Some Properties of Numbers

Notation: **D**(a , b) is the greatest common divisor of a and b.

$a \div b$ means a is divisible by b

$a \not\div b$ means a is not divisible by b

a, b, c, n, s, t etc are integers; p, q etc. are primes

Fundamental theorems:

Theorem 1.1 **D(na, nb) = n . D(a, b)**

For example: if D(21, 35) = 7 then D(63, 105) must be 21

This is pretty self evident

Theorem 1.2 **D(a, b) = D(a, $|a-b|$)**

For example: if D(21,35) = 7 then D(21,14) must also be 7

This is pretty self evident

Theorem 1.3 **If $s \,.\, t \div p$ then either $s \div p$ or $t \div$ p**

Suppose that $s.t \div p$ but that $s \not\div p$ and that $t \not\div p$

Let $s \,.\, t = c \,.\, p$

Since $s \not\div p$ D(p , s) = 1

By Theorem 1.1 t . D(p , s) = D(pt , $s \,.\, t$) = t

Since $t \not\div p$ D($p \,.\, t$, $s \,.\, t$) $\not\div p$

Since $s \,.\, t = c \,.\, p$ D($p \,.\, t$, $c \,.\, p$) $\not\div p$

This is obviously a contradiction, therefore at least one of the initial assumptions must be false

Theorem 1.4 **If $n = p \,.\, s = q \,.\, t$ $(p \neq q)$ then $t \div p$**

Suppose that $n = p \,.\, s = q \,.\, t$ $(p \neq q)$

Since $p \,.\, s \div p$

it follows that $q \,.\, t \div p$

By Theorem 1.3 either $q \div p$ or $t \div p$

Since q is prime $t \div p$

Theorem 1.5 **$(x^n - 1) \div (x - 1)$**

$$(x-1)(x^{(n-1)} + x^{(n-2)} + x^{(n-3)} \ldots\ldots + 1)$$

$$= x^n + x^{(n-1)} + x^{(n-2)} \ldots\ldots + x - x^{(n-1)} - x^{(n-2)} - x^{(n-3)} \ldots\ldots - x - 1$$

$$= \boldsymbol{x^n - 1}$$

Theorem 1.6 **$1 + x + x^2 + x^3 + x^{(n-1)} = (x^n - 1) / (x - 1)$**

See theorem 1.5

The Fundamental Theorem of Arithmetic

Suppose n has two factorizations:

$$n = p \,.\, p' \,.\, p'' \ldots = p \,.\, s$$
$$= q \,.\, q' \,.\, q'' \ldots = q \,.\, t$$

(We can assume that the list of factors is mutually exclusive because if any of the factors are equal, we can divide them out and start again with a new value of n. If we are able to prove that the new n has unique factors, then so must the original N because N is uniquely equal to $n \,.\, p' \,.\, p''$.. where $p \,.\, p' \,.\, p''$.. are the factors we have divided out)

By Theorem 1.4 $q' \ldots = t$ must be divisible by p

but if $q' \,.\, q'' \ldots$ is divisible by p

By Theorem 1.4 $q'' \ldots$ must be divisible by p

Repeat this process until there is only one prime left to test $q^{\#}$

Since $q^{\#}$ is prime $q^{\#} \not\div p$

This is a contradiction so n cannot have two unique factorizations.

An alternative proof of the FTA

Suppose n is the smallest number which has two factorizations:

$$n = p.p'.p'' \ldots = p.s = q.q'.q'' \ldots$$

where the primes are in increasing order of magnitude.

