1 Divisors and multiples

1.1 Divisors and Greatest Common Divisors (GCD)

1.1.1 Divisors

The divisors d of a natural number n are the natural numbers such that $\frac{n}{d} \in \mathbb{N}$.

For example, for 6 the divisors are $1, 2, 3, 6$.

Divisors cannot be bigger than the number they are dividing.

1.1.2 Universal divisors

For any number $n \in \mathbb{N}^+$:

$\frac{n}{n} = 1$

$\frac{n}{1} = n$

Both 1 and n are divisors.

1.1.3 Common divisors

A common divisor is a number which is a divisor to two supplied numbers.

1.1.4 Greatest common divisor

The greatest common divisor of 2 numbers is as the name suggests.

So $GCD(18, 24) = 6$

1.2 Multiples and Lowest Common Multiples (LCM)

1.2.1 Multiples

The multiple of a number is it added to itself iteratively.

The multiples of 18 for example are:

$[18, 36, 54, 72, 90, ...]$

And for 24:

$[24, 48, 72, 96, 120, ...]$

1.2.2 Common multiples

1.2.3 Lowest common multiple

The lowest common multiple of 2 numbers is again as the name suggests.

So $LCM(18, 24) = 72$.

1.3 Remainders

1.3.1 Remainders

Division is defined between natural numbers. However there are many cases where this division does not map to a natural number. For example:

$\frac{7}{3}$

We can divide 6 of the 7 by 3, giving 2 with 1 remaining.

Alternatively we can divide 3 of the 7 by 3, giving 1 with 4 remaining

Or we could divide 0 of the 7 by 3 giving 0 with 7 remaining.

The remainder refers to the lowest possible number - in this case 1.

2 Prime numbers

2.1 Prime numbers and composite numbers

2.1.1 Definition

A prime number is a number which does not have any divisors other than 1 and itself.

By convention we do not refer to 0 or 1 as prime numbers.

2.1.2 Identifying prime numbers

Divisors must be smaller than the number. As a result it is easy to identify early prime numbers, as we can try to divide by all preceding numbers.

2.1.3 Examples of prime numbers

$[2, 35, 7, 11, 13, ...]$

2.1.4 Composite numbers

Composite numbers are numbers that are made up through the multiplication of other numbers.

They are not prime.

2.2 Relatively prime numbers

2.3 Euler's totient function

This functions counst numbers up to n which are relatively prime

eg for 10 we have 1, 3, 7, 9

So $\phi(10) = 4$

2.4 Congruence

5 and 11 are congrument $\mod 3$

If $a \mod (n) = bmod(n)$ then a and b are congruent mod n.

2.5 Coprimes

Greatest commod divisor is 1.

2.6 Residue systems

2.6.1 Least residue system modulo n

This is the set of numbers from 0 to $n - 1$.

2.6.2 Complete residue system

This a set of numbers none of which are congruent $\mod n$. That is, for no pair $\{a, b\}$ does $a \mod (n) = bmod(n)$

2.6.3 Reduced residue system

This is a complete residue system where all numbers are relatively prime to n.

2.7 Euler's theorem

2.8 Fermat's little theorem

2.9 Pseudoprimes

3 The Fundamental Theorem of Arithmetic

3.1 Euclidian division

Euclidian division is the theory for any pair of natural numbers, we can divide one by the other and have a remainder less than the divisor. Formally: $\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^+, \exists q \in \mathbb{N}, \exists r \in \mathbb{N}[(a = bq + r) \land (0 \leq r < b)]$

Where $\mathbb{N}^+$ refers to natural numbers excluding 0.

That is, every natural number a is a multiple q of any other natural number b, plus another natural number r less than the other natural number b.

These are unique. For each jump in q, r falls by b. As the range of r is b there is only one solution.

$17 = 2.8 + 1$

$9 = 3.3 + 0$

3.2 Bezout's identity

For any two non-zero natural numbers a and b we can select natural numbers x and y such that

$ax + by = c$

The value of c is always a multiple of the greatest common denominator of a and b.

