1 Modern Cryptography

(Continued from previous notes.)

1.1 Interlude: Order

Consider the following definition of order:

Definition 1.1: Order

Fix a positive integer n. If a is an integer with $\gcd(a, n) = 1$, the order of a mod n, denoted $\text{ord}_n(a)$, is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

For example, suppose $n = 7$ and $a = 2$. We then compute

$$2^2 = 4 \pmod 7.$$

$$2^3 = 8 \equiv 1 \pmod 7.$$

Here, 3 is the smallest positive exponent such that raising 2 to the power gives us something congruent 1 mod 7, which means $\text{ord}_7(2) = 3$.

1.2 Order Lemmas

Note that $\phi(7) = 6$ and $\text{ord}_7(2) = 3$ happens to be a divisor of 6. This is no coincidence.

Lemma 1.1: First Order Lemma

Fix a positive integer n and an integer a with $\gcd(a, n) = 1$. If m is an integer with $a^m \equiv 1 \pmod{n}$, then $\text{ord}_n(a)$ divides m. In particular, $\text{ord}_n(a)$ divides $\phi(n)$.

The First Order Lemma makes it easier to compute the order of an element. Suppose, for example, we are interested in $n = 7$ and $a = 3$. The lemma guarantees that $\text{ord}_7(3)$ must be a divisor of $\phi(7) = 6$, so it can only be 1, 2, 3, or 6. We check

$$\begin{aligned} 3^1 &\not\equiv 1 \pmod 7 \\ 3^2 &= 9 \equiv 2 \not\equiv 1 \pmod 7 \\ 3^3 &= 27 \equiv 6 \not\equiv 1 \pmod 7 \\ 3^6 &= 729 \equiv 1 \pmod 7. \end{aligned}$$

So, $\text{ord}_7(3)$ cannot be 1, 2, or 3 and thus must be 6.

(Exercise.) Calculate the following orders.

(a) $\text{ord}_5(2)$

We need to find the smallest integer k such that $2^k \equiv 1 \pmod 5$. We find

$$2^1 = 2 \not\equiv 1 \pmod 5$$

$$2^2 = 4 \not\equiv 1 \pmod 5$$

$$2^3 = 8 \equiv 3 \not\equiv 1 \pmod 5$$

$$2^4 = 16 \equiv 1 \pmod 5,$$

so $\text{ord}_5(2) = 4$.

(b) $\text{ord}_9(4)$

We need to find the smallest integer k such that $4^k \equiv 1 \pmod 9$. We find

$$4^1 = 4 \not\equiv 1 \pmod 9$$

$$4^2 = 16 \not\equiv 1 \pmod 9$$

$$4^3 = 64 \equiv 1 \pmod 9,$$

so $\text{ord}_9(4) = 3$.

(c) $\text{ord}_{10}(3)$

We need to find the smallest integer k such that $3^k \equiv 1 \pmod{10}$. We find

$$3^1 = 3 \not\equiv 1 \pmod{10}$$

$$3^2 = 9 \not\equiv 1 \pmod{10}$$

$$3^3 = 27 \not\equiv 1 \pmod{10}$$

$$3^4 = 81 \not\equiv 1 \pmod{10},$$

so $\text{ord}_{10}(3) = 4$.

(d) $\text{ord}_{11}(7)$

We note that

$$\phi(11) = 11 \prod_{\substack{p \mid 11 \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) = 11\left(1 - \frac{1}{11}\right) = 11\left(\frac{10}{11}\right) = 10.$$

By the First Order Lemma, we know that $\text{ord}_{11}(7)$ divides $\phi(11)$. So, $\text{ord}_{11}(7)$ can only be 1, 2, 5, or 10. Let's try the different values:

$$7^1 = 7 \not\equiv 1 \pmod{11}$$

$$7^2 = 49 \not\equiv 1 \pmod{11}$$

$$7^5 = 7^4 7 = (7^2)^2 7 = 49^2 7 \equiv 5^2 7 = 25 \cdot 7 \equiv 3 \cdot 7 = 21 \not\equiv 1 \pmod{11}$$

$$7^{10} = (7^2)^5 = 49^5 \equiv 5^5 = 5^4 5 = (5^2)^2 5 = 25^2 5 \equiv 3^2 5 = 45 \equiv 1 \pmod{11},$$

so $\text{ord}_{11}(7) = 10$.

