ORDERS IN MODULAR ARITHMETIC

KEITH CONRAD

1. Introduction

Fermat's little theorem tells us that $a^{p-1} \equiv 1 \bmod p$ for all primes p and integers $a \not\equiv 0 \bmod p$. More generally, Euler's theorem tell us that $a^{\varphi(m)} \equiv 1 \bmod m$ for all $m \geq 2$ and integers a that are relatively prime to m. Depending on the value of a, it's possible for a smaller power than the $\varphi(m)$-th power to be congruent to 1 mod m.

Example 1.1. Let $m = 7$. The following table shows that the first time a nonzero number mod 7 has a power congruent to 1 varies. While Fermat's little theorem tells us that $a^6 \equiv 1 \bmod 7$ for $a \not\equiv 0 \bmod 7$, we see in the table that the exponent 6 can be replaced by a smaller positive exponent for 1, 2, 4, and 6.

k	1	2	3	4	5	6
$1^k \bmod 7$	1					
$2^k \bmod 7$	2	4	1			
$3^k \bmod 7$	3	2	6	4	5	1
$4^k \bmod 7$	4	2	1			
$5^k \bmod 7$	5	4	6	2	3	1
$6^k \bmod 7$	6	1				

Example 1.2. Since $\varphi(15) = 8$, if $(a, 15) = 1$ then $a^8 \equiv 1 \bmod 15$. But in fact, as the table below shows, the 8th power is always higher than necessary: the first, second, or fourth power of each number relatively prime to 15 is congruent to 1 mod 15.

k	1	2	3	4
$1^k \bmod 15$	1			
$2^k \bmod 15$	2	4	8	1
$4^k \bmod 15$	4	1		
$7^k \bmod 15$	7	4	13	1
$8^k \bmod 15$	8	4	2	1
$11^k \bmod 15$	11	1		
$13^k \bmod 15$	13	4	7	1
$14^k \bmod 15$	14	1		

Definition 1.3. If $(a, m) = 1$ then the *order* of $a \bmod m$ is the least $n \geq 1$ such that $a^n \equiv 1 \bmod m$.

Example 1.4. By the table in Example 1.1, 2 mod 7 has order 3, 3 mod 7 has order 6, and 4 mod 7 has order 3.

Example 1.5. By Example 1.2, 2 mod 15 has order 4 and 11 mod 15 has order 2.

Example 1.6. Always 1 mod m has order 1. If $(a, m) = 1$ and $a \not\equiv 1 \bmod m$ then $a \bmod m$ has order greater than 1.

We do not define the order of a mod m when $(a, m) > 1$. Why? Because in order for the condition $a^n \equiv 1 \bmod m$ to hold for some $n \geq 1$ the number a must be relatively prime to m: if $a^n \equiv 1 \bmod m$ then $a^n = 1 + md$ for some integer d, so any common factor or a and m is a factor of 1 and thus is ± 1.

To emphasize that the order of a mod m is the *least* $n \geq 1$ making $a^n \equiv 1 \bmod m$, we can express the definition of a mod m having order n like this:

$$a^n \equiv 1 \bmod m, \quad a^j \not\equiv 1 \bmod m \text{ for } 1 \leq j < n.$$

Example 1.7. If $m > 2$ then -1 mod m has order 2 since $(-1)^2 \equiv 1 \bmod m$ and $(-1)^1 = -1 \not\equiv 1 \bmod m$. When $m = 2$, $-1 \equiv 1 \bmod 2$, so -1 mod 2 has order 1.

When p is prime the order of a nonzero number mod p is certainly at most $p-1$, and more generally if $(a, m) = 1$ then the order of a mod m is at most $\varphi(m)$, but something stronger happens that was illustrated in the tables in Examples 1.1 and 1.2: the order *divides* $\varphi(m)$.

Warning. If $a^4 \equiv 1 \bmod m$, this *does not* mean a mod m has order 4, since that exponent might not be as small as possible. More generally, from $a^n \equiv 1 \bmod m$ it *does not* follow that a mod m has order n. For example, $(-1)^4 \equiv 1 \bmod m$, but this doesn't mean -1 mod m has order 4, and in fact the order is not 4 since $(-1)^2 \equiv 1 \bmod m$.

In Section 2 we will relate the order of a mod m to periodicity properties of the sequence of powers $1, a, a^2, a^3, \ldots \bmod m$. In Section 3 we will see how the order of a mod m tells us the order of any power a^k mod m.