In addition, there exist x and y such that c is the greatest common denominator itself. This is the smallest positve value of c..

Let's take two numbers of the form $ax + by$:

$d = as + bt$

$n = ax + by$

Where $n > d$. And d is the smallest non-zero natural number form.

We know from Euclidian division above that for any numbers i and j there is the form $i = jq + r$.

So there are values for q and r for $n = dq + r$.

If r is always zero that means that all values of $ax + by$ are multiples of the smallest value.

$n = dq + r$ so $r = n - dq$.

$r = ax + by - (as + bt)q$

$r = a(x - sq) + b(y - tq)$

This is also of the form $ax + by$. Recall that r is the remainder for the division of d and n, and that $d = ax + by$ is the smallest positive value.

r cannot be above or equal to d due to the rules of euclidian division and so it must be 0.

As a result we know that all solutions to $ax + by$ are multiples of the smallest value.

As every possible $ax + by$ is a multiple of d, d must be a common divisor to both numbers. This is because $a.0 + b.1$ and $a.1 + b.0$ are also solutions, and d is their divisor.

So we know that the smallest positive solution is a common mutliple of both numbers.

We now need to show that that d is the largest common denominator. Consider a common denominator c.

$a = pc$

$b = qc$

And as before:

$d = ax + by$

So:

$d = pcx + qcy$

$d = c(px + qy)$

So $d \geq c$

3.3 Euclid's lemma

3.3.1 Statement

If a prime number p divides product $a.b$ then p must divide at least of one of a or b.

3.3.2 Proof

From Bezout's identity we know that:

$d = px + by$

Where p and b are natural numbers and d is their greatest common denominator.

Let's choose a prime number for p. There are no common divisors, other than one. As a result there are exist values for x and y such that:

$1 = px + by$

Now, we are trying to prove that if p divides $a.b$ then p must divide at least one of a and b, so let's multiply this by a.

$a = pax + aby$

We know that p divides pax, and p divides ab by definition. As a result p can divide a.

3.4 Fundamental Theorem of Arithmetic

3.4.1 Statement

Each natural number is a prime or unique product of primes.

3.4.2 Proof: existance of each number as a product of primes

If n is prime, no more is needed.

If n is not prime, then $n = ab$, $a, b \in \mathbb{N}$.

If a and b are prime, this is complete. Otherwise we can iterate to find:

$n = \prod_{i=1} p_i$

3.4.3 Proof: this product of primes is unique

Consider two different series of primes for the same number:

$s = \prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$

We need to show that $n = m$ and $p = q$.

We know that p_i divides s. We also know that through Euclid's lemma that if a prime number divides a non-prime number, then it must also divide one of its components. As a result p_i must divide one of q.

But as all of q are prime then p_i=q_j.

We can repeat this process to to show that $p = q$ and therefore $n = m$.

3.5 Existence of an infinite number of prime numbers

3.5.1 Existence of an infinite number of prime numbers

If there are a finite number of primes, we can call the set of primes P.

We identify a new natural number a by taking the product of existing primes and adding 1.

$a = 1 + \prod_{p \in P} p$

From the fundamental theorem of arithmetic we know all numbers are primes or the products of primes.

If a is not a prime then it can be divided by one of the existing primes to form number n:

$\frac{\prod^n p_i + 1}{p_j} = n$

$\frac{p_j \prod_{i \neq j}^n p_i + 1}{p_j} = n$

$\prod_{i \neq j}^n p_i + \frac{1}{p_j} = n$

As this is not a whole number, n must prime.

We can do this process for any finite number of primes, so there are an infinite number.

3.6 Gödel numbering

Gödel numbering assigns a unique number to each formula.

To contruct this we first assign a natural number to each symbol.

This gives us a sequence:

$\{x_1, x_2, x_3, ..., x_n\}$

We can assign a unique number to this by using the first n prime numbers.

$2^{x_1} 3^{x_2} 5^{x_3} ...$

This number can then be prime factored to recover the sequence, and therefore the formula.