MATH 13150: Freshman Seminar
Unit 10

1. Relatively prime numbers and Euler's function

In this chapter, we are going to discuss when two numbers are relatively prime, and learn how to count the numbers from 1 to n that share no common prime factors with n. This will be needed later for the RSA algorithm.

1.1. **Relatively prime.** We will say two numbers a and b are *relatively prime* if their greatest common divisor is 1.

Remark 1.1. *Two numbers a and b are relatively prime* $\iff$
- *1. No number bigger than 1 divides a and b*
- *2. No prime number divides a and b*
- *3. There is no prime number that appears in the prime factorizations of both a and b.*

For example, 28 and 15 are relatively prime. There are many ways we can see this. The easiest is to note that $28 = 2^2 \cdot 7$ and $15 = 3 \cdot 5$ are the prime factorizations of 28 and 15, and there is no prime appearing in both prime factorizations.
If you really enjoy the Euclidean algorithm, you could work out the steps to get:
$28 = 15 + 13$
$15 = 13 + 2$
$13 = 6 \cdot 2 + 1$
Since we found that 1 was a remainder, we know $1 = \gcd(15, 28)$, so 28 and 15 are relatively prime. It is reassuring to know that we get the same answer whichever way we decide the question of whether 15 and 28 are relatively prime. In practice, we just use the easiest way. Since we can find the prime factorizations of 28 and 15 in a moment, there is no need to use the Euclidean algorithm here.
The Euclidean algorithm is useful if we want to know whether 2091 and 2143 are relatively prime. You probably can't factor these numbers quickly, but the Euclidean algorithm is easy to work out:
$2143 = 2091 + 52$
$2091 = 40 \cdot 52 + 11$
$52 = 4 \cdot 11 + 8$
$11 = 8 + 3$
$8 = 2 \cdot 3 + 2$
$3 = 2 + 1$
so $\gcd(2091, 2143) = 1$. You could actually skip the last few steps by noting that $\gcd(2091, 2143) = \gcd(2091, 52) = \gcd(52, 11)$, and you can probably see that $\gcd(52, 11) = 1$ since 11 is prime and doesn't divide 52.
MORAL: If you can find prime factorizations of a and b, then you can decide if a and b are relatively prime easily. If not, the Euclidean algorithm is a reliable method.

EXAMPLE: Are 30 and 38 relatively prime?

The answer is no. To see this, note that 2 divides 30 and 2 divides 38, so using condition 2. above, we see that 30 and 38 are not relatively prime.

EXAMPLE: Are 55 and 90 relatively prime?

Again, no. 5 divides both 55 and 90.

EXAMPLE: Are 201 and 4329 relatively prime?

No. 3 divides 201 since it divides $2+0+1 = 3$, and 3 also divides 4329 since it divides $4+3+2+9 = 18$.

EXAMPLE: Are 32 and 2431 relatively prime?

Yes (finally). $32 = 2^5$ has 2 as its only prime factor. 2 does not divide 2431 since 2431 is odd. It follows that no prime can divide both 32 and 2431, so they are relatively prime.

Note that prime and relatively prime are different conditions. We can say that a number is prime, but two numbers can be relatively prime whether or not either is prime. For example, $10 = 2 \cdot 5$ and $33 = 3 \cdot 11$ are relatively prime.

To see that these different criteria for determining whether two numbers are relatively prime coincide is pretty easy. Let's see why two numbers a and b are relatively prime $\iff$ no prime appears in both of their prime factorizations. Certainly, if $\gcd(a, b) = 1$, then by the criterion for computing $\gcd(a, b)$ at the bottom of page 8 from Unit 9, then no prime could appear in the prime factorizations of a and b. On the other hand, if no prime appears in the prime factorizations of a and b, then it is clear by the method of computing $\gcd(a, b)$ at the bottom of page 8 from Unit 9 that $\gcd(a, b) = 1$.

Similar arguments show that the other criteria in Remark 1.1 are equivalent.

1.2. **The Euler ϕ-function.** In this section, we'll think about the problem:

PROBLEM: Pick a number n. How many numbers from 1 to n are relatively prime to n?

Remark 1.2. *We denote the number of numbers from* 1 *to* n *by* $\phi(n)$*. The symbol* ϕ *is a Greek letter usually pronounced "fee" (at least by me. You can check with a friend fluent in Greek). This symbol* $\phi(n)$ *was found by the Swiss mathematician Leonhard Euler. The name "Euler" is pronounced more or less the same as "oiler".*

Let's try out some examples.

COMPUTE $\phi(4)$.