2. Orders, Divisibility, and Periodicity

To see how closely the order of a mod m is tied up with the whole sequence of powers $a, a^2, a^3, \ldots \bmod m$, let's look at the first 20 powers of each nonzero number mod 7:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$1^k \bmod 7$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$2^k \bmod 7$	2	4	1	2	4	1	2	4	1	2	4	1	2	4	1	2	4	1	2	4
$3^k \bmod 7$	3	2	6	4	5	1	3	2	6	4	5	1	3	2	6	4	5	1	4	5
$4^k \bmod 7$	4	2	1	4	2	1	4	2	1	4	2	1	4	2	1	4	2	1	4	2
$5^k \bmod 7$	5	4	6	2	3	1	5	4	6	2	3	1	5	4	6	2	3	1	2	3
$6^k \bmod 7$	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1

Each row is evidently periodic. More precisely, the order of a mod 7 tells us the number of different powers of a mod 7 before the powers start to repeat. For instance, 2 mod 7 has order 3 and the sequence of powers of 2 mod 7 has a repeating block of length 3. In general, we want to show that if a mod m has order n then the sequence of powers of a mod m looks like $1, a, a^2, \ldots, a^{n-1}, 1, a, a^2, \ldots \bmod m$ with a repeating block of length n and this repeating block is as small as possible:

(1) (Repeating Block) Every power of a mod m is a^r mod m where $0 \leq r \leq n-1$,
(2) (Minimality) The powers $1, a, a^2, \ldots, a^{n-1}$ mod m are distinct.

Theorem 2.1. *Let a mod m have order n. For $k \geq 0$, $a^k \equiv 1 \bmod m$ if and only if $n|k$.*

Proof. If $n|k$, say $k = nq$, then $a^k = a^{nq} = (a^n)^q \equiv 1^q \equiv 1 \bmod m$.

For the converse direction, that if $a^k \equiv 1 \bmod m$ then $n|k$, write $k = nq + r$ with integers q and r such that $0 \leq r < n$. Then

$$1 \equiv a^k = (a^n)^q a^r \equiv a^r \bmod m.$$

Since $0 \leq r < n$, the minimality built into n as the order of $a \bmod m$ forces r to be zero (why?). Thus $k = nq$, so $n|k$. □

Corollary 2.2. *For $k \geq 0$, the condition $a^k \equiv 1 \bmod m$ is the same as saying the order of $a \bmod m$ divides k.*

Proof. This is just a restatement of Theorem 2.1 without giving a label to the order of $a \bmod m$. □

Example 2.3. Every nonzero number mod 7 satisfies $a^6 \equiv 1 \bmod 7$, so its order must be a factor of 6, and hence is 1, 2, 3, or 6. For example, from $2^3 \equiv 1 \bmod 7$ and $2 \not\equiv 1 \bmod 7$ we know that 2 mod 7 has order 3: the order has to divide 3 and is not 1, so it is 3. More generally, if $a^p \equiv 1 \bmod m$ for a prime number p and $a \not\equiv 1 \bmod m$, then $a \bmod m$ has order p because the only factor of p greater than 1 is p itself.

When $a^n \equiv 1 \bmod m$, the powers of $a \bmod m$ repeat themselves every n turns: for any integers $q \geq 0$ and $\ell \geq 0$,

$$a^{\ell+nq} = a^\ell a^{nq} = a^\ell (a^n)^q \equiv a^\ell (1^q) \equiv a^\ell \bmod m. \tag{2.1}$$

Theorem 2.4. *Let $a \bmod m$ have order n. Then every power of $a \bmod m$ is $a^r \bmod m$ for a unique r from 0 to $n-1$.*

Proof. This will be another application of division with remainder.

Given an arbitrary power a^k, write $k = nq + r$ where $0 \leq r \leq n-1$. Then $a^k \equiv a^r \bmod m$ by (2.1) with $\ell = r$ Thus every power of $a \bmod m$ is some $a^r \bmod m$ where $0 \leq r \leq n-1$. So far we have *not* used the minimality of n, *i.e.*, that n is the order of $a \bmod m$.

To prove each power of $a \bmod m$ has the form $a^r \bmod m$ for exactly one r from 0 to $n-1$ amounts to showing the powers $1, a, a^2, \ldots, a^{n-1} \bmod m$ are distinct. Here is where the *minimality* of n is going to be used.

