When Is the Multiplicative Group Modulo n Cyclic?

Aryeh Zax

November 30, 2015

1 Background

For the sake of completeness, we include a brief background in modern algebra. Anyone comfortable with groups, rings, and fields can safely skip all of this: there are some interesting number-theoretic trivia thrown in, but nothing that would be missed.

A *group* is a 2-tuple $(G, \cdot)$, where G is a set, $\cdot$ is a binary operation, and they satisfy the following four properties:

- For all $x, y \in G$, $x \cdot y \in G$ (*closure*);
- There exists an element in G, often denoted by 1 (or e), such that for all $x \in G$,

  $$1 \cdot x = x \cdot 1 = x$$

  (identity);
- For all $x \in G$, there exists $y \in G$ with

  $$x \cdot y = y \cdot x = 1$$

  (inverses);
- For all $x, y, z \in G$,

  $$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

  (associativity).

One property we have omitted in the list of four above is *commutativity*; for all $x, y \in G$, $x \cdot y = y \cdot x$. There are many interesting examples of noncommutative groups (matrices with multiplication, most prominently), so a group need not be commutative unless otherwise specified. For our purposes, though, groups will always be commutative, since our groups will all arise from working with $\mathbb{Z}$, where addition and multiplication are both commutative. A commutative group is called *abelian* (for Niels Henrik Abel, the founder of group theory).

It is easy to show that $1 \in G$ is unique, and for any $x \in G$, the y such that $x \cdot y = y \cdot x = 1$ is unique as well. Usually the operation in a group is most easily thought of as multiplication; occasionally it is useful to think of it as addition, and we write 0 instead of 1 for the identity and $+$ instead of $\cdot$ for the operation. When the group is multiplicative, we generally write xy in place of $x \cdot y$ to save space. When the operation is understood, it is often said that G itself is a group, although this is not strictly correct.

If G is finite, we can speak of the *order* of an element g; this is the smallest exponent $d > 0$ such that $g^d = 1$. Note that such a d necessarily exists; write out $g^0, g^1, g^2, \cdots, g^{|G|}$. There is one more element here than there is elements in the group, so by the pigeonhole principle two of them must be the same: $g^a = g^b$. Now $g^{|a-b|} = 1$. Actually, it is a theorem of Lagrange that the order of an element is always a divisor of $|G|$; in particular, $g^{|G|} = 1$ always.

A *ring* is a 3-tuple $(R, +, \cdot)$ where R is a set and $+, \cdot$ are binary operations satisfying the following properties:

- $(R, +)$ is an abelian group with identity 0;
- For all $a, b, c \in R$,
$$(ab)c = a(bc)$$
(associativity);
- For all $a, b, c \in R$,
$$a(b + c) = ab + ac$$
$$(b + c)a = ba + ca$$
(distributivity).

Note again that we do not ask for the multiplication to be commutative (at least, not in the definition); but for our purposes it will be. Such a ring is called, to no one's surprise, *commutative*.

A *field* is a ring such that $(R \setminus \{0\}, \cdot)$ is an abelian group with identity 1, and $1 \neq 0$. (This just rules out the "field" of size 1, which tends to behave poorly.)

The *multiplicative group* or *group of units* of a ring R, denoted by R^*, is the set of elements of R with multiplicative inverses, together with multiplication. A field is therefore a ring for which the multiplicative group is as large as possible. The focus of our concern here is the multiplicative group of the ring $\mathbb{Z}/n\mathbb{Z}$, often written succinctly as $(\mathbb{Z}/n\mathbb{Z})^*$.

Theorem 1.0.1. $(\mathbb{Z}/n\mathbb{Z})^*$ *contains precisely the numbers between* 1 *and* n *that are coprime to* n.

Lemma 1 (Bézout)**.** *Let* $a, b, c \in \mathbb{Z}$. *Then the equation*

$$ax + by = c$$

has a solution $(x, y) \in \mathbb{Z}^2$ *iff* $(a, b) \mid c$. *(Here* $(\cdot, \cdot)$ *denote the greatest common divisor function, and* $\mid$ *is read as "divides").*

Proof. The only if direction is clear; (a, b) divides the LHS, so it must divide the RHS. For the if direction, it's sufficient to find a solution for $c = (a, b)$, since then we can just scale that solution up by any desired factor to get the rest of them. The extended euclidean algorithm provides a method for determining x and y in this case, so we're done. □

Proof of Theorem. Clearly this set of numbers is closed under multiplication, has associative multiplication, and contains 1, so it remains to show that these are precisely the invertible elements. Suppose we want to solve $ax \equiv 1 \pmod{n}$ (to invert a); this is equivalent to solving

$$ax + ny = 1$$

in integers. By Lemma 1, we can do this iff a and n are coprime.