(e) $\text{ord}_{13}(1)$

As usual, we find the smallest integer k such that $1^k \equiv 1 \pmod{13}$. Conveniently, we find that $k = 1$ and so $\text{ord}_{13}(1) = 1$.

Lemma 1.2: Second Order Lemma

Fix a positive integer n and an integer a with $\gcd(a, n) = 1$ and let $k = \text{ord}_n(a)$. Then, $a^i \equiv a^k \pmod n$ if and only if $i \equiv j \pmod k$. In particular, the numbers $a^0, a^1, a^2, a^3, \ldots, a^{k-1}$ are all incongruent mod n.

1.3 Primitive Roots and Discrete Logarithms

The First Order Lemma tells us that $\phi(n)$ is the largest possible order mod n that any integer could have, since the order must always be a divisor of $\phi(n)$. The situation when this maximum is achieved gets a special name.

Definition 1.2: Primitive Root

Fix an integer $n \geq 2$. An integer g with $\gcd(g, n) = 1$ and $\mathrm{ord}_n(g) = \phi(n)$ is called a primitive root mod n.

For example, we saw above that $\mathrm{ord}_7(3) = 6 = \phi(7)$, so 3 is a primitive root mod 7. The Second Order Lemma tells us that $3^0, 3^1, 3^2, 3^3, 3^4, 3^5$ are all incongruent mod 7, but there are only 6 nonzero congruence classes mod 7, so the fact that all the nonzero congruence classes mod 7 must be represented among the integers $3^0, 3^1, 3^2, 3^3, 3^4, 3^5$. Let's check this explicitly.

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

All of the nonzero remainders mod 7 appear in this list. This generalizes.

Lemma 1.3: Existence of Discrete Logarithms

Fix an integer $n \geq 2$ and suppose g is a primitive root mod n. If $\gcd(a, n) = 1$, then there exists a unique k such that $0 \leq k \leq \phi(n)$ and $g^k \equiv a \pmod n$. This integer k is called the *discrete log base g of a mod n*, and is denoted $\log_g(a \pmod n)$.

So, our calculations above show that the discrete log base 3 of 6 mod 7 is 3, since $3^3 \equiv 6 \pmod 7$.

(Exercise.) For each of the following, determine whether or not the proposed value of g is actually a primitive root mod n.

(a) $n = 11, g = 2$

Recall that $\phi(11) = 10$. By the First Order Lemma, $\mathrm{ord}_{11}(2)$ must either be 1, 2, 5, or 10. So,

$$2^1 = 2 \not\equiv 1 \pmod{11},$$
$$2^2 = 4 \not\equiv 1 \pmod{11},$$
$$2^5 = 32 \equiv 10 \not\equiv 1 \pmod{11},$$
$$2^{10} = (2^5)^2 = 32^2 \equiv 10^2 = 100 \equiv 1 \pmod{11}.$$

So, in particular, we find that $\mathrm{ord}_{11}(2) = 10$. By the definition of the primitive root, since $\mathrm{ord}_{11}(2) = 10 = \phi(11)$, $g = 2$ is a primitive root.

(b) $n = 11, g = 3$

Recall that $\phi(11) = 10$. By the First Order Lemma, $\text{ord}_{11}(3)$ must either be 1, 2, 5, or 10. So,

$$3^1 = 3 \not\equiv 1 \pmod{11},$$

$$3^2 = 9 \not\equiv 1 \pmod{11},$$

$$3^5 = 3^3 \cdot 3^2 = 27 \cdot 3^2 \equiv 5 \cdot 9 = 45 \equiv 1 \pmod{11}.$$

So, $\text{ord}_{11}(3) = 5$, but because $\text{ord}_{11}(3) \neq \phi(11)$, $g = 3$ is not a primitive root.