To solve this, list the numbers up to 4: $1, 2, 3, 4$. Since $4 = 2^2$, 1 and 3 are relatively prime to 4, but 2 and 4 are not. So the numbers from 1 to 4 relatively prime to 4 are $1, 3$. Since there are two numbers on the list, the answer is $\phi(4) = 2$.

COMPUTE $\phi(12)$.

The answer is $\phi(12) = 4$. To see this, note that $12 = 2^2 \cdot 3$, so a number is relatively prime to 12 $\iff$ neither 2 nor 3 divide 12. The numbers from 1 to 12 not divisible by 2 or 3 are $1, 5, 7, 11$, and there are 4 numbers on this list. So $\phi(12) = 4$.

COMPUTE $\phi(11)$.

The answer is $\phi(11) = 10$. Since 11 is prime, none of the numbers from $1, 2, 3, \ldots, 10$ share a prime factor with 11, while 11 does share a prime factor with 11. So $\phi(11) = 10$ since there are 10 numbers from 1 through 10.

The same argument works with any prime number p. The numbers from 1 to p relatively prime to p are $1, \ldots, p-1$. Since there are $p-1$ numbers on this list, $\phi(p) = p - 1$.

Remark 1.3. *If p is a prime number, than $\phi(p) = p - 1$.*

For example, $\phi(23) = 22$ since 23 is prime, and $\phi(103) = 102$ since 103 is prime.

Let's try computing $\phi(21)$. The prime factorization of 21 is $21 = 3 \cdot 7$. We can compute $\phi(21)$ by listing the numbers from 1 to 21 and counting the numbers that are not multiples of 3 or 7. An easy way to do that is to first cross out multiples of 3:

$1, 2, \not{3}, 4, 5, \not{6}, 7, 8, \not{9}, 10, 11, \not{12}, 13, 14, \not{15}, 16, 17, \not{18}, 19, 20, \not{21}$

and then crossing out also multiples of 7:

$1, 2, \not{3}, 4, 5, \not{6}, \not{7}, 8, \not{9}, 10, 11, \not{12}, 13, \not{14}, \not{15}, 16, 17, \not{18}, 19, 20, \not{21}$

There are 12 numbers left on the list, so $\phi(21) = 12$.

You could do the same thing for any number, but computing $\phi(200)$ by this method would take awhile. In the next section, we'll learn a simple formula for computing $\phi(n)$.

1.3. **Formula for computing $\phi(n)$.**

TO COMPUTE $\phi(n)$ (due to Euler):

Step 1: Find the prime factorization of n and make a list of the different primes dividing n.

Step 2: Start with n and for each of the primes p on your list, multiply by $\dfrac{p-1}{p}$.

The result is $\phi(n)$.

EXAMPLE: Compute $\phi(200)$.

Factor $200 = 2^3 \cdot 5^2$ into a product of primes. The primes dividing 200 are 2 and 5. Now apply Step 2 to get:

$$\phi(200) = 200 \cdot \frac{2-1}{2} \cdot \frac{5-1}{5} = 200 \cdot \frac{1}{2} \cdot \frac{4}{5} = 80.$$

EXAMPLE: Compute $\phi(420)$.

To solve this, factor $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, so the primes dividing 420 are $2, 3, 5, 7$. Now apply Step 2 to get:

$$\phi(420) = 420 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 96,$$

so $\phi(420) = 96$.

EXAMPLE: Compute $\phi(15750)$.

Since $15750 = 2 \cdot 3^2 \cdot 5^3 \cdot 7$, the primes dividing 15750 are $2, 3, 5, 7$. It follows that

$$\phi(15750) = 15750 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 3600.$$

As you can see, we can easily compute $\phi(n)$ even when n is really big, provided we know the prime factorization of n. This formula of Euler's is a major labor-saving device.

In the next section, we'll give an argument explaining why this formula for computing $\phi(n)$ works. For now, let's check that the formula works in some of the examples we worked out in the last section.

EXAMPLE: Compute $\phi(11)$ using the formula.

The prime factorization of 11 is $11 = 11^1$, so 11 is the only prime dividing 11. By the formula for computing $\phi(n)$, we get

$$\phi(11) = 11 \cdot \frac{10}{11} = 10,$$

which agrees with the answer we found in the last section.

EXAMPLE: Compute $\phi(12)$.

Since $4 = 2^2$, 2 is the only prime dividing 4, so

$$\phi(4) = 2^2 \cdot \frac{1}{2} = 2,$$

which agrees with our previous answer.

EXAMPLE: Compute $\phi(21)$.

Since $21 = 3 \cdot 7$, 3 and 7 are the primes dividing 7, so

$$\phi(21) = 21 \cdot \frac{2}{3} \cdot \frac{6}{7} = 12,$$

which again agrees with the answer we got in the last section.