Suppose the list of powers $1, a, a^2, \ldots, a^{n-1} \bmod m$ contains a repetition:

$$a^i \equiv a^j \bmod m$$

where $1 \leq i < j \leq n-1$. (Be attentive to the inequalities here.) Then

$$a^i \equiv a^j \bmod m \Longrightarrow a^i \equiv a^i a^{j-i} \bmod m \Longrightarrow a^{j-i} \equiv 1 \bmod m \tag{2.2}$$

since $a^i \bmod m$ is invertible. But $0 < j - i < n$, so the congruence $a^{j-i} \equiv 1 \bmod m$ contradicts the definition of n, since the exponent $j-i$ is a positive integer less than n, while n is the minimal positive integer satisfying $a^n \equiv 1 \bmod m$. Hence we have a contradiction, so the powers among $1, a, a^2, \ldots, a^{n-1} \bmod m$ are distinct from one another. □

Theorem 2.4 gives a nice combinatorial interpretation of the order of $a \bmod m$: this order is the number of distinct powers of $a \bmod m$. For example, 2 mod 7 has order 3 and there are 3 different powers of 2 mod 7.

Theorem 2.5. *Let $a \bmod m$ have order n. For integers k and $\ell \geq 0$, $a^k \equiv a^\ell \bmod m$ if and only if $k \equiv \ell \bmod n$.*

Proof. Without loss of generality, $k \leq \ell$. Write the condition $a^k \equiv a^\ell \bmod m$ as $a^{\ell-k} \equiv 1 \bmod m$ (see (2.2)). Now use Corollary 2.2. □

3. Orders of Powers

We now compare the orders of $a \bmod m$ and $a^k \bmod m$, when $k \geq 0$. Let $a \bmod m$ have order n. Since $(a^k)^n = (a^n)^k \equiv 1^k \equiv 1 \bmod m$, the order of $a^k \bmod m$ divides n by Corollary 2.2. Which factor of n is it?

Example 3.1. Suppose $a \bmod m$ has order 12, so $a^{12} \equiv 1 \bmod m$ and $a^i \not\equiv 1 \bmod m$ for $i = 1, 2, \ldots, 11$. Any power of $a \bmod m$ has order that is a factor of 12. It is plausible that $a^2 \bmod m$ has order 6: since $a \bmod m$ takes 12 powers until it first cycles around to 1, $a^2 \bmod m$ takes only 6 powers to get there. Thus $a^2 \bmod m$ has order $6 = 12/2$. On the other hand, it is absurd to say $a^8 \bmod m$ has order $12/8$, as $12/8$ is not an integer. The successive powers of $a^8 \bmod m$ are

$$a^8 \not\equiv 1 \bmod m, \quad (a^8)^2 = a^{16} \equiv a^4 \not\equiv 1 \bmod m, \quad (a^8)^3 = a^{24} = (a^{12})^3 \equiv 1^3 \equiv 1 \bmod m,$$

so $a^8 \bmod m$ has order 3, which we can write as $12/4$. What we divide 12 by to get the order of $a^8 \bmod m$ is not 8, but the largest factor that 8 has in common with 12, namely 4.

Theorem 3.2. *Let $a \bmod m$ have order n and k be a positive integer.*

1. *If $k|n$ then $a^k \bmod m$ has order n/k.*
2. *If $(k, n) = 1$ then $a^k \bmod m$ has order n. That is, raising $a \bmod m$ to a power relatively prime to its order doesn't change the order.*
3. *For general $k \in \mathbf{Z}^+$, $a^k \bmod m$ has order $n/(k, n)$.*

The third part includes the first two parts as special cases (if $k|n$ then $n/(k, n) = n/k$, and if $(k, n) = 1$ then $n/(k, n) = n$), but we state those special cases separately because they are worth knowing on their own *and* because they can be proved independently of the general case. Understanding the proof of the first two parts of the theorem will help you better understand the proof of the third part. Basic to everything will be Corollary 2.2.

Proof. Let t be the (unknown) order of $a^k \bmod m$, so $(a^k)^t \equiv 1 \bmod m$ and t is the minimal positive exponent that fits this congruence. We want to show $t = n/k$ if $k|n$, $t = n$ if $(k, n) = 1$, and $t = n/(k, n)$ in general.

