# Chapter 6

# Relatively prime

In the last chapter of this unit, we're going to take up a notion related to primality and prime factorization. Briefly, we say that two numbers $m$ and $n$ are *relatively prime* if their greatest common divisor is 1—that is, if no number other than 1 divides both $m$ and $n$. We'll consider first what this means, and then go on to pose and solve a counting problem that turns out to be absolutely fundamental: what proportion of all numbers are relatively prime to a given number?

## 6.1 What does it mean to be relatively prime?

Well, we just said what it means. But to hammer the point home, we're going to consider first of all a number of equivalent ways of saying it. To start with the definition, $m$ and $n$ are relatively prime if

- $\gcd(m, n) = 1$

which of course means precisely that

- The only number dividing both $m$ and $n$ is 1.

Now, since any number greater than 1 that divided both $m$ and $n$ would in turn be divisible by at least one prime, to say that $m$ and $n$ are relatively prime is equivalent to saying that

- No prime number divides both $m$ and $n$.

or in other words

- The prime factorizations of $m$ and $n$ have no primes in common.

One consequence of this way of putting it: if $m$ and $n$ are relatively prime, then so are any powers of $m$ and $n$, since their prime factorizations involve the same primes to higher powers; and conversely.

Next, recalling our discussion of divisibility earlier in this unit, we have a couple more equivalent formulations: first, we can say that $m$ and $n$ are relatively prime if

- $\operatorname{lcm}(m, n) = mn$

which in turn means precisely that

- Any number divisible by both $m$ and $n$ is a multiple of the product $mn$.

Lastly, from what we saw in the discussion of combinations, we can say that $m$ and $n$ are relatively prime if

- The number 1 is a combination of $m$ and $n$;

or, equivalently, if

- Every whole number is a combination of $m$ and $n$.

Note, by the way, that by our definitions, 1 and any number $n$ are relatively prime (in particular, 0 and 1 are relatively prime), but 0 and any number $n$ bigger than 1 are not relatively prime.

Had enough? Do the following exercise (it's easy) and then we'll get down to a real question.

**Exercise 6.1.1** Say whether each of the following pairs of numbers are relatively prime.

a. 66 and 70
b. 96 and 105
c. 234 and 399
d. 7 and 43,784
e. 64 and 32,965

## 6.2 The Euler $\phi$-function

The problem we're going to solve is simple enough to state: we're going to pick a number $n$ and ask, "How many of the numbers between 0 and $n-1$ are relatively prime to $n$?" The answer is usually denoted $\phi(n)$. (This is called the *Euler $\phi$-function*, after the 17th century mathematician Leonhard Euler, who first discussed it in connection with a result we'll encounter in the next unit.) Here are some examples:

$n = 6$: Of the numbers 0, 1, 2, 3, 4 and 5, only 1 and 5 are relatively prime to 6; so $\phi(6) = 2$.

$n = 8$: Since the only prime dividing 8 is 2, the numbers relatively prime to 8 are just the odd numbers. In particular, of the 8 numbers 0, 1, 2, ... ,7, the ones relatively prime to 8 are 1, 3, 5 and 7; so $\phi(8) = 4$.

$n = 13$: Since 13 is prime, any number not divisible by 13 is relatively prime to it. In particular, the numbers 1, 2, 3, ... , 12 are all relatively prime to 13, so $\phi(13) = 12$. In general, if $p$ is any prime numbers, all the numbers between 1 and $p-1$ are relatively prime to it, so $\phi(p) = p - 1$.

$n = 60$: We know that $30 = 2^2 \cdot 3 \cdot 5$, so the numbers relatively prime to 60 are simply those not divisible by 2, 3 or 5. Here's a list of those between 1 and 59:

$$1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 49,\ 53,\ 59$$

so $\phi(60) = 16$.

