7.5 Modular Exponentiation and Order

The last ingredient we'll need to understand for our study of cryptography in the next chapter is the patterns that emerge from exponentiation in modular arithmetic. In normal arithmetic, powers of positive integers increase without bound, but in modular arithmetic we can focus on the *remainders* of powers, and discover some wonderful properties. For example, 10^{13} is a very large number indeed, but $10^{13} \equiv 3 \pmod 7$! In fact, because there are only a finite number of remainders for any given $n \in \mathbb{Z}^+$, for any $a \in \mathbb{Z}$ the infinite sequence of *remainders* of a^0, a^1, a^2, a^3, ... must repeat at some point.

For example, let's see what happens for each of the possible bases modulo 7:[1]

- 0: $0^1 \equiv 0 \pmod 7$, $0^2 \equiv 0 \pmod 7$
- 1: $1^1 \equiv 1 \pmod 7$, $1^2 \equiv 1 \pmod 7$
- 2: $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$, $2^4 \equiv 2 \pmod 7$
- 3: $3^1 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$, $3^3 \equiv 6 \pmod 7$, $3^4 \equiv 4 \pmod 7$, $3^5 \equiv 5 \pmod 7$, $3^6 \equiv 1 \pmod 7$, $3^7 \equiv 3 \pmod 7$
- 4: $4^1 \equiv 4 \pmod 7$, $4^2 \equiv 2 \pmod 7$, $4^3 \equiv 1 \pmod 7$, $4^4 \equiv 4 \pmod 7$
- 5: $5^1 \equiv 5 \pmod 7$, $5^2 \equiv 4 \pmod 7$, $5^3 \equiv 6 \pmod 7$, $5^4 \equiv 2 \pmod 7$, $5^5 \equiv 3 \pmod 7$, $5^6 \equiv 1 \pmod 7$, $5^7 \equiv 5 \pmod 7$
- 6: $6^1 \equiv 6 \pmod 7$, $6^2 \equiv 1 \pmod 7$, $6^3 \equiv 6 \pmod 7$

[1] Because exponentiation by positive integers corresponds to repeated multiplication, which behaves "nicely" with modular arithmetic, the list below covers all possible integers. For example, because $10 \equiv 3 \pmod 7$, we also know that $10^{13} \equiv 3^{13} \pmod 7$.

No matter which base we start with, we enter a cycle. For example, the cycle starting with 2 is $[2, 4, 1, 2, \ldots]$. We say this cycle has length 3, since it takes three elements in the sequence for the 2 to repeat. Here are the cycle lengths for each possible $a \in \{0, 1, \ldots, 6\}$:

a	Cycle length (modulo 7)
0	1
1	1
2	3
3	6
4	3
5	6
6	2

For each base other than 0, there is another way of looking at the cycle length: the cycle length for base a is the smallest positive integer k such that $a^k \equiv 1 \pmod 7$. For example, $2^3 \equiv 1 \pmod 7$, and the cycle repeats at $2^4 \equiv 2^3 \cdot 2 \equiv 2 \pmod 7$.

This "cycle length" is a fundamental property of modular exponentiation, and warrants its own definition.

Definition. Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. We define the **order of a modulo n** to be the smallest positive integer k such that $a^k \equiv 1 \pmod n$, when such a number exists.

We denote the order of a modulo n as $\text{ord}_n(a)$.

Something you might notice from our above table is that the cycle length for the remainders modulo 7 always divides 6. Here is another table, this time for modulo 17.

a	Cycle length (modulo 17)
0	1
1	1
2	8
3	16
4	4
5	16
6	16
7	16
8	8
9	8
10	16
11	16
12	16
13	4
14	16
15	8
16	2

A similar pattern emerges: the cycle length for these bases always divides 16, which is one less than 17. And again, for each base a other than 0, the cycle length corresponding to a is the least positive integer k such that $a^k \equiv 1 \pmod{17}$.

Here is one more interesting fact about cycle length: because it is a number k such that $a^k \equiv 1 \pmod{17}$, *any* multiple n of k also satisfies $a^n \equiv 1 \pmod{17}$. For example, $13^4 \equiv 1 \pmod{17}$, and so $13^{40} \equiv (13^4)^{10} \equiv 1^{10} \equiv 1 \pmod{17}$.

Combining these two observations allows us to conclude that, at least for 17, *every* base a other than 0 satisfies $a^{16} \pmod{17}$. It is a remarkable fact that this turns out to generalize to every prime number. Proving this theorem is beyond the scope of this section, but we'll state it formally here to let you marvel at it for a moment.

Theorem. (*Fermat's Little Theorem*) Let $p, a \in \mathbb{Z}$ and assume p is prime and that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod p$.

Euler's Theorem

Fermat's Little Theorem is quite beautiful in its own right, but is limited in scope to prime numbers. It turns out that the key to generalizing this theorem lies with our very last definition in this chapter.

Definition. We define the function $\varphi : \mathbb{Z}^+ \to \mathbb{N}$, called the **Euler totient function** (or **Euler phi function**), as follows:

$$\varphi(n) = \left|\{a \mid a \in \{1, \ldots, n-1\}, \text{ and } \gcd(a, n) = 1\}\right|.$$

Here are some examples of the Euler totient function:

- $\varphi(5) = 4$, since $\{1, 2, 3, 4\}$ are all coprime to 5.
- $\varphi(6) = 2$, since only $\{1, 5\}$ are coprime to 6.
- In general, for any prime number p, $\varphi(p) = p - 1$, since all the numbers $\{1, 2, \ldots, p-1\}$ are coprime to p.[2]
- $\varphi(15) = 8$, since the numbers $\{1, 2, 4, 7, 8, 11, 13, 14\}$ are all coprime to 15. Note that the "removed" numbers are all multiples of 3 or 5, the prime factors of 15.
- In general, for any two distinct primes p and q, $\varphi(pq) = (p-1)(q-1)$, although this is certainly not obvious, and requires a proof!

[2] Exercise: prove this using the definition of prime!

With the Euler totient function in hand, we can now state the generalization of Fermat's Little Theorem, called *Euler's theorem*. We'll use this theorem in the next chapter.

Theorem. (*Euler's Theorem*). For all $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, if $\gcd(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod n$.