GENERATORS MOD N

TIM SMITS

1. INTRODUCTION

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

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

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

Corollary 1.2. *$ord_n(a) \leq \varphi(n)$*

The question we will answer is the following: for which n is it true that equality is achievable? In otherwords, 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 $\{1, g, g^2, g^3, \ldots, g^{\varphi(n)-1}\}$ are $\varphi(n)$ distinct invertible elements mod n. We know that 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. *$a^k \equiv 1 \bmod n \iff ord_n(a) \mid k$*

Proof. Let $m = \text{ord}_n(a)$. By the division algorithm, write $n = mq + r$ with $0 \leq r < m$. We have $a^n = a^{mq+r} = (a^m)^q \cdot a^r \equiv a^r \equiv 1 \bmod n$. By definition of m, it's the smallest *positive* integer m with the property that $a^m \equiv 1 \bmod n$, 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 $a^k = (a^m)^q \equiv 1 \bmod n$ as desired. □

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

Proof. We have $(a^k)^{m/(m,k)} = (a^m)^{k/(m,k)} \equiv 1 \bmod n$, where this is justified because (m,k) divides both m and k. This says that $\mathrm{ord}_n(a^k) \mid \frac{m}{(m,k)}$ by the previous proposition. Now, set $t = \mathrm{ord}_n(a^k)$. Then $(a^k)^t = a^{kt} \equiv 1 \bmod n$, this means that $m \mid kt$, so $m\ell = kt$ for some $\ell \in \mathbb{Z}$. Dividing both sides by (m,k) we have $\frac{m}{(m,k)}\ell = \frac{k}{(m,k)}t$. Since $(\frac{m}{(m,k)}, \frac{k}{(m,k)}) = 1$, this means that $\frac{m}{(m,k)} \mid t$, so $\mathrm{ord}_n(a^k) = t = \frac{m}{(m,k)}$ as desired. □

Proposition 3. *Suppose that $ord_n(a) = m$ and $ord_n(b) = \ell$ and $(m,\ell) = 1$. Then $ord_n(ab) = m\ell$.*

Proof. Let $t = \mathrm{ord}_n(ab)$. We have $(ab)^{m\ell} = a^{m\ell}b^{m\ell} \equiv 1 \bmod n$, so $t \mid m\ell$. By definition of t, we have $(ab)^t = a^t b^t \equiv 1 \bmod n$. Raising both sides to the m power, $b^{tm} \equiv 1 \bmod n$ so $\ell \mid tm$. Similarly, raising both sides to the ℓ power we have $a^{t\ell} \equiv 1 \bmod n$, 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 $\mathrm{ord}_n(ab) = t = m\ell$ as desired. □

Proposition 4. *Let m, n be positive integers with $(m,n) = 1$. Then $ord_{mn}(a) = lcm(ord_m(a), ord_n(a))$.*

Proof. Let $t = \mathrm{ord}_{mn}(a)$ and $k = \mathrm{lcm}(\mathrm{ord}_m(a), \mathrm{ord}_n(a))$. Then $a^t \equiv 1 \bmod mn$, so $a^t \equiv 1 \bmod m$ and $a^t \equiv 1 \bmod n$. This says $\mathrm{ord}_m(a) \mid t$ and $\mathrm{ord}_n(a) \mid t$ so $k \mid t$. On the other hand, let $k = \mathrm{lcm}(\mathrm{ord}_m(a), \mathrm{ord}_n(a))$. Then $a^k \equiv 1 \bmod m$ and $a^k \equiv 1 \bmod n$ so by the Chinese remainder theorem, $a^k \equiv 1 \bmod mn$, 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 $ord_p(a) = d$. If $N_p(d) > 0$, then $N_p(d) = \varphi(d)$.*

Proof. Suppose that $\mathrm{ord}_p(a) = d$. Then $a^d \equiv 1 \bmod p$, so a is a root of the polynomial $T^d - 1 \bmod p$. Since this polyomial 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, $\mathrm{ord}_p(a^k) = d \iff (k,d) = 1$, 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 $a \bmod p$, we have $\mathrm{ord}_p(a) \mid p-1$. 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!)

so $p-1 \leq \sum_{d|p-1} N_p(d) \leq \sum_{d|p-1} \varphi(d) = p-1$ by lemma 3.2. This forces equality, so in particular, this must mean that $N_p(d) > 0$, otherwise the second inequality would be strict. By lemma 3.1 again, this means $N_p(p-1) = \varphi(p-1)$, 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 p^k

To show there is a generator mod p^k for $k \geq 2$ 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 p^k for all $k \geq 2$.

