1. INTRODUCTION

Euler’s theorem says for any positive integers $a, n$ with $(a, n) = 1$, that $a^{\varphi(n)} \equiv 1 \mod n$.

**Definition 1.1.** The *order of $a$ mod $n$*, $\text{ord}_n(a)$ is defined as the smallest positive integer $k$ such that $a^k \equiv 1 \mod n$.

Using the language of orders, Euler’s theorem immediately tells us the following:

**Corollary 1.2.** $\text{ord}_n(a) \leq \varphi(n)$

The question we will answer is the following: for which $n$ is it true that equality is achievable? In other words, for which $n$ is there an integer $a$ with $\text{ord}_n(a) = \varphi(n)$? For an integer $a$ with maximal possible order, we give it a special name:

**Definition 1.3.** For an integer $a$ with $\text{ord}_n(a) = \varphi(n)$, we call $a$ a *generator mod $n$*, or a *primitive root mod $n$*.

**Example 1.4.** By direct computation, we find that $\text{ord}_7(3) = 6$, so that 3 is a generator mod 7. However, we see that every integer co-prime to 8 has order 2 mod 8, so that there is no generator mod 8.

The example illustrates that there is some subtlety in our question. Why is such a question even interesting? Suppose we know there is a generator $g$ mod $n$. Then the powers $\{1, g, g^2, g^3, \ldots, g^{\varphi(n)}\}$ are $\varphi(n)$ distinct invertible elements mod $n$. We know that the total count of invertible elements mod $n$ is $\varphi(n)$, so this set hits all of them. This makes doing arithmetic mod $n$ very easy!

2. PROPERTIES OF ORDERS

We’ll start by proving some basic properties of $\text{ord}_n(a)$.

**Proposition 1.** $a^k \equiv 1 \mod n \iff \text{ord}_n(a) \mid k$

*Proof.* Let $m = \text{ord}_n(a)$. By the division algorithm, write $n = mq + r$ with $0 \leq r < m$. We have $a^n = a^{mq+r} = (a^m)^q \cdot a^r \equiv a^r \equiv 1 \mod n$. By definition of $m$, it’s the smallest positive integer $m$ with the property that $a^m \equiv 1 \mod n$, so this forces $r = 0$ since $r < m$. This says $n = mq$, so $\text{ord}_n(a) \mid n$.

Conversely, suppose that $\text{ord}_n(a) \mid k$. Set $m = \text{ord}_n(a)$, and write $k = mq$ for some integer $q$. We then have $a^k = (a^m)^q \equiv 1 \mod n$ as desired. \qed

**Proposition 2.** For any $k \geq 1$, we have $\text{ord}_n(a^k) = \frac{m}{(m,k)}$ where $m = \text{ord}_n(a)$. 


Lemma 3.2. For any $1 \leq m \leq (m, k)$, we find $\phi(d, \frac{m}{(m, k)})$ determine which of these powers have order $T^d$. Proof.

Proposition 3. Suppose that $\text{ord}_n(a) = m$ and $\text{ord}_n(b) = \ell$ and $(m, \ell) = 1$. Then $\text{ord}_n(ab) = m\ell$.

Proof. Let $t = \text{ord}_n(ab)$. We have $(ab)^{m\ell} = a^{m\ell}b^{m\ell} \equiv 1 \pmod{m\ell}$. Therefore, we wish to determine which of these powers have order $t$. By definition, $a^t \equiv 1 \pmod{m\ell}$ so $\ell \mid t$. Similarly, raising both sides to the $\ell$ power we have $a^\ell \equiv 1 \pmod{m\ell}$, so $m \mid t\ell$. Since $(m, \ell) = 1$ this means that $m \mid t$ and $\ell \mid t$, and therefore $m\ell \mid t$. This says $\text{ord}_n(ab) = t = m\ell$ as desired.

Proposition 4. Let $m, n$ be positive integers with $(m, n) = 1$. Then $\text{ord}_{mn}(a) = \text{lcm}(\text{ord}_m(a), \text{ord}_n(a))$.

Proof. Let $t = \text{ord}_{mn}(a)$ and $k = \text{lcm}(\text{ord}_m(a), \text{ord}_n(a))$. Then $a^t \equiv 1 \pmod{mn}$, so $a^t \equiv 1 \pmod{m}$ and $a^t \equiv 1 \pmod{n}$. This says $\text{ord}_m(a) \mid t$ and $\text{ord}_n(a) \mid t$ so $k \mid t$. On the other hand, let $k = \text{lcm}(\text{ord}_m(a), \text{ord}_n(a))$. Then $a^k \equiv 1 \pmod{m}$ and $a^k \equiv 1 \pmod{n}$ so by the Chinese remainder theorem, $a^k \equiv 1 \pmod{mn}$, so $t \mid k$ says $t = k$ as desired.

