Order of Elements

Reading

- Section 10.1

Practice Problems

10.1 2, 3, 5, 6, 7, 11, 14, 15
10.1 (Challenge, Optional) 25-31 (The point of these exercises is to show that computing the order of an element is as hard as factoring the modulus)

Notes

Order of Elements

The reduced residues modulo n form a group under multiplication. In this section we start the study of this group, that has many interesting properties. We will not however assume knowledge of group theory.

> Let $\bar{a} \in \mathbb{Z}_n$ be a reduced residue. The **order** of $\bar{a}$, also called the order of a modulo n, is the smallest positive r such that:
>
> $$\bar{a}^k = 1$$
>
> It is denoted $ord_n(a)$.

As an example, let's recall the orders of various elements modulo 11:

- $ord_{11}(2) = 10$
- $ord_{11}(3) = 5$
- $ord_{11}(4) = 5$
- $ord_{11}(4) = 5$
- $ord_{11}(10) = 2$

Here are some key properties of orders of elements:

> Let a be a reduced residue modulo n with order r. Then:
>
> - For a power e we have $\bar{a}^e = \bar{1} \bmod n$ if and only if r divides e.
> - In particular, r must divide $\phi(n)$.
> - For two powers j, k we have $\bar{a}^j = \bar{a}^k \bmod n$ if and only if $j = k \bmod r$.
> - For any j, we have $ord(\bar{a}^j)|r$.

    - More precisely, $ord(\bar{a}^j) = \frac{r}{\gcd(j,r)}$

- We start by proving the first property.
    - Suppose $a^e = 1$ and perform Euclidean division: $e = kr + r'$.
    - Then $1 = a^e = a^{kr}a^{r'} = 1 \cdot a^{r'}$.
    - So $a^{r'} = 1$. Since $r' < r$, and r was defined to be the smallest positive integer that makes $a^r = 1$, we must have that $r' = 0$.
    - So $e = kr$ is a multiple of r.
    - The converse is straightforward: If $e = kr$ then $a^e = (a^r)^k = 1$
- For the third property:
    - The first condition is equivalent to $\bar{a}^{j-k} = 1 \bmod n$.
    - The second condition is equivalent to $j - k = 0 \bmod r$, which in turn is equivalent to $r|j - k$.
    - The equivalence of these two then follows from the first property.
- For the fourth property:
    - Note that $(a^j)^r = (a^r)^j = 1$. So r is a number that makes a^j equal to 1 when raised to it. So by our first property it must be the case that $ord(a^j)|r$.
- For the fifth property:
    - Let $d = \gcd(j, r)$, $r' = r/d$.
    - We must first show that $(a^j)^{r'} = 1$.
        * Since $d|j$, we also have $r = r'd|r'j$.
        * Hence $(a^j)^{r'} = a^{r'j}$ must also equal 1.
    - Now we must show that it is the smallest such positive power.
        * Suppose $(a^j)^k = 1$.
        * Then $a^{jk} = 1$.
        * Since $d = mj + \ell r$, we also get $dk = mjk + \ell rk$.
        * So $dk = mjk \bmod r$.
        * So we must also have $a^{dk} = (a^{jk})^m = 1$.
        * So $dk \geq r$ (assuming k is positive).
        * So $k \geq r/d = r'$.

Let us see an illustration of some of these results.

- By direct computation we can see that $2^{10} = 1 \bmod 11$ and that is the first power of 2 that equals 1. So the order of 2 modulo 11 is 10.
- Suppose $j = 6$, so $2^6 = (2^3)^2 = 8^2 = (-3)^2 = 9 \bmod 11$.
- Since $\gcd(6, 10) = 2$, and $r' = 10/2 = 5$, we should expect 9 to have order 5.
- In fact $9^5 = (-2)^5 = -10 = 1 \bmod 11$.
- Since 5 is a prime power, there is no smaller power that would divide into it. Hence it must be the order of 9. So it must indeed be the order of 9.
- Similarly consider $j = 5$, so $2^5 = 32 = 10 \bmod 11$. Then it should have order $10/\gcd(5, 10) = 10/5 = 2$. In fact this is the case.