

1. THE EULER FUNCTION

We moved on to a new topic.

(1.1) **Definition.** Let $m \geq 2$ be an integer. We define $\phi(m)$ to be the number of integers a in the range $1 \leq a \leq m$ such that $\gcd(a, m) = 1$. The function ϕ is called the *Euler ϕ -function*.

(1.2) **Question.** For $m = 1, 2, \dots, 16$, find all values of a between 1 and m such that $\gcd(a, m) = 1$. Use this to compute $\phi(m)$. What patterns or conjectures can you make about the ϕ -function?

Kevin filled in the table for us::

m	list of all a with $1 \leq a \leq m$ such that $\gcd(a, m) = 1$	$\phi(m)$
1	1	1
2	1	1
3	1,2	2
4	1,3	2
5	1,2,3,4	4
6	1,5	2
7	1,2,3,4,5,6	6
8	1,3,5,7	4
9	1,2,4,5,7,8	6
10	1,3,7,9	4
11	1,2,3,4,5,6,7,8,9,10	10
12	1,5,7,11	4
13	1,2,3,4,5,6,7,8,9,10,11,12	12
14	1,3,5,9,11,13	6
15	1,2,4,7,8,11,13,14	8
16	1,3,5,7,9,11,13,15	8

(1.3) **Conjecture.** (Alex) If n is a prime integer then $\phi(n) = n - 1$

This conjecture is definitely supported by the examples and also easy to prove. In fact for all primes p , and for all integers n we showed that $\gcd(n, p) = 1$ or $\gcd(n, p) = p$. Since $\gcd(n, p) = 1$ for all $n < p$ then $\phi(p) = p - 1$.

Jay proposed the following conjecture, which was harder to settle.

(1.4) **Conjecture.** If $n = 2^k$ for some integer k then $\phi(2^k) = 2^{k-1}$.

We tried a lot for this one. We tried induction but it did not really work. We noticed that for every integer n the $\gcd(n, 2^k) = 1$ or 2^s , with $s < k$. In fact, Jay noticed that $\gcd(n, 2^k) = 1$ if and only if the n is odd and so it is a matter to count how many odd numbers there are before 2^k . Of course everybody said 2^{k-1} , because half of the numbers before 2^k are even and half are odd. But are we really sure? Can we prove that half of the integers are odd and half are even. In fact it is not trivial. To prove that two sets have the same *cardinality* (which in case of a finite set means that they have the same number of elements), we need to build a bijective function. Here there are the basic definitions:

- (1) A **function** between two sets A and B associates each element of A to only one element of the set B .
- (2) A function f is **surjective** if for every element y in B there exists an element x in A such that $f(x) = y$.
- (3) A function f is **injective** if every two different elements of A are associated to different elements in B . (in math symbols it means that if $f(x) = f(y)$ then $x = y$).
- (4) A function f is bijective if it is surjective and injective.

Back to $\phi(2^k)$. We want to construct a bijective function from the odd numbers which are less than 2^k to the even numbers which are less than 2^k . For every odd number $x \leq 2^k$, we define $f(x) = x + 1$. It is a function. It is surjective because for every even number $y \leq 2^k$, we consider $y - 1$ which is odd and $f(y - 1) = (y - 1) + 1 = y$. It is also injective since if $f(x_1) = f(x_2)$, then $x_1 + 1 = x_2 + 1$; and by cancellation we obtain $x_1 = x_2$. So we have a bijective function between odd numbers and even numbers less or equal than 2^k , this says that we have the same number of even and odd numbers less or equal than 2^k . Therefore $\phi(2^k) = 2^{k-1}$.

(1.5) **Homework.** Show that the rationals and the integers have the same cardinality.

Let's go back to the Euler function. Eric proposed the following:

(1.6) **Conjecture.** for every prime p , $\phi(p^l) = p^l - p^{l-1}$.

We tried to prove it for $p = 3$. The argument was almost the same as for $p = 2$. We are counting all the integers x that are less than 3^k and such that $\gcd(x, 3^k) = 1$. This means that we are counting all the integers x less than 3^k which are not multiple of 3. We are counting all the integers x less or equal than 3^k such that the remainder of the division by 3 is zero. We divide the integers less or equal than 3^k into three sets:

$$\begin{aligned} A &= \{0 < x \leq 3^k \text{ such that } 3^k = 3a, \text{ for some integer } a\} \\ B &= \{0 < x \leq 3^k \text{ such that } 3^k = 3a + 1, \text{ for some integer } a\} \\ C &= \{0 < x \leq 3^k \text{ such that } 3^k = 3a + 2, \text{ for some integer } a\} \end{aligned}$$

We are counting how many elements there are in the sets B and C . We will construct two bijective functions $f : A \rightarrow B$ and $g : A \rightarrow C$. If we manage to do so then the number of elements in the sets A and B will be $\frac{2}{3}3^l$, which is also $\phi(3^l)$. Define $f(x) = x - 2$ and $g(x) = x - 1$, it is an exercise to check that f and g are two bijective functions.

We left the generalization as an exercise for next time:

(1.7) **Homework.** Prove that $\phi(p^l) = p^l - p^{l-1}$.

The following conjecture (Jay and Alex) will be the last hard step to be able to compute the ϕ function for every integer:

(1.8) **Conjecture.** Let p and q two different primes, then $\phi(pq) = \phi(p)\phi(q)$.

We leave the proof of the conjecture for the last class. We will need the Chinese remainder theorem, which will be presented by Chris and Eric. The following classes will be project presentations, according to the following schedule:

- (1) *Tuesday 4th December* Project presentation: Eric–Chris.

- (2) *Thursday 6th December* Project presentation: Kevin–Danny, Kelsey–Sara.
- (3) *Tuesday 11th December* Project presentation: Alex–Matt, Jay–Emily.
- (4) *Thursday 13th December* Last Day of Class, last test due, we will also finish to compute the *phi* function.