□

Remark. The *Euler totient function* is defined as $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|$. It satisfies

$$\varphi(p^m) = p^{m-1}(p - 1)$$

which follows from Theorem 1.0.1. It is also what's known as *multiplicative*:

$$\varphi(ab) = \varphi(a)\varphi(b)$$

whenever $(a, b) = 1$.[1] This can be shown as a consequence of the Chinese remainder theorem, which we will meet soon.

A group G is called *cyclic* if there exists an element $g \in G$ where, for all $x \in G$, $x = g^n$ for some $n \in \mathbb{Z}$. Equivalently, there is an element of order $|G|$. Such an element is called a *generator*. (In the number theoretic special case we're dealing with it is also known as a *primitive root*, but we won't use that language.) Cyclic groups are the easiest groups to understand; all finite groups can be described by giving a small generating set, the orders of the elements in that set, and the relations between the elements in that set (how they multiply together). A cyclic group has a generating set of size only 1, so there are no tricky relations to worry about.

The cyclic groups one thinks about most often are $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ (both with addition); 1 serves as a generator in either case, though there may be others. All cyclic groups are isomorphic to one of these groups. (One simply maps the generator of the group onto 1.) We concern ourselves with when $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic because it allows us to turn multiplication, which is complicated, into addition (of exponents), which is easy.

[1] This sounds stupid: clearly we should call a function f multiplicative if $f(ab) = f(a)f(b)$ *always*, none of this coprime stuff. Functions like that are called *totally multiplicative*; they turn out to be a lot less interesting than multiplicative functions, which is why they get the longer name. φ is one of many interesting number-theoretic functions that is multiplicative, but not totally multiplicative.

2 The Chinese Remainder Theorem

This is a powerful theorem for breaking up arbitrary commutative rings into smaller rings; here we present it in just enough generality to serve our purposes.

Theorem 2.0.1. *Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be a prime factorization. Then*

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$$

as rings.

Remark. The $\times$ just means you do computations in the rings on the RHS one coordinate at a time.

Proof. The map (from left to right) is given by applying the appropriate modulus to each coordinate: if we start with a on the left, the first coordinate is a modulo $p_1^{e_1}$, the second is a modulo $p_2^{e_2}$, and so on. It should be clear that this map respects the operations; it remains to show that it is bijective. There are n elements on the left and $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = n$ elements on the right, so it's enough to show the map is injective.

Take a, b in $\mathbb{Z}/n\mathbb{Z}$ that are mapped to the same k-tuple on the right; then $a - b \equiv 0 \pmod{p_i^{e_i}}$ for all i. Since the $p_i^{e_i}$ are coprime, this means that $a - b \equiv 0 \pmod{\operatorname{lcm}\{p_i^{e_i}\}}$, i.e. $a - b \equiv 0 \pmod{n}$, i.e. $a = b$. This completes the proof. □

Corollary 2.0.2. *Since the above rings are isomorphic, so are their multiplicative groups. Observe that the multiplicative group of a direct product is the direct product of the multiplicative groups.*

3 The Proof

3.1 Ruling Out Most Cases; Problems for $p = 2$

It turns out that for most possible prime factorizations of n we can immediately rule out that $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic. This is by way of a helpful lemma.

Definition 3.1.1. The *exponent* of a group G is the smallest f such that $g^f \equiv 1$ for all $g \in G$.

Remark. If G is cyclic, its exponent is $|G|$ (of course). The converse is not true, though; S_3 has exponent $|S_3| = 6$ but is not cyclic (or even abelian). The contrapositive, though, is quite helpful: if the exponent of G is less than $|G|$, then G is not cyclic.

Lemma 2. *Let C_n denote the cyclic group on n elements (another name for $(\mathbb{Z}/n\mathbb{Z}, +)$). Let*

$$C := C_{i_1} \times C_{i_2} \times \cdots \times C_{i_k}$$

Then C is cyclic if and only if the i_j are pairwise coprime; in particular, the exponent of C is $\operatorname{lcm}(i_1, i_2, \cdots, i_k)$.