Now you do some:

**Exercise 6.2.1** Find the following:
a. $\phi(18)$
b. $\phi(21)$

c. $\phi(27)$
d. $\phi(37)$

How should we go about finding $\phi(n)$ in general? For small values of $n$ we can grind it out: check each number between 1 and $n-1$ in turn to see if it's relatively prime to $n$, make a list of those that are and count the list. But as you can imagine that gets old pretty fast. We'll try instead to be more systematic: we're going to use what we might call a *modified sieve.*

Remember that in the Sieve of Eratosthenes, in order to find the prime numbers we wrote out a list of all numbers and crossed off in turn the numbers divisible by 2, 3, 5, 7 and so on. To find the numbers relatively prime to a number $n$, we're going to do the same thing, but this time we're only going to cross off the numbers divisible by one of the primes dividing $n$. For example, to find the numbers between 0 and 14 relatively prime to 15, we start with the list

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13 \quad 14.$$

Now, since $15 = 3 \cdot 5$, we just want to cross off the numbers divisible by 3 or 5. We'll start with 3:

$$\cancel{0} \quad 1 \quad 2 \quad \cancel{3} \quad 4 \quad 5 \quad \cancel{6} \quad 7 \quad 8 \quad \cancel{9} \quad 10 \quad 11 \quad \cancel{12} \quad 13 \quad 14.$$

Next we cross off the numbers divisible by 5:

$$\cancel{\cancel{0}} \quad 1 \quad 2 \quad \cancel{3} \quad 4 \quad \cancel{5} \quad \cancel{6} \quad 7 \quad 8 \quad \cancel{9} \quad \cancel{10} \quad 11 \quad \cancel{12} \quad 13 \quad 14.$$

Of course, at this point we can simply count the numbers left to see that $\phi(15) = 8$. But we want a recipe for $\phi(n)$ that's going to work in general, without going through this process in full each time. So we should go back over this and ask: *at each stage of this process, how many numbers did we cross off?*

Well, that's easy enough to answer at the first stage: we start with 15 numbers and cross off every third number, so of course the number crossed off is 1/3 of 15, or 5; the number we have left after the first stage is correspondingly 2/3 of 15, or 10.

What about at the second stage? Well, of the 15 numbers we started with, exactly 1/5, or 3, are crossed off at the second stage; 4/5 of them, or

12, are spared. But, you'll say, (correctly) that can't be the answer, since we have double crossings: what we really need to know is not how many of the original 15 are crossed off at the second stage, but how many of those that are left after the first stage are axed at the second stage.

Now we see something really interesting. Of the 10 numbers left after the first pass, exactly 2 are crossed off in the second: in other words, the *fraction* 1/5 of the numbers left that are thrown out is exactly the same as the fraction of the original 15 that are hit. The number left at the end is correspondingly 4/5 of the number left after the first go round, so we see that

$$\phi(15) \;=\; 15 \cdot \frac{2}{3} \cdot \frac{4}{5} \;=\; 8.$$

**Exercise 6.2.2** Try doing the same process in the other order, that is, crossing off first the numbers between 0 and 14 divisible by 5, and then crossing off those divisible by 3. What fraction of the numbers are crossed off at the first step? What fraction *of the numbers left* are crossed off at the second?

Now let's see if this works in another case, say $n = 18$. To find $\phi(18)$, we start with a list of all numbers between 0 and 17:

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13 \quad 14 \quad 15 \quad 16 \quad 17.$$

Since $18 = 2 \cdot 3^2$, we want to cross off first the even numbers, then the numbers divisible by 3. Start with the evens:

$$\cancel{0} \quad 1 \quad \cancel{2} \quad 3 \quad \cancel{4} \quad 5 \quad \cancel{6} \quad 7 \quad \cancel{8} \quad 9 \quad \cancel{10} \quad 11 \quad \cancel{12} \quad 13 \quad \cancel{14} \quad 15 \quad \cancel{16} \quad 17.$$