(c) $n = 11, g = 4$

Recall that $\phi(11) = 10$. By the First Order Lemma, $\text{ord}_{11}(4)$ must either be 1, 2, 5, or 10. So,

$$4^1 = 4 \not\equiv 1 \pmod{11},$$

$$4^2 = 16 \equiv 5 \not\equiv 1 \pmod{11},$$

$$4^5 = (4^2)^2 4 = 16^2 4 \equiv 5^2 4 = 25 \cdot 4 = 100 \equiv 1 \pmod{11}.$$

So, $\text{ord}_{11}(4) = 5$, but because $\text{ord}_{11}(4) \neq \phi(11)$, $g = 4$ is not primitive root.

(Exercise.) For each of the following values of n, find *all* of the primitive roots mod n.

- $n = 5$

We find that

$$\phi(5) = 5 \prod_{\substack{p|5 \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) = 5\left(1 - \frac{1}{5}\right) = 5\frac{4}{5} = 4.$$

By the definition of the Primitive Root (1.2), we know that an integer g with $\gcd(g, 5) = 1$ and $\text{ord}_5(g) = \phi(5) = 4$ is called a primitive root.

Let's consider all $1 \leq g \leq 4$ (since, for $g > 5$, we can mod g such that it's between $0 \leq g \leq 4$; also, for $g = 0$, $g^n = 0$ and $\gcd(0, 5) = 5$.)

g	$g^1 \pmod 5$	$g^2 \pmod 5$	$g^3 \pmod 5$	$g^4 \pmod 5$
1	1			
2	2	4	3	1
3	3	4	2	1
4	4	1		

So, in particular, the order of

- $g = 1$ is 1,
- $g = 2$ is 4,
- $g = 3$ is 4,
- $g = 4$ is 1.

Because $\phi(5) = 4$ and $\text{ord}_5(2) = \text{ord}_5(3) = 4$, it follows that 2 and 3 are the primitive roots.

- $n = 7$

We know that $\phi(7) = 6$. By the definition of the Primitive Root (1.2), we know that an integer g with $\gcd(g, 7) = 1$ and $\text{ord}_7(g) = \phi(7) = 6$ is called a primitive root.

Let's consider all $1 \leq g \leq 6$.

g	$g^1 \pmod 7$	$g^2 \pmod 7$	$g^3 \pmod 7$	$g^4 \pmod 7$	$g^5 \pmod 7$	$g^6 \pmod 7$
1	1					
2	2	4	1			
3	3	2	6	4	5	1
4	4	2	1			
5	5	4	6	2	3	1
6	6	1				

So, in particular, the order of

- $g = 1$ is 1,
- $g = 2$ is 3,
- $g = 3$ is 6,
- $g = 4$ is 3,
- $g = 5$ is 6,
- $g = 6$ is 2.

Because $\phi(7) = 6$ and $\text{ord}_7(3) = \text{ord}_7(5) = 6$, it follows that 3 and 5 are the primitive roots.

- $n = 11$

We know that $\phi(11) = 10$. By the definition of the Primitive Root (1.2), we know that an integer g with $\gcd(g, 11) = 1$ and $\text{ord}_{11}(g) = \phi(11) = 10$ is called a primitive root.

Let's consider all $1 \leq g \leq 10$ (note that the columns g^x for $x = 1, 2, \ldots$ are mod 11.)

g	g^1	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}
1	1									
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1					
4	4	5	9	3	1					
5	5	3	4	9	1					
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1					
10	10	1								

So, in particular, because $\phi(11) = 10$ and $\text{ord}_{11}(2) = \text{ord}_{11}(6) = \text{ord}_{11}(7) = \text{ord}_{11}(8) = 10$, it follows that 2, 6, 7, 8 are the primitive roots.

(Exercise.) For each of the following, find the discrete log base g of a mod n.