Proof. Suppose the i_j are not pairwise coprime, so that $\ell := \operatorname{lcm}(i_1, i_2, \cdots, i_k) < |C|$. The exponent of C certainly divides ℓ, so C can have no element of order $|C|$. In the reverse direction, if the i_j are pairwise coprime, then $\ell = |C|$ and the element $(1, 1, \cdots, 1)$ has order ℓ, so C is cyclic. □

Claim. Suppose p, q are distinct odd primes dividing n. Then $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic.

Proof. The Chinese remainder theorem gives us that $(\mathbb{Z}/n\mathbb{Z})^*$ is isomorphic to a direct product of groups, one of which is $(\mathbb{Z}/p^{e_p}\mathbb{Z})^*$ and another of which is $(\mathbb{Z}/q^{e_q}\mathbb{Z})^*$ for appropriate values of e_p and e_q. But these multiplicative groups have orders $\varphi(p^{e_p})$ and $\varphi(q^{e_q})$ (respectively), which are multiples of $p-1$ and $q-1$ (respectively), and therefore even. Now we're done by Lemma 2. □

Claim. Suppose p is an odd prime dividing n and $4 \mid n$. Then $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic.

Proof. The proof is the same as for the last claim; now $(\mathbb{Z}/n\mathbb{Z})^*$ is isomorphic to a direct product of groups including $(\mathbb{Z}/p^{e_p}\mathbb{Z})^*$ and $(\mathbb{Z}/2^{e_2}\mathbb{Z})^*$, with $e_2 \geq 2$. Again, both groups have even order, and so the direct product can't be cyclic. □

This already rules out all cases except numbers of the form $2^m, p^m$, or $2p^m$ for p an odd prime and $k \geq 0$. Note that, most unfortunately,

$$1 \equiv 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod 8$$

So $(\mathbb{Z}/8\mathbb{Z})^*$ isn't cyclic; it's the darn Klein 4-group instead. Now $(\mathbb{Z}/2^m\mathbb{Z})^*$ can't be cyclic for any $m \geq 3$; after all, if all of the possible remainders modulo, say, 16 appeared as powers of some number k, then all of the possible remainders modulo 8 would as well. We're now left with only the following possible values of n:

$$n \in \{1, 2, 4, p^m, 2p^m\}$$

These actually all work. (1, 2, and 4 are easy to check, of course.)

It is not unusual for a theorem to begin "let p be an odd prime:" 2 is often left out of clubs that all the other primes get to join. There are a number of deep reasons "why" there are no generators modulo 8; at any rate, they're deeper than "I just checked, see? All the elements had order 2." An equine reason is explored later; I may explore more reasons in a future talk.

3.2 A Taste of What's to Come

The proof that $(\mathbb{Z}/p^m\mathbb{Z})^*$ is cyclic proceeds in three parts: first the case $m = 1$, then $m = 2$, and then all $m > 2$. Suppose we had done extensive numerical analysis on such multiplicative groups and found they always seemed to be cyclic; why might we look for a proof that broke into these three stages? The answer is actually quite natural.

The proof is by its nature inductive, so having a base case $m = 1$ is only fair. It is easiest to tackle first for a number of reasons: $\mathbb{Z}/p\mathbb{Z}$ is actually a field, unlike when $m > 1$, which gives us some nice additional structure to work with. Indeed, both proofs we give for $m = 1$ rely on this fact. This is also the simplest case, since we have the fewest elements to deal with, and often a good way to get a handle on a new problem is to prove it for the simplest cases first.

But why the weird stumble at $m = 2$—can't a regular inductive proof work? The reasons for the other joints in how the proof is put together are a little more subtle. Suppose for a moment that $\mathbb{Z}/p^m\mathbb{Z}$ is always cyclic. Note that generators modulo p^m necessarily generate modulo p^{m-1}; if the powers of g give all possible remainders modulo p^m, they'd better also do so modulo p^{m-1}. The question is really whether a generator g modulo p^{m-1} *lifts* to generators modulo p^m. That is, how many of the p different numbers modulo p^m that are congruent to g modulo p^{m-1}, are themselves generators modulo p^m?

