MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough

Two proofs of $\varphi(n) = n \prod_{p|n}(1 - 1/p)$

1 First proof

First, a very useful combinatorial tool:

Lemma 1.1 (Sieve formula)**.** *If $A_1, \dots A_n$ are finite subsets of some set S, then*

$$|A_1 \cup \dots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n| .$$

Proof. Let's compare how many times each $x \in S$ is counted on the two sides. If x is in exactly m of the sets A_i, with $1 \le m \le n$, then, on the left, it is counted once. On the right, in the first sum it is counted m times, in the second sum it is subtracted $\binom{m}{2}$ times, then in the third sum it is added $\binom{m}{3}$ times, and so on, up to $(-1)^{m-1}\binom{m}{m}$. It is not counted in intersections with more than m sets. So, we need to show that

$$1 = \binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \dots + (-1)^{m-1}\binom{m}{m} .$$

This can be done with combinatorial tricks, but the most elegant way is to notice that

$$0 = (1-1)^m = \binom{m}{0} - \binom{m}{1} + \binom{m}{2} - \dots + (-1)^m \binom{m}{m} ,$$

and we are done. □

We now take $A_p := \{i \ : \ 1 \le i \le n, \ p \,|\, i\}$, for all primes $p \le n$. Clearly, $\varphi(n) = n - \left|\bigcup_{p|n} A_p\right|$. By the sieve formula, this is $n - \sum_{p|n} n/p + \sum_{p \ne q\,|\,n} n/(pq) - \dots$, which is just the product with the brackets opened up, as desired. □

2 Second proof

Lemma 2.1. *If p is a prime and $k \in \mathbb{Z}_+$, then $\varphi(p^k) = p^k - p^{k-1}$.*

Proof. This is pretty clear: every pth number falls out. □

Lemma 2.2. *If $\gcd(n, m) = 1$, then $\varphi(nm) = \varphi(n)\,\varphi(m)$.*

Proof. This follows from the Chinese Remainder Theorem, which we will discuss later.

Alternatively (well, the content is basically the same), with a sieve-type argument one can show

$$(n - \varphi(n))m + (m - \varphi(m))n - (n - \varphi(n))(m - \varphi(m)) = mn - \varphi(mn),$$

and rearranging gives the desired formula. □

For $n = p_1^{k_1} \cdots p_m^{k_m}$, factorization into distinct prime factors, by the two lemmas we have

$$\varphi(n) = \prod_{i=1}^{m} \varphi(p_i^{k_i}) = \prod_{i=1}^{m} \left(p_i^{k_i}(1 - 1/p_i)\right) = n \prod_{i=1}^{m} (1 - 1/p_i)\,,$$

and we are done. □