As you might expect, exactly half, or 9, of the 18 numbers are crossed off; half are left. Now we cross off those divisible by 3:

$$\cancel{\cancel{0}} \quad 1 \quad \cancel{2} \quad \cancel{3} \quad \cancel{4} \quad 5 \quad \cancel{\cancel{6}} \quad 7 \quad \cancel{8} \quad \cancel{9} \quad \cancel{10} \quad 11 \quad \cancel{\cancel{12}} \quad 13 \quad \cancel{14} \quad \cancel{15} \quad \cancel{16} \quad 17.$$

Again, of the 18 numbers we started with, exactly 1/3, or 6, receive a slash at this stage. What's more, if we look just at the 9 numbers left after the first stage, we see that the same fraction 1/3 of them get crossed out at the second stage; likewise, of the 9 left after the first step, 2/3, or 6, are left after the second. We see in other words that

$$\phi(18) \;=\; 18 \cdot \frac{1}{2} \cdot \frac{2}{3} \;=\; 6.$$

In fact, exactly the same pattern holds in general. If we're given any number $n$ and asked to find $\phi(n)$, we can just imagine going through the sieve process to find $\phi(n)$—we don't have to actually do it. First, we'd make a list of the $n$ numbers between 0 and $n-1$. Next, we'd figure out what primes divide $n$; we can call them $p$, $q$, $r$ and so on. Then we cross off the numbers on our list divisible by $p$; this involves crossing off exactly $1/p$ of the numbers, so after this stage there are

$$n \cdot \frac{p-1}{p}$$

numbers left. The next step is to cross off the numbers divisible by $q$, and the key observation here is that this involves getting rid of exactly $1/q$ *of the numbers left after the first stage*—in other words, the number left after the second pass will be

$$n \cdot \frac{p-1}{p} \cdot \frac{q-1}{q}.$$

The process continues in this way: at the third stage, we cross off exactly $1/r$ of the numbers left, so the number remaining after the third is

$$n \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} \cdot \frac{r-1}{r}$$

and so on. Imagining how this is going to go, we're led to the following

## Simple recipe for $\phi(n)$

• First, find the prime factorization of $n$, and make a list of the primes dividing $n$.

• Then start with the number $n$, and for each prime $p$ on your list multiply by $\frac{p-1}{p}$.

Here's an example: suppose we want to find $\phi(84)$. We first write the prime factorization of 84:

$$84 = 2^2 \cdot 3 \cdot 7$$

so the primes dividing 28 are 2, 3 and 7. According to our recipe, then, we have

$$\phi(84) = 84 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 24.$$

Now it's your turn.

**Exercise 6.2.3** Find the following:

a. $\phi(55)$
b. $\phi(128)$
c. $\phi(90)$
d. $\phi(89)$
e. $\phi(105)$

**Exercise 6.2.4** Verify that the values of $\phi(n)$ you found in Exercise 6.2.1 agree with the recipe.

At this point you may have one qualm. (Or maybe you have several; but we're only going to deal with one right now.) As simple as this recipe is, it does require one ingredient that may in some cases be hard to come by: in order to find $\phi(n)$, we have to know the prime factorization of $n$. And this, you may remember from the last section, is not necessarily easy to find when $n$ is a large number. Of course, there are other methods of calculating $\phi(n)$—for example, there's the brute force method of just listing the numbers from 1 to $n$ and crossing off those with a common factor—but these are too slow to be of any real use.

This seems to be an intrinsic difficulty: there are no known simple recipes for calculating $\phi(n)$ that don't require that we know the prime factorization of $n$. In fact, as we'll see in the final unit, this turns out to be the essential basis of the codes which we use to transmit secure information over the Internet. To put it another way, the safe transmission of electronic information rests on the presumption that you can't figure out a way to calculate $\phi(n)$, for large $n$, in a reasonably short time.

## 6.3 Why does this work?

You may be a little uneasy at the idea of looking at two examples and extrapolating from them a general formula. We know that the recipe we gave above for $\phi(n)$ works for $n = 15$ and $n = 18$, and we can also check it for the other values of $n$ for which we've calculated $\phi(n)$ already. But does that mean it works every time?