(Note that it is easy to see that both lists must contain more than one prime and the two lists must be mutually exclusive)

since $p^2 < n$ and $q^2 < n$ (p and q being the smallest primes)

it follows that $p \,.\, q < n$

Let $m = n - p.q$

(because $p.q < n$, m will be a positive integer, and because n was deemed to be the smallest number with two factorizations, m must have a unique factorization)

hence $m = p \,.\, p' \,.\, p'' \ldots - p \,.\, q = p \,.\, (p' \,.\, p'' \ldots - q)$

also $m = q \,.\, q' \,.\, q'' \ldots - p \,.\, q = q \,.\, (q' \,.\, q'' \ldots - p)$

hence $m \div p \,.\, q$

now $n = m + p \,.\, q = p \,.\, q \,.\, x + p \,.\, q = p \,.\, q \,.\, (x+1)$

It follows that $p' \,.\, p'' \ldots = q \,.\, (x + 1)$

This number is smaller than n and also has two different factorizations. This contradicts the original assumption that n was the smallest number with two factorizations. It follows that there are no such numbers.

The number of primes is infinite

Suppose the number of primes is finite.

Consider the product of all the primes n

$$n = p \,.\, p' \,.\, p'' \ldots = p \,.\, a$$

Now consider the number $m = n + 1$.

Since m is not on the list of primes, m must be composite and equal to the product of several of the primes p, p', p'' etc.

Let $m = p \,.\, b$

By Theorem 1.1 $D(n\,,\, m) = D(p \,.\, a\,,\, p \,.\, b) = p \,.\, D(a\,,\, b) >= p$

By Theorem 1.2 $D(n\,,\, m) = D(n\,,\, 1) = 1$

But $p \neq 1$

This is a contradiction so the number of primes cannot be finite.

The gap between two primes can be arbitrarily large

Since $n!$ is divisible by all numbers up to n

it follows that $n! + 2 \div 2$, $n! + 3 \div 3$, $n! + 4 \div 4$ etc. up to $n! + n \div n$

There exist $n - 1$ consecutive composite numbers between $n! + 2$ and $n! + n$

But n can be arbitrarily large

The number of twin primes is infinite

This conjecture is unproven

√2 is irrational

Suppose that √2 is rational; ie $\sqrt{2} = a / b$ where $D(a\,,\, b) = 1$

Square $a^2 = 2.b^2$

By Theorem 1.4 $a \div 2$

Let $a = 2.c$

$(2.c)^2 = 2.b^2$

$2.c^2 = b^2$

By Theorem 1.4 $b \div 2$

Hence $D(a\,,\, b)$ is at least 2.

This is a contradiction so √2 must be irrational

$\sqrt[t]{s}$ is either integer or irrational

Suppose that $\sqrt[t]{s} = a/b$ where $D(a, b)=1$

$a^t = s.b^t$

Now either $\sqrt[t]{s}$ is an integer or s is composed of several primes; hence

By Theorem 1.4 $a \div s$

Let $a = s.c$

$(s.c)^t = s.b^t$

$s.c^t = b^t$

By Theorem 1.4 $b \div s$

This is a contradiction

If $M_p = 2^n - 1$ is prime then n is prime

Let $M_p = 2^n - 1$ where M_p is prime (such a number is called a Mersenne prime)

Suppose that n is composite; ie let $n = a.b$

$M_p = 2^{a.b} - 1 = (2^a)^b - 1$

By Theorem 1.5 This is divisible by $2^a - 1$

This is a contradiction as M_p is prime;

therefore n cannot be composite.

Numbers of the form $N = a^n - 1$ can only be prime if $a = 2$ (or $n = 1$)

By theorem 1.5 $(a^n - 1) \div (a - 1)$

If $(a^n - 1)$ is prime, then $(a - 1)$ must be equal to 1 or N

If $(a - 1) = 1$ then $a = 2$

If $(a - 1) = N$ then $n = 1$

If $M_p = 2^n - 1$ is prime then $P = 2^{(n-1)} . M_p$ is a perfect number

Let $2^n - 1 = M_p$

The factors of **P** are $1, 2, 4, \ldots 2^{(n-1)}$ and $p, 2p, 4p, \ldots 2^{(n-1)}p$ (including $2^{(n-1)}p$ which is **P** itself)