3. Generators mod $p$

We’ll start by showing that for an odd prime $p$, there is always a generator mod $p$. The proof relies on the following observation:

Lemma 3.1. Let $N_p(d)$ be the number of integers mod $p$ with $\text{ord}_p(a) = d$. If $N_p(d) > 0$, then $N_p(d) = \varphi(d)$.

Proof. Suppose that $\text{ord}_p(a) = d$. Then $a^d \equiv 1 \pmod{p}$, so $a$ is a root of the polynomial $T^d - 1 \pmod{p}$. Since this polynomial has degree $d$, it has at most $d$ roots mod $p$. Note that $1, a, a^2, \ldots, a^{d-1}$ are distinct roots of $T^d - 1$, so these are all the roots. Therefore, we wish to determine which of these powers have order $d$. By proposition 2, $\text{ord}_p(a^k) = d \iff (k, d) = 1$, and there are precisely $\varphi(d)$ such exponents that work.

Lemma 3.2. For any $n \geq 1$, we have $n = \sum_{d|n} \varphi(d)$.

Proof. By computing the sum backwards, we find $\sum_{d|n} \varphi(d) = \sum_{dd'=n} \varphi(d') = \sum_{dd'=n} \varphi(d') = \sum_{d|n} \varphi(n/d)$. By definition, $\varphi(n/d) = \#\{1 \leq k \leq n/d : (k, n/d) = 1\}$ i.e., $\varphi(d)$ counts the number of integers between 1 and $n/d$ that are co-prime to $n/d$. Note that $(k, n/d) = 1 \iff (dk, n) = d$. If $(m, n) = d$, this means $m = dk$ for some $1 \leq k \leq n/d$, so this means $\varphi(n/d) = \#\{1 \leq m \leq n : (m, n) = d\}$. That is to say, $\varphi(n/d)$ is the number of integers $m$ with $(m, n) = d$. Let $S_d = \{1 \leq m \leq n : (m, n) = d\}$, so that $S_d$ has size $\varphi(n/d)$. For any $1 \leq m \leq n$, we have $(m, n) = d$ for some integer $d$, so $m$ falls into one of the sets $S_d$. Summing up the sizes of all such $S_d$, we find $n = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)$ as desired.

Theorem 3.3. There are $\varphi(p-1)$ generators mod $p$.

Proof. For any unit $a$ mod $p$, we have $\text{ord}_p(a) \mid p-1$. There are $p-1$ units mod $p$, so we must have $p-1 = \sum_{d|p-1} N_p(d)$. Lemma 3.1 says that $N_p(d) \leq \varphi(d)$ ($N_p(d)$ could be 0!)
By the binomial theorem, we have (g) means that ord does not divide c is an integer c is an integer N so particular, this means that N(p − 1) = ϕ(p − 1), which is what we wanted.

Note that we cannot just easily adapt our proof above to work for an arbitrary n. This is because lemma 3.1 does not generalize to a non-prime modulus! The subtlety is that a polynomial of degree d can have more than d roots mod n. For example, T^2 − 1 has 4 roots mod 8.

4. Generators mod pk

To show there is a generator mod pk for k ≥ 2 and p an odd prime, our approach will be the lifting philosophy: starting with a generator g mod p, we should be able to lift it to a generator mod pk for all k ≥ 2.

Lemma 4.1. There is a generator mod pk.

Proof. Let g be a generator mod p, so that g is a root of the polynomial f(T) = Tp−1 − 1 mod p. Since f(T) = 0 mod p and f’(T) = (p − 1)gp−2 ≠ 0 mod p, by Hensel’s lemma, there is an integer c with c ≡ g mod p such that f(g + cp) = 0 mod p^2, i.e. (g + cp)p−1 ≡ 1 mod p^2.