The group $\mathbb{Z}/p^m\mathbb{Z}$ has order $\varphi(p^m) = p^{m-1}(p-1)$. As we'll see later, a cyclic group of order n has $\varphi(n)$ generators: if g is one generator, all of the powers of g with exponent coprime to n are as well. Therefore there are

$$\varphi(\varphi(p^m)) = \varphi(p^{m-1}(p-1)) = \varphi(p^{m-1})\varphi(p-1) = p^{m-2}(p-1)\varphi(p-1)$$

many generators modulo p^m for $m \geq 2$. What this means is that the number of generators *usually* increases by a factor of p when we change m to $m+1$, so it must be that all of the different lifts of generators modulo p^m also generate modulo p^{m+1}, and the proof merely consists of showing that fact. However, for $m = 1$,

$$\varphi(\varphi(p)) = \varphi(p-1)$$

and for $m = 2$,

$$\varphi(\varphi(p^2)) = \varphi(p(p-1)) = (p-1)\varphi(p-1)$$

Here, even though the group is p times as large, it has only $p-1$ times as many generators, so occasionally lifting a generator will fail to yield a generator of the bigger group. (As we'll see, there is precisely one "bad" lift per generator; there aren't any generators whose lifts are all good, which then get cancelled out by having some generators with multiple bad lifts.) In other words, once we've found a generator modulo p we'll have to be careful about how we lift it to modulo p^2. This is what causes the kink in the proof.

3.3 The case $m = 1$

Theorem 3.3.1 (Gauss)**.** *The group $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.*

Proof 1. We prove a superficially stronger claim. Let S_d denote the number of elements of G with order d. Then we claim that $|S_d| = \varphi(d)$; in particular, there are $\varphi(p-1)$ generators.

This proof is entirely elementary, and proceeds in two parts. First, we show that $|S_d| \in \{0, \varphi(d)\}$; second, we show that the 0 case can't happen. We'll need two lemmas.

Lemma 3. *Let G be a group and let $a \in G$ have order d. Then a^k has order $\frac{d}{(d,k)}$.*

Proof. Suppose $\left(a^k\right)^\ell = a^{k\ell} = 1$; then $d \mid k\ell$, so the minimal ℓ that works is $\frac{d}{(d,k)}$. □

Corollary 3.3.2. *A cyclic group on n elements has $\varphi(n)$ generators. (This was promised in Section 3.2.)*

Lemma 4.

$$\sum_{d|n} \varphi(d) = n$$

Proof. We use a double-counting argument; specifically, both sides count the number of fractions in the list $\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n}$. The LHS does so by putting each fraction in simplest form and counting the number of times each denominator appears; how the RHS does so is obvious. □

Suppose $|S_d| = 0$; then we're done. Otherwise, take $a \in S_d$, and consider the polynomial equation $x^d - 1 = 0$ in G (viewed as a field). This has at most d roots[2]; but aha! $1, a, a^2, \cdots, a^{d-1}$ are all roots of this polynomial, and distinct, so this must be all of them. We just have to examine which of them genuinely have order d (as opposed to a divisor thereof). By Lemma 3, this is true precisely for the $\varphi(d)$ powers of a with exponent coprime to d.

Since the S_d partition G, we now have

$$\sum_{d|p-1} \varphi(d) = p - 1 = \sum_{d|p-1} |S_d|$$

But each term in the RHS sum is $\leq$ to the corresponding term in the LHS sum, so it must be that we have equality, and the proof is complete. □

[2]But that's the fundamental theorem of algebra—we haven't proven that for arbitrary fields! Yes, you're right. But in a field we can use the polynomial long division algorithm, just like with $\mathbb{R}$, to "pull out" roots one at a time and decrease the degree by 1. Since a linear equation has only one root, induction shows that my claim is true.

Proof 2. We actually prove the stronger statement that the multiplicative group of *any* field is cyclic.[3]

Lemma 5. *Let G be a finite abelian group, and let the exponent of G be the smallest number f such that $a^f = 1$ for all $a \in G$. Then there exists $g \in G$ such that the order of g is f.*

Proof. We appeal to the structure theorem for finite abelian groups. Write

$$G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_k}$$

For the q_i prime powers. (The groups on the right are viewed additively, and generated by 1.) Clearly G has exponent dividing $\operatorname{lcm}(q_1, q_2, \cdots, q_k)$. Also, the element $(1, 1, \cdots, 1)$ on the right has order $\operatorname{lcm}(q_1, q_2, \cdots, q_k)$. The result is now shown. □

Now to prove the theorem it's enough to show that G has exponent $p-1$. By Lagrange, $x^{p-1} - 1 = 0$ is satisfied by all elements $x \in G$. Any lower-degree polynomial, however, can't have $p-1$ distinct nonzero roots in the field $\mathbb{Z}/p\mathbb{Z}$, so $p-1$ is indeed the exponent of G. Now Lemma 5 gives us an element of order $p-1$, and we're done. □

3.4 The case $m = 2$

As discussed above, we have reason to believe that most ways of lifting generators modulo p are good, but some are bad. It's not too difficult to make this notion rigorous.

