ALEXANDER A. STEPANOV
DANIEL E. ROSE

FROM MATHEMATICS TO GENERIC PROGRAMMING

From Mathematics to Generic Programming

Theorem 5.6 (Converse of Fermat's Little Theorem): *If for all* $a, 0 < a < n$,

$$a^{n-1} = 1 + q_a n$$

then n is prime.

Proof. Suppose n is not prime; that is, $n = uv$. Then by the Non-invertibility Lemma, u is not invertible. But by the condition of the theorem, $u^{n-1} = u^{n-2}u = 1 + q_u n$. In other words, u has an inverse u^{n-2}, which is a contradiction. So n must be prime. □

5.5 Euler's Theorem

Like any great mathematician, Euler was not satisfied with just proving Fermat's Little Theorem; he wanted to see if it could be generalized. Since Fermat's Little Theorem was only for primes, Euler wondered whether there was a similar result that would include composite numbers. But composite numbers do strange things in modular arithmetic. To illustrate this, let's take a look at the multiplication table modulo 10, which we've annotated by showing inverses of the left-hand factor on the right-hand side of the table:

×	1	2	3	4	5	6	7	8	9	
1	1	2	3	4	5	6	7	8	9	1
2	2	4	6	8	0	2	4	6	8	
3	3	6	9	2	5	8	1	4	7	7
4	4	8	2	6	0	4	8	2	6	
5	5	0	5	0	5	0	5	0	5	
6	6	2	8	4	0	6	2	8	4	
7	7	4	1	8	5	2	9	6	3	3
8	8	6	4	2	0	8	6	4	2	
9	9	8	7	6	5	4	3	2	1	9

The table should look a bit familiar, because it's just like the traditional 10×10 multiplication table, if you keep only the last digit of each product. For example, $7 \times 9 = 63$, which is 3 mod 10. Immediately we can see differences from the table we did for 7, which was prime (see p. 74). For one thing, the rows are no longer permutations of each other. More importantly, some rows now contain 0. That's a problem for multiplication—how can the product of two things be 0? That would mean that we get into a situation where we can never escape zero—any product of the result will be zero.

The other property we noted earlier about primes—that only 1 and -1 are self-canceling—happens to be true for 10 as well, but is not always true for composite numbers. (The integer 8, for example, has four self-canceling elements: 1, 3, 5, and 7.)

Let's look at the multiplication table for 10 again, focusing on certain entries:

×	1	2	3	4	5	6	7	8	9	
1	**1**	2	**3**	4	5	6	**7**	8	**9**	**1**
2	2	4	6	8	0	2	4	6	8	
3	**3**	6	**9**	2	5	8	**1**	4	**7**	**7**
4	4	8	2	6	0	4	8	2	6	
5	5	0	5	0	5	0	5	0	5	
6	6	2	8	4	0	6	2	8	4	
7	**7**	4	**1**	8	5	2	**9**	6	**3**	**3**
8	8	6	4	2	0	8	6	4	2	
9	**9**	8	**7**	6	5	4	**3**	2	**1**	**9**

The rows that contain only "good" products (i.e., no zeros) are the ones whose first factor is shown in a rectangular box on the left—which also happen to be the rows where that factor has an inverse, shown on the right side of the table. Which rows have this property? Those that represent numbers that are coprime with 10. (Remember, being coprime means having no common factors greater than 1.)

So could we just use the good rows and leave out the rest? Not quite, because some of the results in good rows would themselves lead to bad rows if used in a successive product. (For example, 3 is a good row, but $(3 \times 5) \times 2 = 0$.) Euler's idea was to use only the entries in good *columns* as well as good rows—the numbers in shaded cells. Notice that those numbers have all the nice properties we saw for primes: the shaded numbers in each row are permutations of each other, each set of shaded numbers contains a 1, and so on.