Actually, you may not be as uneasy as we are. Mathematicians are fairly unique in our desire to see every assertion we make and use proved, and also in our refusal to accept observed behavior as proof. A mathematician will see a pattern repeated a billion times and will not consider it an established fact that the pattern holds in general.[1] Most people would be more than happy to consider the issue settled a lot sooner than that. You're probably not upset at all by the leap of faith we made in the last section—unless you're a mathematician, in which case you're probably livid.

What we're saying, in other words, is that the inclusion of the following argument, which tries to demonstrate that the simple recipe given above for $\phi(n)$ always works, is not for your sake. It's for ours. And if you don't need to be further convinced that the recipe works, you can feel free to skip the rest of this section.

That said, let's start by looking at the second stage of the modified sieve process and seeing why the recipe works there. To say that we're at the second stage means that we've started with a number $n$, and identified two primes $p$ and $q$ dividing $n$. We've made a list of the numbers between 0 and $n-1$, and crossed off the numbers divisible by $p$; that is, there're $\frac{n}{p}$ numbers crossed off and there are

$$n \cdot \frac{p-1}{p}$$

numbers left.

Now we cross off the numbers divisible by $q$. Since $q$ divides $n$, this involves crossing exactly $n/q$ of the original $n$ numbers. But how many of those are repeats, that is, number already crossed off? Well, the repeats are exactly the numbers divisible by both $p$ and $q$; and as we saw in the original chapter of this unit, since $\gcd(p,q) = 1$, *the numbers divisible by both $p$ and $q$ are just the numbers divisible by $pq$*. The number $n$ is divisible by $pq$, so the number of numbers crossed off twice is thus exactly $n/pq$. We have, in other words

$$\text{Number of numbers we start with} \quad = \quad n$$

$$\text{Number of numbers crossed off in the first step} \quad = \quad \frac{n}{p}$$

[1] This is not an exaggeration. One of the most famous open problems in mathematics is the *Riemann hypothesis*, which asserts that the solutions of a certain equation all lie on a line. This has been verified directly for the first 1,000,000,000, solutions of the equation, but it not considered an established fact.

$$\text{Number of numbers crossed off in the second step} = \frac{n}{q}$$

and

$$\text{Number of numbers crossed off in the both steps} = \frac{n}{pq}$$

Now we can apply the inlcusion/exclusion principle, which tells us that the number of numbers left is

$$\begin{aligned}\text{Number of numbers left} &= n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq} \\ &= n\left(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right) \\ &= n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) \\ &= n \cdot \frac{p-1}{p} \cdot \frac{q-1}{q}.\end{aligned}$$

In other words, at the second stage we lop off exactly $1/q$ of the remaining numbers, as we said.

The same sort of analysis can be carried out to see that at each stage, when we cross off the numbers divisible by a prime $r$ dividing $n$, we cross off not just one out of every $r$ of the original numbers, but exactly one out of every $r$ of the numbers remaining at that stage—in other words, the simple recipe we gave for $\phi(n)$ works in general.

## 6.4 Odds and ends

If we had any sense whatsoever, we'd stop this chapter right here. But we don't. And there is one more fact that is so mind-bogglingly and perversely wonderful that we can't not tell you about it.

To start with, let's go back to the question we raised at the beginning of this chapter: for a particular number $n$, what proportion of all numbers are relatively prime to $n$? In other words, what are the odds that a number chosen at random will be relatively prime to $n$?

The first thing to see is that we have (despite appearances) already answered that question. It may seem that we answered only a very limited version of the question: we asked, "of the $n$ numbers between 0 and $n-1$, how many are relatively prime to $n$?" But if we look a little closer, we see that we have in fact answered the original question.