Theorem 3.4.1. *Let r be a generator modulo p, and let k be such that $p \nmid k$. Then either r or $r + kp$ generates modulo p^2.*

Proof. The order of $\mathbb{Z}/p^2\mathbb{Z}$ is $\varphi(p^2) = p(p-1)$, so $r, r+kp$ must have orders dividing this. But their orders must *also* be multiples of $p-1$; otherwise, they wouldn't generate modulo p. (Note that $r + kp$ is just r when taken modulo p.) This leaves only $p-1$ and $p(p-1)$ for possible orders. If either one has order $p(p-1)$ then we're done, so suppose both have order $p-1$. But then

$$1 \equiv (r+kp)^{p-1} \equiv r^{p-1} + \binom{p-1}{1} r^{p-2} kp + \binom{p-1}{2} r^{p-3} k^2 p^2 + \cdots \pmod{p^2}$$

On the RHS, the zeroth and first terms are fine, but all subsequent terms have a factor of p^2 and can therefore be discarded. This leaves us with

$$1 \equiv 1 + kp(p-1)r^{p-2} \pmod{p^2}$$

$$0 \equiv kp(p-1)r^{p-2} \pmod{p^2}$$

[3]One can be even more zealous: any finite subgroup of the multiplicative group of a field is cyclic. The proof given here generalizes easily enough.

$$p^2 \mid kp(p-1)r^{p-2} \pmod{p^2}$$

But try as we might, there is only one factor of p to be found in $kp(p-1)r^{p-2}$, so this is a contradiction. □

Corollary 3.4.1. *Each generator modulo p has exactly one failed lift modulo p^2.*

Proof. Since all the lifts of a given number differ from each other by a multiple of p, Theorem 3.4.1 gives us that at most one lift of each generator mod p can fail to generate modulo p^2. Since we need an average of one failed lift per generator, this proves the corollary. □

For those interested only in proving the existence of primitive roots modulo p^2, the theorem can be stated more compactly:

Theorem 3.4.1. *Let r generate modulo p. Then either r or $r+p$ generates modulo p^2.*

Note that this is a little weaker than the statement we gave. It does not immediately imply that each generator modulo p has only one bad lift, but does provide a simpler set of instructions for finding a generator modulo p^2 once you have one modulo p: try it mod p^2, and if that fails, just add p to it.

3.5 A Brief Interlude for Horseplay

Theorem 3.5.1. *All horses are the same color.*

Proof. We proceed by induction. The base case, a set of $n = 1$ horses, is trivial. For the inductive step, suppose we know that all sets of n horses are the same color, and consider a set of $n+1$ horses. The first n horses are the same color, as are the last n; since the first horse is the same color as the middle horses, which are the same color as the last horse, we conclude that the first and last horse are also the same color, and hence all $n+1$ horses are the same color. The set of horses was arbitrary, so the inductive step is shown, and the conclusion follows. □

What's going on? The problem is in jumping from $n = 1$ to $n = 2$; at this stage, "the initial one horse" and "the final one horse" are two sets without overlap, and the inductive step falls apart. The base case $n = 1$ is true, and if the statement holds for $n = 2$, it holds for $n = 3$, which then means it holds for $n = 4$, and so on. We're so close to a real inductive proof! But mathematical truth doesn't give partial credit. The proof is garbage.

(Don't worry about me; I haven't gone insane yet. To mix metaphors a bit, our horses will soon come to roost.)