Lemma 4.1. *There is a generator mod p^2.*

Proof. Let g be a generator mod p, so that g is a root of the polynomial $f(T) = T^{p-1} - 1$ mod p. Since $f(T) = 0 \bmod p$ and $f'(T) = (p-1)g^{p-2} \not\equiv 0 \bmod p$, by Hensel's lemma, there is an integer c with $c \equiv g \bmod p$ such that $f(g+cp) = 0 \bmod p^2$, i.e. $(g+cp)^{p-1} \equiv 1 \bmod p^2$. By the binomial theorem, we have $(g+cp)^{p-1} = g^{p-1} + cp(p-1) + \cdots + (cp)^{p-1}$. Since p does not divide $c(p-1)$, working mod p^2, this says $1 \equiv (g+cp)^{p-1} \equiv g^{p-1} - cp \bmod p^2$, so $g^{p-1} \equiv 1 + cp \not\equiv 1 \bmod p^2$. Since $(g^{p-1})^p = g^{p(p-1)} \equiv 1 \bmod p^2$ by Euler's theorem, this means that $\mathrm{ord}_{p^2}(g^{p-1}) = p$. Now, set $t = \mathrm{ord}_{p^2}(g+cp)$. Since $(g+cp)^{p-1} \equiv 1 \bmod p^2$, this means that $t \mid p-1$. We have $1 \equiv (g+cp)^t \bmod p^2$, so $1 \equiv g^t \bmod p$. Since g is a generator mod p, this means that $p-1 \mid t$, so that $t = p-1$. By proposition 3, this means that $(g+cp)g^{p-1}$ has order $p(p-1) = \varphi(p^2)$ as desired. □

Theorem 4.2. *If g is a generator mod p^2, then g is a generator mod p^k for all $k \geq 2$. In particular, there is a generator mod p^k for $k \geq 2$.*

Proof. By the above lemma, there is a generator g mod p^2. We'll show that g is a generator mod p^k for all $k \geq 2$ by induction. The case $k = 2$ is true by assumption, so suppose we know that g is a generator mod p^k for some k, i.e. that $\mathrm{ord}_{p^k}(g) = p^{k-1}(p-1)$. Let $t = \mathrm{ord}_{p^{k+1}}(g)$. Since $g^{p^k(p-1)} \equiv 1 \bmod p^{k+1}$, this says $t \mid p^k(p-1)$, and since $g^t \equiv 1 \bmod p^k$, this says $p^{k-1}(p-1) \mid t$. Combining these two divisibilities, this says either $t = p^{k-1}(p-1)$ or $t = p^k(p-1)$. Therefore, it's sufficient to prove that $g^{p^{k-1}(p-1)} \not\equiv 1 \bmod p^{k+1}$. Since $g^{p-1} \equiv 1 \bmod p$, we can write $g^{p-1} = 1 + p\ell$ for some ℓ, and since g is a generator mod p^2, we know that $\ell \not\equiv 0 \bmod p$. We compute $g^{p(p-1)} = (1+p\ell)^p = 1 + p^2\ell + \cdots + (p\ell)^p \equiv 1 + p^2\ell \bmod p^3$. Now, we have $(g^{p-1})^{p^2} \equiv (1+p^2\ell)^p \equiv 1 + \ell p^3 \bmod p^4$. Repeating this procedure, we find that $(g^{p-1})^{p^{k-1}} \equiv 1 + \ell p^k \bmod p^{k+1}$. This proves that $t = p^k(p-1)$, 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 p^k for $k \geq 2$.

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 $(g+cp)g^{p-1}$, where c comes from the proof of Hensel's lemma. Explicitly going through the proof, set $f(T) = T^{p-1} - 1$. We have $f(g+cp) \equiv f(g) + f'(g)cp \bmod p^2$. Since $f(g) \equiv 0 \bmod p$, we choose c so that $p(\frac{f(g)}{p} +$

$f'(g)c) \equiv 0 \bmod p^2$, i.e. $\frac{f(g)}{p} + f'(g)c \equiv 0 \bmod p$. Solving for c says $c \equiv -\frac{f(g)}{p}[f'(g)]^{-1} \bmod p$. Since $f'(g) \equiv (p-1)g^{p-2} \bmod p$, we see that $[f'(g)]^{-1} \equiv -g \bmod p$, so $c \equiv \frac{f(g)}{p} g \bmod p$. Therefore, our generator is given by $(g + (\frac{f(g)}{p} g)p)g^{p-1} = (1 + f(g))g^p = g^{p-1}g^p = \boxed{g^{2p-1}}$.

As an explict example, we mentioned earlier that 3 is a generator mod 7, so $3^{13} \equiv 10 \bmod 49$ 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 $(g^{p-1})^{p^k} \equiv 1 + p^{k+1}\ell \bmod p^{k+2} \implies (g^{p-1})^{p^{k+1}} \equiv 1 + p^{k+2}\ell \bmod p^{k+3}$. What goes wrong? When $p = 2$, if $g^{2^k} \equiv 1 + 2^{k+1}\ell \bmod 2^{k+2}$, then $g^{2^{k+1}} \equiv 1 + 2^{k+2}\ell + 2^{2k+2}\ell^2 \bmod 2^{k+3}$, 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 $g^{2^{k-1}} \equiv 1 \bmod 2^k$. 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 $g^\ell = -1 \bmod 2^k$ for some ℓ. Squaring says $g^{2\ell} = 1 \bmod 2^k$, so $2^{k-1} \mid 2\ell$ says $2^{k-2} \mid \ell$, i.e. $2^{k-2} = \ell$. On the other hand, we have $g^2 \equiv 1 \bmod 8$ since *every* unit squares to 1 mod 8. This says $g^2 = 1 + 8\ell$ for some ℓ, so that $g^4 \equiv (1 + 8\ell)^2 \equiv 1 \bmod 16$. Inductively repeating this, we find that $g^{2^{k-2}} \equiv 1 \bmod 2^k$, which says $1 \equiv -1 \bmod 2^k$, a contradiction. Therefore, there is no generator mod 2^k for $k \geq 3$. □