1) We assume $k|n$. The condition $(a^k)^t \equiv 1 \bmod m$ is the same as $a^{kt} \equiv 1 \bmod m$, so $n|kt$ by Corollary 2.2. Thus $n \leq kt$, so $n/k \leq t$. We also have the reverse inequality: since $(a^k)^{n/k} = a^{k(n/k)} = a^n \equiv 1 \bmod m$, $t \leq n/k$ by the definition of what the order of an element means. From $n/k \leq t$ and $t \leq n/k$, we have $t = n/k$.

2) We assume $(k, n) = 1$ and want to show $a^k \bmod m$ has order n.

The equation $(a^k)^t \equiv 1 \bmod m$ is the same as $a^{kt} \equiv 1 \bmod m$, so $n|kt$ by Corollary 2.2. Since n and k are relatively prime, from $n|kt$ we conclude that $n|t$, so $n \leq t$. We have the reverse inequality too: $(a^k)^n = a^{kn} = (a^n)^k \equiv 1^k \equiv 1 \bmod m$, so $t \leq n$ by the definition of the order of an element. Therefore $t = n$.

3) In the general case, for any k, we want to show $t = n/(k, n)$. The congruence $(a^k)^t \equiv 1 \bmod m$ is the same as $a^{kt} \equiv 1 \bmod m$, so $n|kt$ by Corollary 2.2. Write $kt = nq$ for some integer $q \geq 1$.

Factor (k, n) out of both k and n: write $k = (k, n)k'$ and $n = (k, n)n'$, so $(k', n') = 1$. Notice $n' = n/(k, n)$, so we want to show $t = n'$. In the equation $kt = nq$ we can cancel (n, k) from both sides:

$$kt = nq \Longrightarrow (k, n)k't = (k, n)n'q \Longrightarrow k't = n'q,$$

so $n'|k't$. Since n' and k' are relatively prime, from $n'|k't$ we get $n'|t$, so $n' \leq t$.

We have the reverse inequality too:

$$(a^k)^{n'} = a^{kn'} \stackrel{!}{=} a^{nk'} = (a^n)^{k'} \equiv 1^{k'} \equiv 1 \bmod m.$$

Let's explain the equality with the exclamation point. The exponents kn' and nk' are equal since they are each the same as $kn/(k,n)$.

From $(a^k)^{n'} \equiv 1 \bmod m$ we have $t \leq n'$. Earlier we saw $n' \leq t$, so $t = n' = n/(k,n)$ and we are done. □

Example 3.3. If $a \bmod m$ has order 12, here is a list of orders of powers of $a \bmod m$. The order of $a^k \bmod m$ is equal to $12/(k,12)$. Compute successive powers of $a^k \bmod m$ for each k to verify directly that the values in the table are correct.

k	1	2	3	4	5	6	7	8	9	10	11	12
order of $a^k \bmod m$	12	6	4	3	12	2	12	3	4	6	12	1

Example 3.4. If $a \bmod m$ has order 12 then $a^k \bmod m$ has order 12 precisely when $(k,12) = 1$. Look at the table above and notice 12 appears under $k = 1, 5, 7$, and 11, which are relatively prime to 12.

Remark 3.5. A unit mod m and its inverse have the same order, since the powers of the inverse are the same as the powers of the original unit in reverse order.

For some moduli m, there is a unit whose order is $\varphi(m)$. That means its powers fill up all possible units.

Example 3.6. The order of 2 mod 7 is $6 = \varphi(7)$ and every unit mod 7 is a power of 2. We can see this in the row of powers of 2 mod 7 in the table in Example 1.1.

Example 3.7. The order of 2 mod 9 is $6 = \varphi(9)$: the powers of 2 mod 9 are 2, 4, 8, 7, 5, 1, which are all the units mod 9.

Any unit mod m whose order is $\varphi(m)$ is called a *generator* or *primitive root* mod m. For instance, Examples 3.6 and 3.7 tell us that 2 is a generator mod 7 and mod 9. It is not a generator mod 31 since $\varphi(31) = 30$ and 2 mod 31 has order 5. The order of 3 mod 31 turns out to be 30, so 3 is a generator mod 31. There is no generator for modulus 8 since $\varphi(8) = 4$ while all units square to 1, so no unit mod 8 has order 4. One of the problems studied by number theorists like Gauss was determining all m for which there is a generator mod m.