(a) $n = 7, g = 3, a = 5$

We know that $\phi(7) = 6$, so by lemma (1.3) there exists a unique integer k such that $0 \le k \le 6$ and $3^k \equiv 5 \pmod 7$. So,

$$3^0 = 1 \not\equiv 5 \pmod 7,$$

$$3^1 = 3 \not\equiv 5 \pmod 7,$$

$$3^2 = 9 \equiv 2 \not\equiv 5 \pmod 7,$$

$$3^3 = 27 \equiv 6 \not\equiv 5 \pmod 7,$$

$$3^4 = 81 \equiv 4 \not\equiv 5 \pmod 7,$$

$$3^5 = 3^4 3 = 9^2 3 = 81(3) \equiv 4(3) = 12 \equiv 5 \pmod 7.$$

So, in particular, $k = 5$.

(b) $n = 5, g = 2, a = 4$

We know that $\phi(5) = 4$, so by lemma (1.3) there exists a unique integer k such that $0 \le k \le 4$ and $2^k \equiv 4 \pmod 5$. So,

$$2^0 = 1 \not\equiv 4 \pmod 5,$$

$$2^1 = 2 \not\equiv 4 \pmod 5,$$

$$2^2 = 4 \pmod 5.$$

By said lemma, we have $k = 2$.

(c) $n = 11, g = 2, a = 3$

We know that $\phi(11) = 10$, so by lemma (1.3) there exists a unique integer k such that $0 \le k \le 10$ and $2^k \equiv 3 \pmod{11}$. Additionally, by lemma (1.2) we know that $2^0, 2^1, \ldots, 2^8, 2^9$ are all incongruent mod 11, so we only care about $0 \le k \le 9$. So,

$$2^0 = 1 \not\equiv 3 \pmod{11},$$

$$2^1 = 2 \not\equiv 3 \pmod{11},$$

$$2^2 = 4 \not\equiv 3 \pmod{11},$$

$$2^3 = 8 \not\equiv 3 \pmod{11},$$

$$2^4 = 16 \equiv 5 \not\equiv 3 \pmod{11},$$

$$2^5 = 2^4 2 \equiv 5 \cdot 2 = 10 \not\equiv 3 \pmod{11},$$

$$2^6 = 2^5 2 \equiv 10 \cdot 2 = 20 \equiv 9 \not\equiv 3 \pmod{11},$$

$$2^7 = 2^6 2 \equiv 9 \cdot 2 = 18 \equiv 7 \not\equiv 3 \pmod{11},$$

$$2^8 = 2^7 2 \equiv 7 \cdot 2 = 14 \equiv 3 \pmod{11}.$$

So, by said former lemma, $k = 8$.

1.4 Existence of Primitive Roots

We haven't yet shown that primitive roots always exist, and in fact, it is not true that primitive roots always exist. Here is the statement:

Theorem 1.1: Primitive Root Theorem

Fix an integer $n \geq 2$. Then, there exists a primitive root mod n if and only if $n = 2, 4, p^k, 2p^k$ for an odd prime p and a positive integer k. In particular, there always exists a primitive root mod p (a prime).

(Exercise.) Use the Primitive Root Theorem to find the 5 smallest integers $n \geq 2$ such that there does *not* exist a primitive root mod n.

Referring to theorem (1.1), we know that every prime has a primitive root. In other words, we know that

- 2, 4 are special cases.
- 3, 5, 7, 11, 13, 17, 19, etc. are all primes.
- 6, 10, 14, 22, 26, etc. all have primitive roots (these are just primes multiplied by 2, i.e., $2p^1$, but we omitted 2 since we only care about odd primes).
- 9, 25, 49, 121, etc. all have primitive roots (these are just the primes multiplied by themselves, i.e., p^2).
- 18, 50, 98, etc. all have primitive roots (these are just $2p^2$, but notice how we omitted 8 because powers only apply to odd primes).

So, in particular, 8, 12, 15, 16, 20.