By the binomial theorem, we have (g + cp)p−1 = gp−1 + cp(p − 1) + · · · + (cp)p−1. Since p does not divide c(p − 1), working mod p^2, this says 1 ≡ (g + cp)p−1 ≡ gp−1 − cp mod p^2, so gp−1 ≡ 1 + cp ≡ 1 mod p^2. Since (gp−1)p = gp(p−1) ≡ 1 mod p^2 by Euler’s theorem, this means that ord_p(gp−1) = p. Now, set t = ord_p(g + cp). Since (g + cp)p−1 ≡ 1 mod p^2, this means that t | p − 1. We have 1 ≡ (g + cp)^t mod p^2, so 1 ≡ g^t mod p. Since g is a generator mod p, this means that p − 1 | t, so that t = p − 1. By proposition 3, this means that (g + cp)gp−1 has order p(p − 1) = ϕ(p^2) as desired.

Theorem 4.2. If g is a generator mod p^2, then g is a generator mod pk for all k ≥ 2. In particular, there is a generator mod pk for k ≥ 2.

Proof. By the above lemma, there is a generator g mod p^2. We’ll show that g is a generator mod pk for all k ≥ 2 by induction. The case k = 2 is true by assumption, so suppose we know that g is a generator mod pk for some k, i.e. that ord_{pk}(g) = pk−1(p − 1). Let t = ord_{pk+1}(g). Since gpk−1(p−1) ≡ 1 mod pk+1, this says t | pk(p − 1), and since g^t ≡ 1 mod pk, this says pk−1(p − 1) | t. Combining these two divisibilities, this says either t = pk−1(p − 1) or t = pk(p − 1). Therefore, it’s sufficient to prove that gpk−1(p−1) ≠ 1 mod pk+1. Since gp−1 ≡ 1 mod p, we can write gp−1 = 1 + pl for some l, and since g is a generator mod p^2, we know that l ≡ 0 mod p. We compute gp(p−1) = (1 + pl)p = 1 + p^2l + · · · + (pl)p ≡ 1 + p^2l mod p^3.

Now, we have (gp−1)p^2 ≡ (1 + p^2l)p ≡ 1 + plp^3 mod p^4. Repeating this procedure, we find that (gp−1)p^{k−1} ≡ 1 + lp^k mod pk+1. This proves that t = pk(p − 1), so by induction, we’re done.

Note that unlike the proof that there is a generator mod p, the proof above is constructive. Once we know a generator mod p, we can explicitly find a generator mod pk for k ≥ 2.

Example 4.3. Suppose that g is a generator mod p. We’ll explicitly construct a generator mod p^2. The proof of 4.1 says our generator will be (g + cp)gp−1, where c comes from the proof of Hensel’s lemma. Explicitly going through the proof, set f(T) = Tp−1 − 1. We have f(g + cp) ≡ f(g) + f’(g)cp mod p^2. Since f(g) ≡ 0 mod p, we choose c so that p\left(\frac{f(g)}{p}\right) +
\(f'(g)c \equiv 0 \pmod{p^2}\), i.e. \(\frac{f(g)}{p} + f'(g)c \equiv 0 \pmod{p}\). Solving for \(c\) says \(c \equiv -\frac{f(g)}{p}[f'(g)]^{-1} \pmod{p}\).

Since \(f'(g) \equiv (p - 1)g^{p-2} \pmod{p}\), we see that \([f'(g)]^{-1} \equiv -g \pmod{p}\), so \(c \equiv \frac{f(g)}{p}g \pmod{p}\).

Therefore, our generator is given by \((g + \frac{f(g)}{p}g)p^{p-1} = (1 + f(g))g^p = g^{p-1}g^p = g^{2p-1}\).

As an explicit example, we mentioned earlier that 3 is a generator mod 7, so \(3^{13} \equiv 10 \pmod{49}\) says 10 is a generator mod 49, and therefore a generator mod \(7^k\) \(k \geq 2\).

5. Generators mod \(2^k\)

Unfortunately, we cannot adapt our proof above for \(p = 2\). What breaks down is the last step, that \((g^{p-1})^{\ell} \equiv 1 + p^{k+1}\ell \pmod{p^{k+2}} \Rightarrow (g^{p-1})^{\ell+1} \equiv 1 + p^{k+2}\ell \pmod{p^{k+3}}\). What goes wrong? When \(p = 2\), if \(g^{2^k} \equiv 1 + 2^{k+1}\ell \pmod{2^{k+2}}\), then \(g^{2^{k+1}} \equiv 1 + 2^{k+2}\ell + 2^{2k+2}\ell^2 \pmod{2^{k+3}}\), and the last term only disappears as long as \(2k + 3 \geq k + 3\), i.e. \(k \geq 1\). This means the \(k = 0\) step doesn’t hold, i.e. that a generator mod 4 doesn’t necessarily lift to a generator mod 8! Indeed, we see this is false, as there are no generators mod 8.