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 $\mathrm{ord}_{p^k}(g + p^{k-1}) = \mathrm{ord}_{p^k}(g)$, so $g + p^{k-1}$ is a generator mod $2p^k$. Conversely, write $n = 2^e p_1^{e_1} \cdots p_k^{e_k}$. We have $\mathrm{ord}_n(a) = \mathrm{lcm}(\mathrm{ord}_{2^e}(a), \mathrm{ord}_{p_1^{e_1}}(a), \ldots, \mathrm{ord}_{p_k^{e_k}}(a))$. For each i, we have $\mathrm{ord}_{p_i^{e_i}}(a) \leq \varphi(p_i^{e_i})$. If $e \geq 3$, the proof of 5.1 says $\mathrm{ord}_{2^e}(a) \leq 2^{e-2}$, so $\mathrm{ord}_n(a) < 2^{e-2}\varphi(p_1^{e_i} \cdots p_k^{e_k}) < \varphi(n)$. 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, so $\mathrm{lcm}(\mathrm{ord}_{p_2^{e_2}}(a), \mathrm{ord}_{p_1^{e_1}}(a)) < \varphi(p_1^{e_1} p_2^{e_2})$ so that $\mathrm{ord}_n(a) < \varphi(n)$. This leaves the only possible cases of $n = 2^e p^k$ where $e = 0, 1$ and $k \geq 0$, which leaves the 4 possible cases above. □

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, $(p-1)! \equiv -1 \bmod p$.*

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

$$\prod_{\substack{i=1 \\ (k,n)=1}}^{n} k \equiv \begin{cases} -1 \bmod n & n = 2, 4, p^k, 2p^k \\ 1 \bmod n & \textit{otherwise} \end{cases}$$

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

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

Proof. Note that $\pm 1, \pm 1 + 2^{e-1} \bmod 2^e$ are four solutions to $x^2 \equiv 1 \bmod 2^e$. 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 $a^2 \equiv 1 \bmod 2^{e+1}$, then $a^2 \equiv 1 \bmod 2^e$, 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 $a^2 = 1 + 2^{2e-2}k^2 + 4^e \ell^2 \pm 2^e k \pm 2^{e+1}\ell + 4^e k\ell$. Since $2e - 2 \geq e + 1$, reducing mod 2^{e+1} says $a^2 \equiv 1 + 2^e k \bmod 2^{e+1}$. By assumption, this forces $k = 0$, i.e. $a \equiv \pm 1 \bmod 2^e$. Thus, $a = \pm 1 + 2^e \ell$. If ℓ is even, then $a \equiv \pm 1 \bmod 2^{e+1}$, and if ℓ is odd, then $a \equiv \pm 1 + 2^e \bmod 2^{e+1}$, 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 $g \bmod n$. The invertible elements mod n are given by $1, g, g^2, \ldots, g^{\varphi(n)-1}$. Therefore, $\displaystyle\prod_{\substack{i=1 \\ (k,n)=1}}^{n} k \equiv \prod_{i=0}^{\varphi(n)-1} g^i \equiv g^{\sum_{i=0}^{\varphi(n)-1} i} \bmod n$. We have $\sum_{i=0}^{\varphi(n)-1} i = \frac{\varphi(n)(\varphi(n)-1)}{2}$. Since g is a generator mod n, $g^{\varphi(n)/2} \equiv -1 \bmod n$, and since $n > 2$ we have $\varphi(n)$ is even, so $\varphi(n) - 1$ is odd. Therefore, $g^{\varphi(n)(\varphi(n)-1)/2} \equiv (g^{\varphi(n)/2})^{\varphi(n)-1} \equiv -1 \bmod n$. Let $S_d = \{1 \leq a \leq n : \operatorname{ord}_n(a) = d\}$, 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 $a^2 \equiv 1 \bmod n$, 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 $x^2 \equiv 1 \bmod n$. Write $n = 2^e p_1^{e_1} \ldots p_k^{e_k}$. By problem 2(b), the number of solutions to $x^2 \equiv 1 \bmod n$ is the product of the number of solutions of $x^2 \equiv 1 \bmod 2^e$ and $x^2 \equiv 1 \bmod p_i^{e_i}$ for $1 \leq i \leq k$. By problem 6 there are 2 solutions to $x^2 \equiv 1 \bmod p_i^{e_i}$, and by the previous lemma, there are 4 solutions to $x^2 \equiv 1 \bmod 2^e$ 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 $x^2 \equiv 1 \bmod n$ 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 $\displaystyle\prod_{\substack{i=1 \\ (k,n)=1}}^{n} k \equiv \prod_{d|n} \prod_{a \in S_d} a \equiv 1 \bmod n$ as desired.

□