Element Order in Number Theory

Wim Ruitenburg

These are notes useful for our Number Theory class.

1 The Order of an Element

Let $n > 1$ be a natural number. The *order* modulo n of an $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ is the least $m > 0$ such that $a^m \equiv 1 \bmod n$. Equation $\gcd(a, n) = 1$ holds exactly when there are s and t such that $sa + tn = 1$ exactly when a is invertible modulo n (in this case $as \equiv 1 \bmod n$).

By Euler's Theorem we know that $a^{\varphi(n)} \equiv 1 \bmod n$. So the order of a modulo n divides $\varphi(n)$. For example when $n = 15$, then $\varphi(15) = (3-1)(5-1) = 8$. Since $\gcd(2, 15) = 1$ we have $2^8 \equiv 1 \bmod 15$. We easily see that 2 has order 4 modulo 15 since $2^4 \equiv 1 \mod 15$. Obviously order 4 divides $\varphi(15) = 8$. Element a is called *primitive* modulo n if its order equals $\varphi(n)$. For example modulo $n = 10$ we have $\varphi(10) = (2-1)(5-1) = 4$ and the invertible elements are 1 of order 1, 3 of order 4, 7 of order 4, and 9 of order 2. So 3 and 7 are the primitive elements modulo 10. However, there are $n > 1$ for which there are no primitive elements. For example modulo $n = 15$ the invertible elements are 1, 2, 4, 7, 8, 11, 13, and 14, whose orders all divide 4, while $\varphi(15) = 8$.

When do we have primitive elements modulo n? The following Proposition helps a little.

Proposition 1.1. *Let a and b be invertible elements modulo n of orders k and l respectively, where $\gcd(k, l) = 1$. Then ab has order kl modulo n.*

Proof. Since $(ab)^{kl} = a^{kl}b^{kl} \equiv 1 \bmod n$, we have that the order of ab modulo n divides kl. There is a least s with $0 < s \leq kl$ with $(ab)^s = a^s b^s \equiv 1 \bmod n$. So $a^s \equiv (b^{-1})^s \bmod n$. Now the order of a^s modulo n divides k while the order of $(b^{-1})^s$ modulo n divides l. Since $a^s \equiv (b^{-1})^s \bmod n$, their orders are the same modulo n. Thus their order modulo n divides $\gcd(k, l) = 1$. Thus $a^s \equiv (b^{-1})^s \equiv 1 \bmod n$, that is, the orders of a and b^{-1} divide s. Since a has order k and b^{-1} has order l, we have that least common multiple kl divides s. Thus $s = kl$. □

Let us look at the special case when $n = p$ is prime. Then $\varphi(p) = p - 1$, and $\gcd(a, p) = 1$ for all $a \in \{1, 2, 3, 4, \ldots, p-1\}$. So if $0 < a < p$, then $a^{p-1} \equiv 1 \bmod p$ (Fermat's Little Theorem). So the order of a modulo p divides $p - 1$. Element a is primitive if its order equals $p - 1$. Below we show that we have primitive elements modulo prime p.

First a brief story about polynomials $a_0 + a_1X + a_2X^2 + \ldots + a_mX^m \bmod p$. We can add, subtract, and multiply such polynomials as we are used to, except that we take the coefficients modulo prime p. An important property that holds modulo prime p but not always modulo a composite number n is that the degree of a product of two non-zero polynomials equals the sum of the degree of these polynomials,as is easily seen when we look at the product

$$(a_0 + a_1X + \ldots + a_kX^k)(b_0 + b_1X + \ldots + b_lX^l) =$$
$$a_0b_0 + (a_1b_0 + a_0b_1)X + \ldots + a_kb_lX^{k+l},$$

where $a_k \not\equiv 0 \bmod p$ and $b_l \not\equiv 0 \bmod p$ imply that $a_k b_l \not\equiv 0 \bmod p$. As a consequence a polynomial modulo prime p can have no more roots than its degree, even when we count multiplicities of roots. This is a key property which always works modulo primes p, but not so modulo composite numbers.

Now look at polynomial $X^{p-1}-1$ modulo prime p. This polynomial has at most $p-1$ roots modulo p. By Fermat's Little Theorem all $p-1$ elements $a \in \{1,2,3,4,\ldots,p-1\}$ are such that $a^{p-1}-1 \equiv 0 \bmod p$. So these are all the roots. So

$$X^{p-1}-1 \equiv (X-1)(X-2)(X-3)(\ldots)(X-(p-1)) \bmod p.$$

Recall from geometric sequences the simple formula

$$Y^m - 1 = (Y-1)(Y^{m-1}+Y^{m-2}+\ldots+Y+1).$$

So for all positive k and l we have

$$X^{kl}-1 = (X^k-1)(X^{k(l-1)}+X^{k(l-2)}+\ldots+X^k+1).$$

When $p-1=kl$, the formula above applies to $X^{p-1}-1 = X^{kl}-1$, which splits into a product of $p-1$ different linear factors of the form $X-i$ modulo p. So therefore X^k-1 is a product of k such linear factors $X-i$ of all the i such that $i^k \equiv 1 \bmod p$. Integer $p-1$ has a standard prime decomposition $p-1 = p_1^{r_1}p_2^{r_2}\ldots p_s^{r_s}$. Set $k = p_1^{r_1}$ and $l = p_2^{r_2}\ldots p_s^{r_s}$. So

$$X^{p-1}-1 = (X^{p_1^{r_1}}-1)(X^{p_1^{r_1}(l-1)}+X^{p_1^{r_1}(l-2)}+\ldots+X^{p_1^{r_1}}+1).$$

Factor $X^{p_1^{r_1}}-1$ equals a product of $p_1^{r_1}$ many factors of the form $X-i$ modulo p. Each i of such a factor $X-i$ is such that $i^{p_1^{r_1}} \equiv 1 \bmod p$. So the order of this i divides $p_1^{r_1}$. Next we show that $p_1^{r_1}-p_1^{r_1-1}$ many of these i have order equal to $p_1^{r_1}$. Here is how. All roots i of $X^{p_1^{r_1}}-1$ that have order less than $p_1^{r_1}$, have an order that divides $p_1^{r_1-1}$, and so are roots of the polynomial $X^{p_1^{r_1-1}}-1$ modulo p. But

$$X^{p_1^{r_1}}-1 = (X^{p_1^{r_1-1}}-1)(X^{p_1^{r_1-1}(p_1-1)}+X^{p_1^{r_1-1}(p_1-2)}+\ldots+X^{p_1^{r_1-1}}+1)$$

splits into linear factors. All i of order less than $p_1^{r_1}$ are roots of $X^{p_1^{r_1-1}}-1$ modulo p. There are $p_1^{r_1}-p_1^{r_1-1}$ roots left, which all have order $p_1^{r_1}$ modulo p.

What works for prime power $p_1^{r_1}$ above works for all prime powers that divide $p-1$. So for all such $p_i^{r_i}$ there is an element a_i of order $p_i^{r_i}$ modulo p. By Proposition 1.1 the product $c = a_1 a_2 \ldots a_s$ has order $p-1 = p_1^{r_1}p_2^{r_2}\ldots p_s^{r_s}$ modulo prime p. Thus c is primitive.

We showed elsewhere (with a short proof) that if there is one primitive element modulo n, then there are $\varphi(\varphi(n))$ many primitive elements modulo n. So there are $\varphi(p-1)$ many primitive elements modulo prime p. Note that this also follows with the calculations above.