By theorem 1.6 $\Sigma\{1, 2, 4, \ldots 2^{(n-1)}\} = (2^n - 1) / (2 - 1) = 2^n - 1$

So the sum of all the factors of **P** (including **P**) is $2^n - 1 + (2^n - 1)p$

But $2^n - 1$ is p

so the sum of all the factors of **P** (including **P**) is $p + (2^n - 1)p$

which equals $2^n p$

Now $\mathbf{P} = 2^{(n-1)}p$ which is exactly half of $2^n p$

so the sum of all the factors of **P** (excluding **P**) is therefore equal to **P** itself - which is the definition of a perfect number

For example, take $n = 3$; $M_p = 7$; **P** = 28. The factors of **P** are 1, 2, 4, 7 & 14

Fermat's Little Theorem

Consider the operation of doubling in modulus-N arithmetic.

Suppose $N = 7$. This generates the following cycles:

$0 \rightarrow 0$

$1 \rightarrow 2 \rightarrow 4 \rightarrow 1$

$3 \rightarrow 6 \rightarrow 5 \rightarrow 3$

It is obvious that whatever the modulus, 0 always $\rightarrow$ 0

It is also obvious that every starting number will always generate a cycle but it is not true that every starting number is included in the cycle which it generates.

For example, consider $N = 6$

$[0 \rightarrow 0]$

$1 \rightarrow [2 \rightarrow 4 \rightarrow 2]$

$3 \rightarrow [0 \rightarrow 0]$

$5 \rightarrow [4 \rightarrow 2 \rightarrow 4]$

The numbers 1, 3 and 5 are not part of any cycle.

In general, the process of doubling takes a number a to either $2a$ or $2a - N$. If N is even, then both these numbers are even. This explains why, if N is even, no odd number can be part of a cycle.

Let us consider the case N is odd. In this case $2a$ is even and $2a - N$ is odd. This gives us a clue as to how the operation of doubling can be reversed. If a is even, halve it. If a is odd, add N and halve. (It is easy to see that both of these will always return a unique number between N and N - 1)

It follows from this that, if N is odd, **all** numbers from 0 to N are part of one and only one unique cycle. For example, if $N = 7$, there are three cycles; the first contains one number [0] and the other two contain three numbers each [$1 \rightarrow 2 \rightarrow 4$] and [$3 \rightarrow 5 \rightarrow 6$]. We can summarise this by saying that **all cycles are mutually exclusive** and **every number is included in one and only one cycle**.

Here is a list of the cycles relating to the first few odd numbers

1 [0]

3 [0] [$1 \rightarrow 2$]

5 [0] [$1 \rightarrow 2 \rightarrow 4 \rightarrow 3$]

7 [0] [$1 \rightarrow 2 \rightarrow 4$] [$3 \rightarrow 6 \rightarrow 5$]

9 [0] [$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 7 \rightarrow 5$] [$3 \rightarrow 6$]

11 [0] [$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 5 \rightarrow 10 \rightarrow 9 \rightarrow 7 \rightarrow 3 \rightarrow 6$]

13 [0] [$1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 3 \rightarrow 6 \rightarrow 12 \rightarrow 11 \rightarrow 9 \rightarrow 5 \rightarrow 10 \rightarrow 7$]

15 [0] [$1 \rightarrow 2 \rightarrow 4 \rightarrow 8$] [$3 \rightarrow 6 \rightarrow 12 \rightarrow 9$] [$5 \rightarrow 10$] [$7 \rightarrow 4 \rightarrow 13 \rightarrow 11$]

A close look at these examples will suggest the following theorems:

Let us restrict ourselves to the cases when ***N* is a prime** (p)

Any starting number a becomes either $2a$ or $2a - p$. On the next doubling, there are four possibilities: $4a$, $4a - p$; $4a - 2p$ or $4a - 3p$. After n doublings, the result will be $2^n a - zp$ where $0 \leq z < n$.

