Section 6 Lecture 36 – Euler's totient function

Coprime

Two positive integers are said to be *coprime* if the only factor they have in common is 1. For example, 15 and 8 are coprime as they do not share any common factors (apart from 1) but 12 and 9 are not coprime as they both have a factor of 3.

By this definition 1 is coprime to every number as it has no factors apart from itself 1, so cannot share a factor with any other number.

Euler's totient function

Given a positive integer n, we define *Euler's totient function* $\varphi(n)$ to be the number of integers from 1 to $n - 1$ that are coprime to n.

For example, $\varphi(12) = 4$ since the numbers from 1 to 11 that are coprime to 12 are 1, 5, 7 and 11 – everything else has a factor in common.

There is no known fast way to work this out in general – you really need to just check every possibility. So for example to work out $\varphi(15)$ you just list the numbers 1, 2, …14 and count how many are coprime (you might find it easier to cross out those that aren't coprime so share a factor) – you should find that 1, 2, 4, 7, 8, 11, 13 and 14 are coprime, so there are eight coprime numbers and hence $\varphi(15) = 8$

If you know the prime factorisation of n then you can deduce $\varphi(n)$ – as an example if $n = pq$ for primes p and q, then $\varphi(n) = (p - 1)(q - 1)$.

Theorem

If p and q are distinct primes then the Euler totient function $\varphi(n) = (p - 1)(q - 1)$.

Proof:

Recall that the Euler totient function is the number of integers in the range 1 to (n -1) that are coprime to n. Since $n = pq$ where p and q are prime, this is its prime factorisation. So the only numbers that are not coprime to n must have a factor of at least one of either p or q.

Our intention will be to eliminate the integers that are not coprime (so have a factor in common with n), leave us with all the coprime integers.

There are n - 1 numbers to consider (1 up to $n - 1$, remember we don't count n itself). Since $n = pq$ then $n - 1 = pq - 1$. So we have $pq - 1$ possible numbers to consider.

Of these, the numbers p, $2p$, $3p$, $4p$, ……, $(q - 1)p$ are all the multiples of p, that is all the numbers that have p as a factor. There next multiple of p is $qp = n$ which is not in the range of numbers we are considering. So these numbers have a factor in common with n (namely p) and there are $(q - 1)$ of them, and so we will need to eliminate $q - 1$ numbers

Similarly, there are $(p - 1)$ numbers less than n which have a common factor of q (the numbers q, $2q$, $3q$, $4q$, ……, $(p - 1)q$) and so we need to eliminate those $(p - 1)$ numbers.

Every other number must be coprime to n because the only two prime factors of n are p and q and we've already accounted for all the multiples of those – nothing else can have a factor in common.

So, the total numbers less than n which are coprime to n can be worked out by subtracting the multiples of p and q from the total $pq - 1$ number, which gives

$\varphi(n) = (pq - 1) - (q - 1) - (p - 1) = pq - p - q + 1 = (p - 1)(q - 1)$ as required.