**Theorem 5.1.** There is a generator mod \(2^k\) if and only if \(k = 1\) or \(k = 2\).

**Proof.** If \(k = 1\), then 1 is a generator mod 2. If \(k = 2\), then 3 is a generator mod 4. Now we show that if \(k \geq 3\), that there is no generator mod \(2^k\). Suppose otherwise, that \(g\) is a generator mod \(2^k\) for some \(k \geq 3\). This means \(g^{2^{k-1}} \equiv 1 \pmod{2^k}\). Since \(g\) is a generator, the powers \(\{1, g, g^2, \ldots, g^{2^{k-2}}\}\) are the \(2^{k-1}\) different units mod \(2^k\). We have \(g^2 = 1 \pmod{2^k}\) for some \(\ell\). Squaring says \(g^{2\ell} = 1 \pmod{2^k}\), so \(2^{k-1} | 2\ell\) says \(2^{k-2} | \ell\), i.e. \(2^{k-2} = \ell\). On the other hand, we have \(g^{2^k} \equiv 1 \pmod{8}\) since every unit squares to 1 mod 8. This says \(g^2 = 1 + 8\ell\) for some \(\ell\), so that \(g^4 \equiv (1 + 8\ell)^2 \equiv 1 \pmod{16}\). Inductively repeating this, we find that \(g^{2^{k-2}} \equiv 1 \pmod{2^k}\), which says \(1 \equiv -1 \pmod{2^k}\), a contradiction. Therefore, there is no generator mod \(2^k\) for \(k \geq 3\). \(\square\)

6. Generators mod \(n\)

We’re now ready to tackle the question of when there is a generator mod \(n\) for general \(n\).

**Theorem 6.1.** There is a generator mod \(n\) if and only if \(n = 2, 4, p^k, 2p^k\) for \(p\) an odd prime and \(k \geq 1\).

**Proof.** If \(n = 2, 4, p^k\) we have seen this already. If \(n = 2p^k\), let \(g\) be a generator mod \(p^k\). If \(g\) is odd, then \(g\) has order 1 mod 2 and \(g\) has order \(\varphi(p^k)\) mod \(p^k\); so \(g\) has order \(\varphi(p^k) = \varphi(2p^k)\) mod \(2p^k\) by proposition 4, and therefore is a generator. If \(g\) is even, then \(g + p^{k-1}\) is odd, and it’s easy to check that \(\text{ord}_{p^k}(g + p^{k-1}) = \text{ord}_{p^k}(g)\), so \(g + p^{k-1}\) is a generator mod \(2p^k\).

Conversely, write \(n = 2e^{p_1^{e_1}} \cdots p_k^{e_k}\). We have \(\text{ord}_n(a) = \text{lcm}(\text{ord}_{2^e}(a), \text{ord}_{p_1^{e_1}}(a), \ldots, \text{ord}_{p_k^{e_k}}(a))\).

For each \(i\), we have \(\text{ord}_{p_i^{e_i}}(a) \leq \varphi(p_i^{e_i})\). If \(e \geq 3\), the proof of 5.1 says \(\text{ord}_{2^e}(a) \leq 2e - 2\), so \(\text{ord}_n(a) < 2e - 2\varphi(p_1^{e_1} \cdots p_k^{e_k}) < \varphi(n)\). If we have at least two odd prime factors \(p_1\) and \(p_2\), then both \(\varphi(p_1^{e_1})\) and \(\varphi(p_2^{e_2})\) are even, and \(\text{lcm}(\text{ord}_{p_1^{2e}}(a), \text{ord}_{p_1^{e_1}}(a)) < \varphi(p_1^{e_1}p_2^{e_2})\) so that \(\text{ord}_n(a) < \varphi(n)\). This leaves the only possible cases of \(n = 2e^{p^k}\) where \(e = 0, 1\) and \(k \geq 0\), which leaves the 4 possible cases above. \(\square\)
7. Applications

As an application of theorem 6.1, we give a generalization of Wilson’s theorem.

**Theorem 7.1 (Wilson).** For a prime $p$, $(p - 1)! \equiv -1 \mod p$.

**Theorem 7.2 (Gauss).** Let $n \geq 2$. Then

$$\prod_{(k,n) = 1}^n k \equiv \begin{cases} -1 \mod n & n = 2, 4, p^k, 2p^k \\ 1 \mod n & \text{otherwise} \end{cases}$$

for some odd prime $p$ and $k \geq 1$.