4. Order of products

How is the order of a product $a_1a_2 \bmod m$ related to the orders of the factors $a_1 \bmod m$ and $a_2 \bmod m$? In this generality not much can be said!

Example 4.1. Suppose $a \bmod m$ has order 5. Then $a^4 \bmod m$, the inverse of $a \bmod m$, has order 5 and $a^2 \bmod m$ has order 5, but the product $aa^4 \equiv 1 \bmod m$ has order 1 while the product $aa^2 = a^3 \bmod m$ has order 5.

If $a_1^{n_1} \equiv 1 \bmod m$, and $a_2^{n_2} \equiv 1 \bmod m$, then $(a_1a_2)^{n_1n_2} = a_1^{n_1n_2}a_2^{n_1n_2} \equiv 1 \cdot 1 \equiv 1 \bmod m$. For example, if $a_1^6 \equiv 1 \bmod m$ and $a_2^4 \equiv 1 \bmod m$ then $(a_1a_2)^{24} = a_1^{24}a_2^{24} \equiv 1 \cdot 1 \equiv 1 \bmod m$. So when $a_1 \bmod m$ has order dividing 6 and $a_2 \bmod m$ has order dividing 4 then $a_1a_2 \bmod m$ has order dividing 24. (Remember, $a_1^6 \equiv 1 \bmod m$ does *not* mean $a_1 \bmod m$ has order 6, but rather than the order divides 6. It might be 1, 2, or 3 and still satisfy $a_1^6 \equiv 1 \bmod m$.)

Actually, we can bound the order of $a_1a_2 \bmod m$ by something a little bit better in general than the product n_1n_2. The least common multiple $[n_1, n_2]$ is divisible by n_1 and

n_2, so $(a_1a_2)^{[n_1,n_2]} = a_1^{[n_1,n_2]}a_2^{[n_1,n_2]} \equiv 1 \cdot 1 \equiv 1 \bmod m$. For example, if $a_1^6 \equiv 1 \bmod m$ and $a_2^4 \equiv 1 \bmod m$ then $(a_1a_2)^{12} = a_1^{12}a_2^{12} \equiv 1 \cdot 1 \equiv 1 \bmod m$. So when $a_1 \bmod m$ has order dividing 6 and $a_2 \bmod m$ has order dividing 4, $a_1a_2 \bmod m$ has order dividing 12, not just 24.

When the orders of $a_1 \bmod m$ and $a_2 \bmod m$ are relatively prime, we can say *exactly* what the order of $a_1a_2 \bmod m$ is:

Theorem 4.2. *Let $a_1 \bmod m$ and $a_2 \bmod m$ have respective orders n_1 and n_2. If $(n_1, n_2) = 1$ then $a_1a_2 \bmod m$ has order n_1n_2.*

In words, for units with *relatively prime* orders, the order of their product is the product of their orders.

Proof. Since

$$(a_1a_2)^{n_1n_2} = a_1^{n_1n_2}a_2^{n_1n_2} = (a_1^{n_1})^{n_2}(a_2^{n_2})^{n_1} \equiv 1 \cdot 1 \equiv 1 \bmod m,$$

we see $a_1a_2 \bmod m$ has order dividing n_1n_2 by Corollary 2.2.

Let n be the order of $a_1a_2 \bmod m$. In particular, $(a_1a_2)^n \equiv 1 \bmod m$. From this we will show $n_1|n$ and $n_2|n$. Since

$$a_1^n a_2^n \equiv 1 \cdot 1 \equiv 1 \bmod m, \tag{4.1}$$

raising both sides of (4.1) to the power n_2 (to kill off the a_2 factor) gives us

$$a_1^{nn_2} \equiv 1 \bmod m.$$

Therefore $n_1|nn_2$ by Corollary 2.2. Since $(n_1, n_2) = 1$, we conclude $n_1|n$. Now raising both sides of (4.1) to the power n_1 gives $a_2^{nn_1} \equiv 1 \bmod m$, so $n_2|nn_1$ by Corollary 2.2, and thus $n_2|n$.

Since $n_1|n$, $n_2|n$ *and* $(n_1, n_2) = 1$, we conclude that $n_1n_2|n$. Since we already showed $n|n_1n_2$ (in the first paragraph of the proof), we conclude $n = n_1n_2$. □

Example 4.3. Modulo 21, -1 has order 2 and 4 has order 3. Therefore $-4 = 17$ has order 6.