The formula seems to work in examples, which is reassuring. I'll close this section with two comments:

(1) Never forget that $\phi(n)$ counts the numbers from 1 to n relatively prime to n.

(2) A really common mistake for students to make is to forget to factor the numbers completely as a product of primes. Do NOT make the mistake of writing $20 = 4 \cdot 5$ and saying that $\phi(20)$ should then be $20 \cdot \frac{3}{4} \cdot \frac{4}{5} = 12$. This gives the wrong answer, because we know the right answer is 8. The point is we have to factor 20 completely, as $20 = 2^2 \cdot 5$, so $\phi(20) = 20 \cdot \frac{1}{2} \cdot \frac{4}{5} = 8$.

1.4. **Why this works.** Let's see how to compute $\phi(175)$ in two different ways. Since $175 = 5^2 \cdot 7$, we can see in a flash that

$$\phi(175) = 175 \cdot \frac{4}{5} \cdot \frac{6}{7} = 120.$$

Now let's try to compute it without using the formula.

We should list the numbers from 1 to 175 and cross out all multiples of 5 or 7. But we know how to do this already!! We're trying to count the numbers from 1 to 175 that are multiples of 5 or 7. Let's say this number is N. Then by the subtraction principle, the number of numbers left should be $175 - N$. Let's see if this equals 120.

We certainly know that the # of numbers from 1 to 175 that are multiples of 5 or 7 is:

# of numbers that are multiples of 5
+ # of numbers that are multiples of 7
- # of numbers that are multiples of 5 and 7

Since joint multiples of 5 and 7 are multiples of 35, we can rewrite this as:

# of numbers that are multiples of 5
+ # of numbers that are multiples of 7
- # of numbers that are multiples of 35

There are $\frac{175}{5} = 35$ numbers from 1 to 175 that are multiples of 5 (as we learned to do in Unit 1).

There are $\frac{175}{7} = 25$ numbers from 1 to 175 that are multiples of 7.

There are $\frac{175}{35} = 5$ numbers from 1 to 175 that are multiples of 35.

Putting this together, we see that there are:

$35 + 25 - 5 = 55$ numbers from 1 to 175 that are multiples of 5 or 7, so there are:

$175 - 55 = 120$ numbers from 1 to 175 that are not divisible by 5 or 7. This means that we have shown that $\phi(175) = 120$ without actually listing all numbers and crossing out some of them.

At the beginning of this section, we found that $\phi(175) = 120$ using the formula from the last section. This means that we have verified that the formula is correct in this case.

For any number n that is a product of only two primes, the same kind of argument will show that our formula for $\phi(n)$ is correct. Arguments along these lines can show that for any n, our formula for $\phi(n)$ is correct. I'll spare you, but if you're really interested, you can take the graduate level math course I'll teach in the fall:)

EXERCISES: Explain your answer.

(1) Determine whether each of the following pairs of numbers is relatively prime? (hint: you should only need the Euclidean algorithm for two of these)
   (a) 24 and 68 (i.e., are 24 and 68 relatively prime?).
   (b) 309 and 471
   (c) 405 and 1235
   (d) 1031 and 1097

(e) 527 and 697
(f) 13 and 1411
(g) 13 and 2639
(h) 32 and 2035
(i) 32 and 2034

(2) Compute the following:
(a) $\phi(69)$
(b) $\phi(256)$
(c) $\phi(205)$
(d) $\phi(729)$
(e) $\phi(77)$
(f) $\phi(2)$
(g) $\phi(1,000,000,000)$

(3) List the numbers from 1 to 36 that are relatively prime to 36. Count them. Does your answer agree with the formula for $\phi(36)$.

(4) Compute the following. You may want to use the first few to guess the answer for the last part:
(a) $\phi(2^2)$
(b) $\phi(2^3)$
(c) $\phi(2^4)$
(d) $\phi(2^5)$
(e) $\phi(2^{123})$
(f) $\phi(2^k)$ for any number k.

(5) Look at all the computed values of $\phi(n)$ in this section besides $\phi(2) = 1$. How many of them are odd? Make a guess as to how many numbers n there are greater than 2 so that $\phi(n)$ is odd. Try to explain why your guess is correct using the formula for computing $\phi(n)$.

(6) (a) How many numbers are there from 1 to 90 relatively prime to 90? (hint: this is very easy using what we did in this section).
(b) How many numbers are there from 1 to 180 that are relatively prime to 90? (hint: what's the relation between being relatively prime to 90 and relatively prime to 180?)
(c) How many numbers are there from 1 to 270 that are relatively prime to 90?

(7) Find a number n so that $\phi(n) = 24$ (hint: this may require some playing around. If you don't have a better idea, just compute $\phi(n)$ for a bunch of numbers until you get 24 as your answer).