3.6 Lifting the Generators Modulo p^2

The theorem statement is as we know it must be:

Theorem 3.6.1. *Let p be an odd prime and r be a generator modulo p^2. Then r is a generator modulo p^m for all $m > 2$.*

Lemma 6. *Let p be an odd prime and $a \geq 1$. Then*

$$(1 + kp)^{p^a} \equiv 1 + kp^{a+1} \pmod{p^{a+2}}$$

Proof. We proceed by induction on a. For the base case $a = 1$, Observe that

$$(1 + kp)^p = 1 + \binom{p}{1} kp + \cdots$$

where the omitted terms are all divisible by p^3 or better (once from the binomial coefficient, and twice or more from the power of kp).[4] This gives

$$(1 + kp)^p = 1 + kp^2 + n_1 p^3$$

for some n_1, and the base case is shown.

Suppose the statement holds for some $a \geq 1$, so

$$(1 + kp)^{p^{a+1}} = \left((1 + kp)^{p^a}\right)^p = \left(1 + kp^{a+1} + np^{a+2}\right)^p$$

for some n. In a trinomial expansion of the RHS, p^{a+3} divides most terms, since we get:

- Three "pure" terms, 1^p, $(kp^{a+1})^p$, and $(np^{a+2})^p$; of these, only 1^p is not divisible by p^{a+3}.
- Cross terms involving at least one factor of np^{a+2}; we only need one more factor of p. We'll certainly find it if we use another factor of np^{a+2}; otherwise, we're using at least two distinct factors, which implies that p divides the associated trinomial coefficient.
- Cross terms involving no factors of np^{a+2}, but at least two factors of kp^{a+1}; these are also divisible by p^{a+3}.
- One cross term involving no factors of np^{a+2} and only one factor of kp^{a+1}, i.e.

$$\binom{p}{p-1, 1, 0} 1^{p-1} \left(kp^{a+1}\right)^1 \left(np^{a+2}\right)^0 = kp^{a+2}$$

And therefore

$$(1 + kp)^{p^{a+1}} = \left((1 + kp)^{p^a}\right)^p = \left(1 + kp^{a+1} + np^{a+2}\right)^p = 1 + kp^{a+2} + n'p^{a+2}$$

for some n', completing the inductive step, and therefore the proof. □

[4] The explanation here is a little sloppy. Can you see why it fails if, and only if, $p = 2$?

Proof of Theorem. Note that r has order $p-1$ modulo p, so the order of r modulo p^m is a multiple of $p-1$ dividing $p^{m-1}(p-1)$; i.e. it is of the form $p^a(p-1)$ for some $0 \leq a < m$. All of these possibilities divide $p^{m-2}(p-1)$ except for $p^{m-1}(p-1)$ (the order we want), so to show that the order is the latter, it's enough to show that it does not divide the former, i.e. that $r^{p^{m-2}(p-1)} \not\equiv 1 \pmod{p^m}$.

Since r generates modulo p^2, we have that $r^{p-1} = 1 + kp$ for $p \nmid k$. Now by Lemma 6,

$$r^{p^{m-2}(p-1)} = (r^{p-1})^{p^{m-2}} = (1+kp)^{p^{m-2}} = 1 + kp^{m-1} + np^m$$

for some n. Since $p \nmid k$, this is notably not congruent to 1 modulo p^m, from which the result follows. □

Remark. Note that the inductive step of Lemma 6 didn't depend on p being odd; only the base case did. Proving that the lemma holds in the base case (with p in the exponent) is used in the theorem to show that there is a primitive root when $m = 3$. There are generators modulo 4, and if there were generators modulo 8, they would generate modulo 16, modulo 32, and so on. Unfortunately, our generators fail to make the hop over from $m = 2$ to $m = 3$, and the whole edifice crashes.

In some sense, then, $(\mathbb{Z}/2^m\mathbb{Z})^*$ is not cyclic ($m \geq 3$) for the same reason that not all horses are the same color ($n \geq 2$).

3.7 The $2p^m$ Afterthought

Theorem 3.7.1. *Let p be an odd prime and $m > 1$. Then $(\mathbb{Z}/(2p^m)\mathbb{Z})^*$ is cyclic.*

Proof. By the Chinese remainder theorem,

$$(\mathbb{Z}/(2p^m)\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^m\mathbb{Z})^*$$

and the first group on the RHS is the trivial group, so

$$(\mathbb{Z}/(2p^m)\mathbb{Z})^* \cong (\mathbb{Z}/p^m\mathbb{Z})^*$$

The group on the right is cyclic, so the one on the left must also be. If r is a generator on the right, then either r or $r + p^m$ (whichever one is odd) generates on the left. □