6.3 Modular Exponentiation

Most technological applications of modular arithmetic involve exponentials with very large numbers. For example, a typical problem related to encryption might involve solving one of the following two equations:

$$67930^{32319} \equiv a \pmod{103969} \tag{70}$$

$$67930^{b} \equiv 48560 \pmod{103969}. \tag{71}$$

It turns out that $a = 6582$ and $b = 32320$ solve these equations, but those answers are not obvious at all from looking at the equations. More importantly, it is not even clear *how* we would go about determining a and b. In what is part of a great mystery of the modern study of computational complexity, the first equation is relatively easy for computers to solve, whereas there is no known way of efficiently solving the second problem. In this section we will look at some problems involving modular exponentiation and some techniques we can use to solve such problems.

Suppose we are asked to determine the remainder of the enormous number $10^{51239203}$ after dividing it by 5. This number has over 50 million digits! How on earth can we hope to ever figure out such a difficult problem without a calculator that can hold more than 8 or even a few dozen digits? Although this might appear impossible to solve, you might notice that 10 is divisible by 5, and the enormous number is just a multiple of 10. If the remainder of 10 when divided by 5 is 0, then so is any multiple of 10, including the enormous number. Of course the answer would be the same if we were attempting to divide it by 2 instead, but what would happen if we divide it by 3, 7, or some other number?

Patterns

We begin by considering how to search for patterns among the remainders when we taken a number to subsequently higher powers. For example, let us consider the remainders of 10, 100, 1000, and so forth when we divide them by 3. The first thing we notice is that the remainder of 10 after dividing it by 3 is 1. In the language of modular arithmetic we can write:

$$10^1 \equiv 1 \pmod{3}. \tag{72}$$

The exponent next to the 10 is not necessary but we place it there to make the next step slightly easier. Say that at this point we want to determine the remainder of 100 after dividing it by 3. There are two ways we can go about doing this. First, we can do simple arithmetic to determine that 100/3 equals 33, remainder 1. Although this calculation is not terribly difficult, we can actually avoid it using a rule we saw in the previous section. Namely, if we have two congruence relations, then we can combine them by multiplying both left-hand sides and both right-hand sides to obtain a new congruence relation:

Theorem.

$$\begin{aligned} \textit{If} \qquad a &\equiv b \pmod{m} \qquad \textit{and} \\ c &\equiv d \pmod{m}, \qquad \textit{then} \\ a \times c &\equiv b \times d \pmod{m}. \end{aligned}$$

In our particular case, we know that

$$\begin{aligned} 10^1 &\equiv 1 \pmod{3}, \qquad \text{and} \\ 10^1 &\equiv 1 \pmod{3}. \end{aligned}$$

Of course these are the same equation, but writing them out in this way allows us to think of them in terms of the previous theorem. More specifically, this theorem allows us to multiply both sides of the equation together, to get:

$$\begin{aligned} 10^1 \times 10^1 &\equiv 1 \times 1 \pmod{3}, \\ 10^2 &\equiv 1 \pmod{3}. \end{aligned}$$

We can then use the same technique, through induction, to show that *all* integer powers of 10 are congruent to 1 mod 3, since we can continue multiplying our resulting equation by the initial equation $10^1 \equiv 1 \pmod{3}$. In other words, all positive integer powers of 10, when divided by 3, give us a remainder of 1!

We have chosen a relatively simple case to highlight the usefulness of Theorem 2 for simplifying what might otherwise be very complicated calculations. We now consider several more complex examples in which we can determine patterns as we consider $a^n \pmod{m}$ as n increases.