The point is, if a number $a$ is relatively prime to $n$, then so is $a+n$; if $a$ is not, then $a+n$ isn't either. What this means is that if we look among the next $n$ numbers after $n-1$—in other words, the numbers between $n$ and $2n-1$—we'll see exactly the same pattern of numbers relatively prime to $n$ and not as in the numbers from 0 to $n-1$. For example, when $n$ was 15 we saw that the numbers between 0 and 14 that were relatively prime to 15 are exactly the un-crossed numbers on the list

$$\cancel{0} \quad 1 \quad 2 \quad \cancel{3} \quad 4 \quad \cancel{5} \quad \cancel{6} \quad 7 \quad 8 \quad \cancel{9} \quad \cancel{10} \quad 11 \quad \cancel{12} \quad 13 \quad 14.$$

Now suppose we want to extend the list through another 15 numbers, that is, up to 29. Writing the next 15 numbers under the first 15, we have

$$\begin{array}{ccccccccccccccc} \cancel{0} & 1 & 2 & \cancel{3} & 4 & \cancel{5} & \cancel{6} & 7 & 8 & \cancel{9} & \cancel{10} & 11 & \cancel{12} & 13 & 14 \\ \cancel{15} & 16 & 17 & \cancel{18} & 19 & \cancel{20} & \cancel{21} & 22 & 23 & \cancel{24} & \cancel{25} & 26 & \cancel{27} & 28 & 29 \end{array}$$

and we see that the pattern is the same. In particular, there are exactly as many numbers between 15 and 29 relatively prime to 15 as there are between 0 and 14; and there'll be the same number in the next group of 15, and so on. What this means is that it makes sense to say that, on average, 8 out of 15 numbers are relatively prime to 15. Similarly, we can say in general that

$$\boxed{\textit{The fraction of all numbers that are relatively prime to } n \textit{ is } \frac{\phi(n)}{n}.}$$

Now we're going to talk about a problem whose answer we'll only be able to state, not to justify. But it's a natural question to ask, and the answer is startling. If we pick a number $n$ then we've seen how to figure out the percentage of all numbers $a$ that are relatively prime to it—for example, if

$n = 15$, then the odds that a number $a$ picked at random will be relatively prime to 15 will be $8/15$. But what if we just pick *two* numbers $a$ and $b$ at random—what are the odds that they're relatively prime?

It's a tricky question, in part because it's not immediately clear that it makes sense. Let's try to make sense out of it, though, by imagining a sort of "thought experiment". Suppose we made a list of all pairs of one-digit numbers (0 to 9), and figured out, of the 100 such pairs, what fraction were relatively prime; suppose we called this fraction $x_1$. Now say we did the same thing for pairs of 2-digit numbers: in other words, of the 10,000 pairs of numbers between 0 and 99 we figured out what fraction are relatively prime, and called that $x_2$. Then suppose we did the same for three-digit numbers, and called the resulting fraction $x_3$, and so on. We would then ask: as we increase the number of digits, how do the numbers $x_1, x_2, x_3, \ldots$ behave? Do they approach 0, or 1, or some number in between? If in fact they do approach a fixed number, we can say that that number represents the fraction of all pairs of numbers that are relatively prime—the odds, in other words, that a randomly selected pair of large numbers will be relatively prime.

The answer is that the numbers $x_1, x_2, x_3, \ldots$ do approach a definite number, and a remarkable number at that. We will just state the final result.

*The fraction of all pairs of numbers that are relatively prime approaches the number* $\dfrac{6}{\pi^2}$.

Now, $6/\pi^2$ is a real number, with decimal expansion $.6079271\ldots$—in particular, it's a little larger than three-fifths. This may seem a little counterintuitive: what we're saying is that, if you pick a couple of, say, 10-digit numbers at random, the odds are in your favor that you can express 1 as a combination of the two.

But the truly strange thing about the number is the factor $\pi^2$. What's that doing there? And if that's not weird enough, here's something else. First, it has been figured out what the odds are that four numbers, picked at random, are relatively prime (by which we mean that 1 can be expressed as a combination of them): the odds are $90/\pi^4$, or $.9238384\ldots$. But no one has ever been able to determine exactly what the odds are for three numbers!