* * *

To extend Fermat's Little Theorem for composite numbers, Euler uses only these bold values. He starts by defining the size of the set of coprimes:

Definition 5.2. The **totient** of a positive integer n is the number of positive integers less than n that are coprime with n. It is given by the formula:

$$\phi(n) = |\{0 < i < n \ \wedge \ \text{coprime}(i, n)\}|$$

This is known as the **Euler totient function** or **Euler ϕ function**.

$\phi(n)$ gives us the number of rows containing shaded entries in the multiplication table modulo n. For example, $\phi(10) = 4$, and $\phi(7) = 6$, as we can see from the multiplication tables given earlier.

Since primes by definition don't share any prime factors with smaller numbers, the totient of a prime number is

$$\phi(p) = p - 1$$

In other words, all numbers less than a given prime are coprime with it.

What Euler realized was that the $p - 1$ in Fermat's theorem is just a special case; it's what ϕ happens to be for primes. Now we can state Euler's generalization of Fermat's Little Theorem.

Theorem 5.7 (Euler's Theorem): coprime$(a, n) \iff a^{\phi(n)} - 1$ *is divisible by* n.

Exercise 5.2. Prove Euler's Theorem by modifying the proof of Fermat's Little Theorem. Steps:

- Replace Permutation of Remainders Lemma with Permutation of Coprime Remainders Lemma. (Essentially, use the same proof but look only at "good" elements.)
- Prove that every coprime remainder has a multiplicative inverse. (We just showed that the remainders form a permutation, so 1 has to be somewhere in the permutation.)
- Use the product of all coprime remainders where the proof of Little Fermat has the product of all nonzero remainders.

* * *

We would like to be able to compute the ϕ function for any integer. Since we can express any integer as the product of powers of primes, we'll start by seeing how to compute the totient of a power of a prime p. We want to know the number of coprimes of p^m. We know there are at most $p^m - 1$ of them, because that's all the possible numbers less than p^m. But we also know that those divisible by p (i.e., multiples of p) are not coprime, so we need to subtract however many of these there are from our total:

$$\begin{aligned}\phi(p^m) &= (p^m - 1) - |\{p, 2p, \ldots, p^m - p\}| \\ &= (p^m - 1) - |\{1, 2, \ldots, p^{m-1} - 1\}| \\ &= (p^m - 1) - (p^{m-1} - 1) \\ &= p^m - p^{m-1} \\ &= p^m \left(1 - \frac{1}{p}\right)\end{aligned}$$

What happens if we have $\phi(p^u q^v)$, where p and q are both primes? Again, we start with the maximum possible and then subtract off all the multiples. So we'll subtract the number of multiples of p and also the number of multiples of q, but then we have to add back multiples of both p and q, because otherwise they'd be subtracted twice. (This general technique, known as the *inclusion-exclusion* principle, is often used in combinatorics.) Let us assume $n = p^u q^v$:

$$\begin{aligned}\phi(n) &= (n-1) - \left(\frac{n}{p} - 1\right) - \left(\frac{n}{q} - 1\right) + \left(\frac{n}{pq} - 1\right) \\ &= n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq} \\ &= n\left(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right) \\ &= n\left[\left(1 - \frac{1}{p}\right) - \frac{1}{q}\left(1 - \frac{1}{p}\right)\right] \\ &= n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) \\ &= p^u \left(1 - \frac{1}{p}\right) q^v \left(1 - \frac{1}{q}\right) \\ &= \phi(p^u)\phi(q^v)\end{aligned}$$

As a special case when we have a simple product of two primes, p_1 and p_2, we now know that

$$\phi(p_1 p_2) = \phi(p_1)\phi(p_2) \tag{5.5}$$

For example, since $10 = 5 \times 2$,

$$\phi(10) = \phi(5)\phi(2) = 4$$

Although the case we care most about is the one given here, we can generalize the formula to handle a product of any number of primes raised to powers, not just two. For example, if we had three factors p, q, and r, we'd subtract all the multiples of each, then add back the double-counted multiples of pq, pr, and qr,

and then compensate for our overcompensation by again subtracting multiples of pqr. Extending this to m primes gives this formula, where $n = \prod_{i=1}^{m} p_i^{k_i}$:

$$\begin{aligned}\phi(n) &= \phi\left(\prod_{i=1}^{m} p_i^{k_i}\right) \\ &= n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^{m}\phi\left(p_i^{k_i}\right)\end{aligned}$$

Euler's interest in proving his theorem led to his need to count coprimes. His derivation of the ϕ function gave him a tool that allowed him to efficiently compute this count in the cases where the prime decomposition is known.