Example 1. Consider the very large number $7^{1383921}$ and how we might determine its remainder after dividing it by 4. Of course we know that the only possible remainder are 0, 1, 2, and 3, but it is not clear how to determine which of those it is. Simple calculations show the following pattern:

$$\begin{aligned} 7^1 &\equiv 3 \pmod{4}, \\ 7^2 &\equiv 1 \pmod{4}, \\ 7^3 &\equiv 3 \pmod{4}, \\ 7^4 &\equiv 1 \pmod{4}, \ldots \end{aligned}$$

It seems that if n is odd, then $7^n \equiv 3 \pmod{4}$, and if n is even, then $7^n \equiv 1 \pmod{4}$. We can prove that this pattern will repeat as n increases by noticing that $7^2 \equiv 1 \pmod{4}$. Combining this with Theorem 16 shows that if $7^n \equiv 3 \pmod{4}$ then $7^{n+2} \equiv 3 \pmod{4}$, and likewise if $7^n \equiv 1 \pmod{4}$ then $7^{n+2} \equiv 1 \pmod{4}$. Therefore, the pattern repeats with a period of 2. Determining the remainder of $7^{1383921}$ when dividing by 4 is then straightforward – since the exponent $n = 1383921$ is odd, the remainder must be 3.

Example 2. Let us consider the very large number $4^{2349321230}$ and determine its remainder after dividing it by 15. Of course we know that the only possible solutions are in $\{0, 1, 2, \ldots, 14\}$, but that is still a wide range of options,

and it is not clear how to determine which of those it is. Simple calculations show the following pattern:

$$\begin{aligned} 4^1 &\equiv 4 \pmod{15}, \\ 4^2 &\equiv 1 \pmod{15}, \\ 4^3 &\equiv 4 \pmod{15}, \\ 4^4 &\equiv 1 \pmod{15}, \ldots \end{aligned}$$

It seems that if the exponent n is odd, then $4^n \equiv 4 \pmod{15}$, and if n is even, then $4^n \equiv 1 \pmod{15}$. This pattern too will repeat ad infinitum, because in this case we have $4^2 \equiv 1 \pmod{15}$, and so increasing the exponent n by 2 will never change the remainder mod 15, and $4^n \equiv 4^{n+2} \pmod{15}$ for all exponents n. Determining the remainder of $4^{2349321230}$ when dividing by 15 is then straightforward – since the exponent $n = 2349321230$ is even, the remainder must be 1.

Example 3. The particular patterns need not have a length of 2, and indeed most of the time they don't. Here we consider a repeating pattern with a slightly longer period. Let us consider the very large number 7^{30001} and determine its remainder after dividing by 18. Simple calculations show the following pattern:

$$\begin{aligned} 7^1 &\equiv 7 \pmod{18}, \\ 7^2 &\equiv 13 \pmod{18}, \\ 7^3 &\equiv 1 \pmod{18}, \\ 7^4 &\equiv 7 \pmod{18}, \\ 7^5 &\equiv 13 \pmod{18}, \\ 7^6 &\equiv 1 \pmod{18}, \ldots \end{aligned}$$

Here the pattern repeats every 3, because $4^3 \equiv 1 \pmod{18}$ and so increasing n by 3 will never change the remainder mod 18. Determining the remainder of 7^{30001} when dividing by 18 then requires us to look at the exponent $n = 30001$. Since adding and subtracting multiple of 3 from this number will not change the remainder, we should subtract from it 30000, which of course is a multiple of 3. We can then determine that $7^{30001} \equiv 7^1 \equiv 7 \pmod{18}$.

Example 4. Here we consider a repeating pattern with a period of 4. Let us consider remainders of all numbers 5^n after dividing them by 13. Simple calculations show the following pattern:

$$\begin{aligned} 5^1 &\equiv 5 \pmod{13}, \\ 5^2 &\equiv 12 \pmod{13}, \\ 5^3 &\equiv 8 \pmod{13}, \\ 5^4 &\equiv 1 \pmod{13}, \\ 5^5 &\equiv 5 \pmod{13}, \\ 5^6 &\equiv 12 \pmod{13}, \ldots \end{aligned}$$