**Lemma 7.3.** The number of solutions to $x^2 \equiv 1 \mod 2^e$ is 4 for $e \geq 3$.

**Proof.** Note that $\pm 1, \pm 1 + 2^{e-1} \mod 2^e$ are four solutions to $x^2 \equiv 1 \mod 2^e$. We’ll prove that these are the only solutions. This is true for $e = 3$, so assume it’s true for some $e \geq 3$. If $a^2 \equiv 1 \mod 2^{e+1}$, then $a^2 \equiv 1 \mod 2^e$, so $a$ must be one of the four solutions listed. Write $a = \pm 1 + 2^{e-1}k + 2^e\ell$ for some $\ell \in \mathbb{Z}$ and $k \in \{0, 1\}$. Then $a^2 = 1 + 2^{2e-2}k^2 + 4^e\ell^2 \pm 2^e k \pm 2^{e+1}\ell + 4^ek\ell$. Since $2e - 2 \geq e + 1$, reducing mod $2^{e+1}$ says $a^2 \equiv 1 + 2^e k \mod 2^{e+1}$. By assumption, this forces $k = 0$, i.e. $a \equiv \pm 1 \mod 2^e$. Thus, $a = \pm 1 + 2^e\ell$. If $\ell$ is even, then $a \equiv \pm 1 \mod 2^{e+1}$, and if $\ell$ is odd, then $a \equiv \pm 1 + 2^e \mod 2^{e+1}$, which is what we wanted. By induction, the result holds true for $e \geq 3$.

**Proof of theorem 7.2.** The case of $n = 2, 4$ are trivial, so suppose that $n = p^k, 2p^k$. Then by theorem 6.1, there is a generator $g \mod n$. The invertible elements mod $n$ are given by $1, g, g^2, \ldots, g^{\varphi(n)-1}$. Therefore, $\prod_{(k,n) = 1}^n k \equiv \prod_{i=0}^{\varphi(n)-1} g^i \equiv g^{\sum_{i=0}^{\varphi(n)-1} i} \mod n$. We have $\sum_{i=0}^{\varphi(n)-1} i = \frac{\varphi(n)(\varphi(n)-1)}{2}$. Since $g$ is a generator mod $n$, $g^{\varphi(n)/2} \equiv -1 \mod n$, and since $n > 2$ we have $\varphi(n)$ is even, so $\varphi(n) - 1$ is odd. Therefore, $g^{\varphi(n)/2}^{\varphi(n)/2} \equiv (g^{\varphi(n)/2})^{\varphi(n)-1} \equiv -1 \mod n$.

Let $S_d = \{1 \leq a \leq n : \text{ord}_n(a) = d\}$, the set of elements mod $n$ with order $d$. If $a \in S_d$, then $a^{d-1} \in S_d$ because $(d - 1, d) = 1$. This says we can group all elements of $S_d$ into pairs $(a, a^{d-1})$ (which are distinct for $d \neq 2$), whose product is 1 mod $n$. Therefore, the product of all elements in $S_d$ is 1 mod $n$ for $d \geq 3$.

It remains to analyze the set $S_2$, the set of elements of order 2. If $a \in S_2$, then $-a \in S_2$, so $S_2$ consists of pairs of elements $(a, -a)$. Since $a \in S_2$ means $a^2 \equiv 1 \mod n$, then the product of all elements in $S_2$ is given by $(-1)^k$, where $k$ is the number of pairs $(a, -a) \in S_2$. To answer this, we must count the number of solutions to $x^2 \equiv 1 \mod n$. Write $n = 2^ei_1 \cdots p_k^e_k$. By problem 2(b), the number of solutions to $x^2 \equiv 1 \mod p_i^e_i$ is 2 for $1 \leq i \leq k$. By problem 6 there are 2 solutions to $x^2 \equiv 1 \mod p_i^e_i$, and by the previous lemma, there are 4 solutions to $x^2 \equiv 1 \mod 2^e$ for $e \geq 3$. Since $n \neq 2, 4, p^k, 2p^k$, we must have either $e \geq 3$ or at least two odd prime factors. In either case, the number of solutions to $x^2 \equiv 1 \mod n$ is divisible by 4, so there are an even number of pairs in $S_2$. Therefore, the product of all elements in $S_2$ is 1 mod $n$. We have $\prod_{(k,n) = 1}^n k \equiv \prod_{d|n} \prod_{a \in S_d} a \equiv 1 \mod n$ as desired.