When the cycle is complete, the result is equal to the starting number ie

$$2^n a - zp = a$$

hence $$a(2^n - 1) = zp$$

Now we know that a (the starting number) is less than p (the modulus) so a cannot be divisible by p. It follows that $2^n - 1$ must be divisible by p. This is obviously true for the degenerate cycle $[0 \rightarrow 0]$ because $n = 1$

In general there will be a finite number of cycles (excluding the degenerate one) with period i, j, k etc. where $i + j + k + \ldots = p - 1$ (the number of numbers less than p excluding 0)

Consider the product

$$(2^i - 1).(2^j - 1) = 2^{(i+j)} - 2^i - 2^j + 1 = (2^{(i+j)} - 1) - (2^i - 1) - (2^j - 1)$$

Since the last two terms are divisible by p, it follows that $(2^{(i+j)} - 1)$ is also divisible by p.

Applying this theorem to all the cycles we see that $(2^{(i+j+k+\ldots)} - 1)$ is divisible by p.

But as we have seen, $i + j + k + \ldots = p - 1$ so

> If p is prime then
> $2^{(p-1)} - 1$ is divisible by p

This is Fermat's little theorem.

It is frequently used as a test for prime numbers. If you want to know whether a number p is prime, you calculate $[2^{(p-1)} - 1] \text{Mod } p$. If the answer is not zero, you can reject p as it must be composite. If the result is zero, there is a good chance that p is prime. In fact between 2 and 7919 there are 1000 prime numbers but only 18 numbers which pass Fermat's test that are not prime.

The theorem is also linked to Pascal's triangle:

2^1	1	$= 1$
2^2	$1 + 2 + 1$	$= 4$
2^3	$1 + 3 + 3 + 1$	$= 8$
2^4	$1 + 4 + 6 + 4 + 1$	$= 16$
2^5	$1 + 5 + 10 + 10 + 5 + 1$	$= 32$
2^6	$1 + 6 + 15 + 20 + 15 + 6 + 1$	$= 64$
2^7	$1 + 7 + 21 + 35 + 35 + 21 + 7 + 1$	$= 128$

It is easy to see that the sum of all the coefficients in a line is equal to a power of 2 by considering the expansion of $(1 + 1)^n$.

In general, the i^{th} term of the expansion of $(a + b)^n$ is

$$\frac{n!}{i!.(n-i)!} = \frac{n.(n-1).(n-2)...(n-i+1)}{1.2.3...i}$$

Now if n is prime p it is obvious that the factor n is going to appear in every term (except the first and last which are both unity). eg 2^3, 2^5, 2^7 etc. In other words, $2^p - 2$ is divisible by p. This is equivalent to saying that $2^{(p-1)} - 1$ is divisible by p.

The above analysis suggests an elegant proof which leads to a more general form of Fermat's little theorem.

Suppose that $a^p - a$ is divisible by p. Consider $b^p - b$ where $b = a + 1$

$$\begin{aligned} b^p - b &= (a+1)^p - (a+1) \\ &= \left(a^p + \frac{p(p-1)}{1.2} a^{(p-1)} + \frac{p(p-1)(p-2)}{1.2.3} a^{(p-2)} + \ldots + 1 \right) - a - 1 \end{aligned}$$

Now if p is prime, all the middle terms in the expansion are divisible by p. The two 1's cancel so all that is left is $a^p - a$ which we have assumed is also divisible by p. It follows that if $a^p - a$ is divisible by p, then $b^p - b$ is divisible by p also.

To prove the theorem for all values of a it is only necessary to show that $1^p - 1$ is divisible by p – a fact which is obvious as 0 is divisible by every number (because the remainder is also 0).

Hence we have proved that if p is prime, $a^p - a$ is divisible by p. If a is not itself divisible by p, then we can conclude that:

If p is prime then $a^{(p-1)} - 1$ is divisible by p for all values of a which are not multiples of p