5.6 Applying Modular Arithmetic

In Section 5.3, we saw how modular multiplication was related to remainders. Let's take a look at a couple of our important results from earlier in the chapter and see what some examples look like if we do them modulo 7. Wilson's Theorem states that for a prime p, there exists some m such that

$$(p-1)! = (p-1) + mp$$

Another way to say this is

$$(p-1)! = (p-1) \bmod p$$

Let's see if we can confirm that result if p is 7. $p-1$ is 6, so we start by expanding 6! into its factors, rearranging them, and using our modular multiplication table to cancel inverses:

$$\begin{aligned}\mathbf{6!} &= 1 \times 2 \times 3 \times 4 \times 5 \times 6 \\ &= 1 \times (2 \times 4) \times (3 \times 5) \times 6 \\ &= (1 \times 1 \times 1 \times 6) \bmod 7 \\ &= 6 \bmod 7\end{aligned}$$

which is what Wilson's Theorem predicts.

Similarly, let's use modular multiplication to see what Fermat's Little Theorem says. The original form is

If p is prime, $a^{p-1} - 1$ is divisible by p for any $0 < a < p$.

But with modular arithmetic, we could restate it as

$$\text{If } p \text{ is prime,} \quad a^{p-1} - 1 = 0 \bmod p \quad \text{for any } 0 < a < p.$$

or

$$\text{If } p \text{ is prime,} \quad a^{p-1} = 1 \bmod p \quad \text{for any } 0 < a < p.$$

Again, let's use $p = 7$, and try $a = 2$. This time we'll expand our expression, multiply both sides by 6!, and then use modular multiplication to cancel terms:

$$\begin{aligned}
2^6 &= (2 \times 2 \times 2 \times 2 \times 2 \times 2) \\
2^6 \times 6! &= (2 \times 2 \times 2 \times 2 \times 2 \times 2) \times (1 \times 2 \times 3 \times 4 \times 5 \times 6) \\
&= (2 \times 1) \times (2 \times 2) \times (2 \times 3) \times (2 \times 4) \times (2 \times 5) \times (2 \times 6) \\
&= (2 \times 4 \times 6 \times 1 \times 3 \times 5) \bmod 7 \\
&= (1 \times 2 \times 3 \times 4 \times 5 \times 6) \bmod 7 \\
&= 6! \bmod 7 \\
2^6 &= 1 \bmod 7
\end{aligned}$$

which is what Fermat's Little Theorem tells us.

5.7 Thoughts on the Chapter

Earlier, we saw how the ancient Greeks were interested in perfect numbers. There wasn't any practical value to this work; they were simply interested in exploring properties of certain kinds of numbers for their own sake. Yet as we have seen in this chapter, over time the search for these "useless" perfect numbers led to the discovery of Fermat's Little Theorem, one of the most practically useful theorems in all of mathematics. We'll see why it's so useful in Chapter 13.

This chapter also gave us a first look at the process of abstraction in mathematics. Euler looked at Fermat's Little Theorem and realized that he could extend it from one specific situation (primes) to a more general one (integers). He saw that the exponent in Fermat's theorem was a special case of a more general concept, the number of coprimes. That same process of abstraction lies at the heart of generic programming. Generalizing code is like generalizing theorems and their proofs. Just as Euler saw how to extend Fermat's result from one type of mathematical object to another, so programmers can take a function that was designed for one type of computational object (say, vectors) and extend it to work equally well on another (perhaps linked lists).