Math From Scratch Lesson 21: Totients

W. Blaine Dowler

May 21, 2012

Contents

1 Definition of Totients

The *totient* of a number n is the number $\phi(n)$ of integers less than or equal to n which are also coprime to n. Note that the totient may equal 1, but not n. In the ambiguous case, $\phi(1) = 1$.

For example, let us compute $\phi(6)$. Manually checking the numbers 1, 2, 3, 4 and 5, we find that two of them (1 and 5) are coprime to 6, so that $\phi(6) = 2$.

2 General Properties

2.1 $\phi(p)$

The totient function for a prime number p is $\phi(p) = p - 1$. This is fairly straightfoward to work out: there are $p - 1$ integers that are at least 1 but less than p, and as p is prime, they are all coprime to p.

2.2 $\phi(p^n)$

The totient function for a power of a prime $\phi(p^n)$ can be calculated by taking the total $p^n - 1$ integers that are at least 1 but less than p^n, and subtracting the $p^{n-1} - 1$ multiples of p within that range. Thus,

$$\phi\left(p^n\right) = p^n - 1 - \left(p^{n-1} - 1\right) = p^n - p^{n-1} = p^n\left(1 - \frac{1}{p}\right)$$

2.3 $\phi(mn)$

The totient of a product is more challenging to calculate. The Chinese Remainder Theorem provides a way to calculate $\phi(mn)$ relatively quickly on the condition that m and n are coprime. The Chinese Remainder Theorem ensures that, for some value of a, if we have $\gcd(a, mn) = 1$ then both $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$.

Now we define the set $\{a : a \equiv 1\,(mod\ mn)\}$. The size of this set is $\phi(mn)$, the number of integers ranging from 1 to $mn - 1$ which are coprime to mn. By the Chinese Remainder Theorem, the size of this set must be identical to the set defined by $\{a : a \equiv 1\,(mod\ m)\ \&a \equiv 1\,(mod\ n)\}$. This set has the size $\phi(m) \cdot \phi(n)$. Therefore, $\phi(mn) = \phi(m) \cdot \phi(n)$, provided m and n are coprime. This property of the totient function is the *multiplicative* property.

So, how do we calculate $\phi(mn)$ when m and n are not coprime? Well, when we multiply the pair of integers together, we get a new integer. This new integer has a prime factorization of some kind. It is this prime factorization that we use to compute $\phi(mn)$. So, given that $mn = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$, we can calculate $\phi\left(mn\right) = \phi\left(p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}\right)$ instead.

Well, we know how to deal with $\phi\left(p^n\right)$ when p is prime, and how to deal with $\phi(mn)$ when m and n are relatively prime. Once we have the prime factorization,

we find that

$$\begin{aligned}
\phi(mn) &= \phi(p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}) \\
&= \phi(p_1^{e_1})\,\phi(p_2^{e_2})\,\phi(p_3^{e_3}) \dots \phi(p_k^{e_k}) \\
&= p_1^{e_1}\left(1-\frac{1}{p_1}\right) p_2^{e_2}\left(1-\frac{1}{p_2}\right) p_3^{e_3}\left(1-\frac{1}{p_3}\right) \dots p_k^{e_k}\left(1-\frac{1}{p_k}\right) \\
&= p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right) \dots \left(1-\frac{1}{p_k}\right) \\
&= mn\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right) \dots \left(1-\frac{1}{p_k}\right)
\end{aligned}$$

We can now calculate the totient for nonprime numbers. For example, let us calculate $\phi(120)$. The prime factorization of 120 is $120 = 2^3 \cdot 3 \cdot 5$, so we can apply the above definition to find

$$\phi(120) = 120\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 120\frac{1}{2}\frac{2}{3}\frac{4}{5} = 32$$

2.4 Sums of Totients

A surprising result is that, if D is the set of all divisors d of n, then

$$\sum_D \phi(d) = n$$

For example, 6 is divisible by 1, 2, 3 and 6: $\phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$.

This is proven using Lagrange's Theorem, introduced back in lesson 9. In short, Lagrange's theorem states that, if a group of size n has a subgroup, then the size of the subgroup d is a divisor of n. Let us now show that all such subgroups are partitions of the set $\{1, 2, 3, \dots n\}$ to complete the proof.

Let us look at the cyclic group C_n, using addition as the operation. This is the group formed by the elements $\{0, 1, 2, 3, \dots n-1\}$. The generators of this group are those which cannot divide n; i.e. they are coprime to n. Thus, the number of generators of this group is $\phi(n)$. Let us examine the number of unique subgroups which may be formed.

If $n = 6$, for example, the subgroup $\{0, 3\}$ is cyclic with two members, and can be generated by 3. Either 2 or 4 can generate $\{0, 2, 4\}$, and 0 generates the trivial $\{0\}$. The other elements (1 and 5) generate the complete group, and

not proper subgroups; there are two such elements, just as $\phi(6) = 2$. Each subgroup of order d can be generated by $\frac{n}{d}$ possible generators. Thus, the sum $\sum_D \phi(d) = d \cdot \frac{n}{d} = n$, and the proof is complete.

3 Properties in Modular Algebras

The study of totients here has been motivated by a result known as Euler's Theorem, which is the basis of an utterly critical step in the RSA encryption algorithm. The theorem is as follows:

Theorem 3.1 $a^{\phi(n)} \equiv 1 \, (mod \; n)$ *if and only if* a *and* n *are coprime.*

To prove this, we must prove that, if $\gcd(a, n) = 1$, then the numbers ranging from 1 to $n-1$ which are coprime to n form a cyclic subgroup. (If $\gcd(a, n) \neq 1$, then a and n are not coprime and the theorem does not apply.) To establish this, we test the four group axioms.

3.1 Identity

As $\gcd(1, n) = 1$ regardless of n, we can guarantee the existence of the identity element.

3.2 Closure

This follows directly from the the definition of factors and the fundamental theorem of arithmetic (lesson 15): if $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.

3.3 Associativity

The associativity of elements is inherited from the properties of $\mathbb{Z}$ and modular arithmetic. If a, b, c are in the group, then $(ab)\, c = a\, (bc)$.

3.4 Inverses

The existence of inverses follows from a previous result about modular arithmetic from lesson 19: if $\gcd(a, n) = 1$, then a is a unit modulo n. If it is a unit, then it has an inverse.

Thus, the group of elements coprime to n is a cyclic group of order $\phi(n)$. Euler's theorem follows on the basis that any element a of a cyclic group of order k satisfies $a^k = 1$ within the cyclic group.

3.5 Example: $\phi(18)$

Let us examine $\phi(18)$ as an example. The numbers 1, 5, 7, 11, 13 and 17 are those coprime to 18 in the range from 1 to 17. We can build a multiplication table showing that these are a cyclic group mod 18 as follows:

$\cdot$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Every element appears once per row and once per column. Therefore, this is a cyclic group.

4 Next

The next lesson details the RSA encryption algorithm.