Here the pattern repeats every 4 powers, since $5^4 \equiv 1 \pmod{13}$. Therefore, increasing the exponent n by 4 will never change the remainder when dividing by 13, and $5^n \equiv 5^{n+4} \pmod{13}$ for all exponents n. Determining the remainder of 5^n when dividing by 13 then requires us to determine whether the exponent n is divisible by 4. If it is divisible by 4, then the remainder must be 1. Otherwise, if the remainder is 1, then $5^n \equiv 5 \pmod{13}$; if the remainder is 2, then $5^n \equiv 12 \pmod{13}$; and if the remainder is 3, then $5^n \equiv 8 \pmod{13}$.

Maximum Length of Patterns

Every sequence of powers $a^1, a^2, a^3, \ldots \pmod{m}$ eventually forms a repeating pattern, though the length of these patterns can be significantly larger than 4. Here we consider the question – how long can the period of such a pattern be? So far we have seen patterns of periods 1, 2, 3, and 4. In all cases, the length of the period was smaller than the modulus m. Was this coincidental? Can a repeating pattern have a period longer than the modulus?

To see that the maximum length of a repeating pattern is $m-1$, we first point out that there are only m possible remainders when dividing by m: $0, 1, 2, \ldots m-1$. Second, we note that if 0 appears anywhere in the pattern, then all subsequent remainders must be 0. To understand why this is true, consider a number a and some power n for which

$$a^n \equiv 0 \pmod{m}. \tag{73}$$

The next number in the pattern is the remainder of a^{n+1} after dividing it by m. Of course it is always true that

$$a \equiv a \pmod{m}, \tag{74}$$

since a number is always congruent to itself. Theorem 16, which we have already seen several times, allows us to combine these two equations to obtain:

$$a^n \times a \equiv 0 \times a \pmod{m},$$

and so

$$a^{n+1} \equiv 0 \pmod{m}.$$

The same technique can be used to show that $a^{n+2}, a^{n+3}, \ldots$ are all congruent to 0 mod m, and so all subsequent powers must be congruent to 0.

Therefore, a repeating pattern that does not consist merely of 0's can only contain the $m-1$ distinct numbers: $1, 2, \ldots m-1$. Next, it is easy to see that any of these $m-1$ numbers can appear at most once in a repeating pattern. It is not possible, for example, to have a repeating pattern 2, 3, 2, 1 that repeats itself over and over. Why not? Each consecutive term in the sequence can be calculated from the term before it, by multiplying it by a. If we multiply 2 by a, the result can either be 3 or it can be 1, but it can't be both. So if 2 is followed by 3 in the pattern, then it must always be followed by 3, and it cannot sometimes be followed by a 1. Since each number is always followed by the same number, once we return to a number we have seen before, the pattern will begin

to repeat again. The longest possible pattern then includes all integers between 1 and $m-1$, but not 0, as explained. Therefore, if we are dividing powers of a by m, then the maximum length of a repeating pattern of remainders is $m-1$.

To see that this is indeed possible, consider the remainders of $5^1, 5^2, 5^3, \ldots$ when divided by $m = 277$. We obtain: 5, 25, 125, 71, 78, 113, 11, 55, ...; the pattern will not repeat before we reach 5^{277}, which is congruent to 5 and which thus begins the pattern again. Now that we are aware of patterns with very long periods, the approach of finding short patterns will not always help us simplify large exponents. Fermat's Little Theorem gives us an alternate shortcut for computing modular remainders of large exponents.

Fermat's Little Theorem

As we have seen, every sequence of powers $a^1, a^2, a^3, \ldots \pmod m$ will eventually form a repeating pattern, which can be as long as $m-1$. If the length of such a pattern is $m-1$, then multiplying any number by a^{m-1} is equivalent to multiplying it by 1. In the language of modular arithmetic, this can be stated $a^{m-1} \equiv 1 \pmod m$.

