 6. *If $a + b \equiv 0 \pmod{n}$, then $a \equiv -b \pmod{n}$.*

Examples:

1. Find the remainder when $2001^{2001^{2001}}$ is divided by 1000.
2. Prove that it is impossible for the square of an integer to leave a remainder of 2 when divided by 3, or a remainder fo 2 or 3 when divided by 4.

3.2 Chinese Remainder Theorem

Modular arithmetic also provides us with a very useful theorem called the Chinese Remainder Theorem.

Theorem 7. ***The Chinese Remainder Theorem**. If m is relatively prime to n, then there is a one to one correspondence between the residues of $a \pmod{m}$ and $a \pmod{n}$ and the residue of $a \pmod{mn}$.*

In other words, you can break the modulus (the part which you are dividing by) up into its distinct prime factors when trying to find a remainder.

Example: Sloan has a certain number of cultists which he wishes to divide into groups. He finds that if the cultists were divided int groups of 5, there would be 1 left over. If the cultists were divided into groups of 7, there would be 3 left over. If the cultists were divided into groups of 8, there would be 4 left over. Finally, if the groups were divided into groups of 9, there would be 5 left over. Given that Sloan's cult has diminished and now has less than 3000 cultists, what is the total number of cultists?

4 Numerical Bases

A numerical base is a number which defines the set of digits used to write a number. In normal mathematics, we use base 10 for most of our calculations, which has 10 unique digits that are used to write every number (0, 1, 2 ... 8, 9). Bases are denoted by subscripts, 31_5 reads as 31 base 5. To convert between bases, it is usually simplest to convert to and from base 10.

Theorem 8. *For a number* $(a_1a_2a_3...a_{n-1}a_n)_b$ *where every* a_n *is a digit, the corresponding number in base 10 is* $a_n + a_{n-1} \cdot b^1 + a_{n-2} \cdot b^2 + \ldots + a_{n-k} \cdot b^k + \ldots + a_1 \cdot b^{n-1}$.

Theorem 9. *To convert a number from base 10 to another base, you use a repeated algorithm:*

1: Divide the desired base into the number you are trying to convert.
2: Write the quotient with a remainder.
3: Repeat this division process using the whole number from the previous quotient.
4: Repeat this division until the number in front of the remainder is only zero.
5: The answer is the remainders read from the bottom up.

Examples:

1. Convert 282_{10} to base 9.
2. Convert 212_3 to base 10.

5 Multiplicative Functions

A multiplicative function is a function $f(x)$ such that when m and n are relatively prime, $f(m) \cdot f(n) = f(mn)$ for all integers m and n. Multiplicative functions satisfy the following properties:

Theorem 10. *If* $f(x)$ *is multiplicative,* $f(1) = 1$ *or* $f(x) = 0$ *for all* x.

Theorem 11. *If* $f(x)$ *is multiplicative, and the prime factorization of* n *is* $p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \ldots p_n^{a_n}$*, then* $f(n) = f(p_1^{a_1}) \cdot f(p_2^{a_2}) \cdot f(p_3^{a_3}) \ldots f(p_n^{a_n})$.

There are some well-known multiplicative functions which often show up in competitions.

5.1 The Divisor Function

The Divisor Function, commonly referred to as $d(n)$ counts the number of factors of n. It can be computed by adding 1 to each of the exponents in the prime factorization of n and multiplying all of the results. That is, if $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_n^{a_n}$, then $d(n) = (a_1 + 1)(a_2 + 1)(a_3 + 1) \ldots (a_n + 1)$.

Example: Find the total number of factors of $37748736 = 2^{22} \cdot 3^2$.

5.2 The Sum Function

The Sum Function, commonly referred to as $\sigma(n)$ finds the sum of the factors of n. It can be computed by finding the sum of the factors of each of the prime powers in the prime factorization of n and multiplying the results. That is, if $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_n^{a_n}$, then $\sigma(n) = (p_1^{a_1} + p_1^{a_1-1} + \ldots p_1 + 1)(p_2^{a_2} + p_2^{a_2-1} + \ldots p_2 + 1) \ldots (p_n^{a_n} + p_n^{a_n-1} + \ldots p_n + 1)$.

Example: Find the sum of the factors of 236.

5.3 Euler's Totient Function

The Totient Function, commonly referred to as $\phi(n)$ finds the number of integers between 0 and $n-1$ inclusive which are relatively prime to n. It can be computed by multiplying n by $\frac{p-1}{p}$ for all distinct prime factors p of n. That is, if $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \ldots \cdot p_n^{a_n}$, then $\phi(n) = n \cdot (\frac{p_1 - 1}{p_1}) \cdot (\frac{p_2 - 1}{p_2}) \ldots (\frac{p_n - 1}{p_n})$.

Euler's Totient Theorem has a very important application to number theory in Euler's Totient Theorem.

Theorem 12. ***Euler's Totient Theorem.*** *If a and b are relatively prime to each other, then* $a^{\phi(b)} \equiv 1 \pmod{b}$.

This tells us that the modular inverse of $a \pmod{b}$ is congruent to $a^{\phi(b)-1} \pmod{b}$.

Example: Let $f_0 = 1$, and for $n \geq 1$, let $f_n = 3^{f_{n-1}}$. Find the remainder when f_{2015} is divided by 2520.