Example 4.4. If $a_1 \bmod m$ has order 5 and $a_2 \bmod m$ has order 8, then $a_1a_2 \bmod m$ has order 40.

Remark 4.5. While Theorem 4.2 shows that a product of units with relatively prime orders has a predictable order, we can ask what can be said if we *start* with $a \bmod m$ of order n and write $n = n_1n_2$ where $(n_1, n_2) = 1$. Can we express $a \bmod m$ as a product of units with orders n_1 and n_2? The answer is yes, and such units are unique mod m. We omit the proof.

The least common multiple is not just an upper bound on the order of a product of two units, but can be realized as the order of *some* product of their powers:

Corollary 4.6. *Let $a_1 \bmod m$ and $a_2 \bmod m$ be two units with respective orders n_1 and n_2. For some positive integers k_1 and k_2, $a_1^{k_1}a_2^{k_2}$ has order $[n_1, n_2]$.*

Proof. The basic idea is to write $[n_1, n_2]$ as a product of two relatively prime factors and then find exponents k_1 and k_2 such that $a_1^{k_1} \bmod m$ and $a_2^{k_2} \bmod m$ have orders equal to those factors. Then the order of $a_1^{k_1} \bmod m$ and $a_2^{k_2} \bmod m$ will be equal to the product of the factors (Theorem 4.2), which is $[n_1, n_2]$ by design.

Here are the details. Factor n_1 and n_2 into primes:

$$n_1 = p_1^{e_1} \cdots p_r^{e_r}, \quad n_2 = p_1^{f_1} \cdots p_r^{f_r}.$$

We use the same list of (distinct) primes in these factorizations, and use an exponent 0 on a prime that is not a factor of one of the integers. The least common multiple is

$$[n_1, n_2] = p_1^{\max(e_1, f_1)} \cdots p_r^{\max(e_r, f_r)}.$$

Break this into a product of two factors, one being a product of the prime powers where $e_i \geq f_i$ and the other using prime powers where $e_i < f_i$. Call these two numbers ℓ_1 and ℓ_2:

$$\ell_1 = \prod_{e_i \geq f_i} p_i^{e_i}, \quad \ell_2 = \prod_{e_i < f_i} p_i^{f_i}.$$

Then $[n_1, n_2] = \ell_1 \ell_2$ and $(\ell_1, \ell_2) = 1$ (since ℓ_1 and ℓ_2 have no common prime factors). By construction, $\ell_1 | n_1$ and $\ell_2 | n_2$. Then $a_1^{n_1/\ell_1} \bmod m$ has order ℓ_1 and $a_2^{n_2/\ell_2} \bmod m$ has order ℓ_2. Since these orders are relatively prime and the two powers of $a_1 \bmod m$ and $a_2 \bmod m$ commute with each other, $a_1^{n_1/\ell_1} a_2^{n_2/\ell_2} \bmod m$ has order $\ell_1 \ell_2 = [n_1, n_2]$. □

Example 4.7. Suppose $a_1 \bmod m$ has order $n_1 = 60 = 2^2 \cdot 3 \cdot 5$ and $a_2 \bmod m$ has order $n_2 = 630 = 2 \cdot 3^2 \cdot 5 \cdot 7$. Then $[n_1, n_2] = 2^2 \cdot 3^2 \cdot 5 \cdot 7$. We can write this as $(2^2 \cdot 5) \cdot (3^2 \cdot 7)$, where the first factor appears in n_1, the second in n_2, and the factors are relatively prime. Then $a_1^3 \bmod m$ has order $2^2 \cdot 5$ and $a_2^{10} \bmod m$ has order $3^2 \cdot 7$ (why?). These orders are relatively prime, so $a_1^3 a_2^{10} \bmod m$ has order $2^2 \cdot 5 \cdot 3^2 \cdot 7 = [n_1, n_2]$.

Since the same power of 5 appears in both n_1 and n_2, there is another factorization of $[n_1, n_2]$ we can use: placing the 5 in the second factor, we have $[n_1, n_2] = (2^2)(3^2 \cdot 5 \cdot 7)$. Then $a_1^{15} \bmod m$ has order 2^2 and $a_2^2 \bmod m$ has order $3^2 \cdot 5 \cdot 7$ (why?). These orders are relatively prime, so $a_1^{15} a_2^2 \bmod m$ has order $2^2 \cdot 3^2 \cdot 5 \cdot 7 = [n_1, n_2]$.