Fermat's Little Theorem, which we will not prove here, can be thought of as a generalization of this result that does not involve consideration of repeating patterns. More specifically:

Theorem 20 (Fermat's Little Theorem)**.** *If a is an integer and p is a prime number that does not divide a, then $a^{p-1} \equiv 1 \pmod p$.*

You may have noticed the requirement that p does not divide a. Why is this? To explain this, it pays to consider an example where p does divide a. Consider what happens, for example, if $a = 20$ and $p = 5$. Of course $p = 5$ is a prime number, but it is also clear that $a^{p-1} \equiv 0 \pmod p$, since 5 evenly divides 20, and so there is never a remainder after dividing 20, or any power of it, by 5. So Fermat's Little Theorem can only consider cases where p does not divide a.

Example 1. What is the remainder of 50^{72} when divided by 73? Since 73 is a prime number, and since 50 is not a multiple of 73, then we have $50^{72} \equiv 1 \pmod{73}$. So the remainder of 50^{72} when divided by 73 is 1.

Example 2. What is the remainder of 100^{10} when it is divided by 11? Since 11 is a prime number, and since 100 is not a multiple of 11, then we have $100^{10} \equiv 1 \pmod{11}$. So the remainder of 100^{10} when divided by 11 is 1. Of course we can combine this congruence relation with itself (using Theorem 16) to obtain $100^{20} = 100^{10} \times 100^{10} \equiv 1 \times 1 = 1 \pmod{11}$. The same process can be repeated to show that 100^{30}, 100^{40}, etc, are also congruent to 1 mod 11.

Example 3. What is the remainder of 3^{49} when divided by 7? Fermat's Little Theorem tells us that $3^6 \equiv 1 \mod 7$, so we write 3^{50} in terms of 3^6. We can write this as $3^{49} = 3 \cdot (3^6)^8$, which we can then reduce: $3 \cdot (3^6)^8 \equiv 3 \cdot 1^8 \equiv 3 \pmod 7$.

Example 4. What is the remainder of 2^{432} when divided by 11? Of course 11 is a prime number, but the exponent here is not $p-1$, so how can we use Fermat's Little Theorem to help us? We can rewrite 2^{432} as $2^{430}2^2 = (2^{10})^{43}2^2$.

Note that Fermat's Little Theorem tells us that $2^{10} \equiv 1 \mod 10$, which means that we can replace 2^{10} in this equation with 1. So we have $2^{432} = 2^{430}2^2 = (2^{10})^{43}2^2 \equiv 1^{43}2^2 \equiv 1 \cdot 2^2 \equiv 4 \pmod 1)1$. Hence, the remainder of dividing 2^{432} by 11 is 4.

Example 5. What is $29^{25} \pmod{11}$? Fermat's Little Theorem tells us that $29^{10} \equiv 1 \pmod{11}$, so we want to rewrite 29^{25} as $29^{10} \cdot 29^{10} \cdot 29^5$. We then have $29^{25} \equiv 29^{10} \cdot 29^{10} \cdot 29^5 \equiv 1 \cdot 1 \cdot 29^5 \equiv 29^5 \pmod{11}$. Since $29 \equiv 7 \pmod{11}$, we can further simplify this to $7^5 = 7^2 \cdot 7^2 \cdot 7 \equiv 49 \cdot 49 \cdot 7 \equiv 5 \cdot 5 \cdot 7 \equiv 10 \pmod{11}$.

Example 6. What is $1^{10} + 2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \pmod{11}$? Fermat's Little Theorem has $a^{10} \equiv 1 \pmod{11}$ for each term. Even when we take multiples of the exponent 10, we still have the same result. Therefore, each term contributes 1, and so the answer is the number of terms, 6.

Notice that each problem is different and requires thinking. Oftentimes, rewriting a large exponent as the product of smaller exponents can enable the use of patterns of Fermat's Little Theorem to further simplify a problem.