ORDERS OF UNITS IN MODULAR ARITHMETIC

KEITH CONRAD

1. INTRODUCTION

If $a \bmod m$ is a unit then $a^{\varphi(m)} \equiv 1 \bmod m$ by Euler's theorem. Depending on a, it might happen that $a^n \equiv 1 \bmod m$ for a positive integer n that is *smaller* than $\varphi(m)$.

Example 1.1. Let $m = 7$. The following table shows that the first time a unit mod 7 has a power congruent to 1 varies with the unit. While Euler's theorem (or 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 when $a \not\equiv 3$ or 5 mod 7.

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. Let $m = 15$. Since $\varphi(15) = 8$, Euler's theorem says $a^8 \equiv 1 \bmod 15$ when $(a, 15) = 1$. But in fact exponent 8 is *higher* than necessary: the table below shows we can use exponent 1, 2, or 4.

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		

The fact that sometimes $a^n \equiv 1 \bmod m$ where $0 < n < \varphi(m)$, depending on a, leads us to give a name to the first exponent that fits this condition when the base is a.

Definition 1.3. The *order* of a unit $a \bmod m$ 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, we see 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.

Example 1.7. A unit mod m and its inverse (like 2 mod 15 and 8 mod 15) have the same order, since their powers are the same except in reverse order.

Example 1.8. For a fraction a/b in reduced form with $(10, b) = 1$, the number of digits in the repeating part of its decimal expansion is the order of 10 mod b. We will discuss this in Section 4.

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 1.9. If $m > 2$ then $-1 \bmod m$ 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 $-1 \bmod 2$ has order 1.

The order of any unit mod m is at most $\varphi(m)$, by Euler's theorem. We will see that the relation is stronger than an inequality: the order is a *factor* of $\varphi(m)$. For instance, in Example 1.1 we see that the order of every unit mod 7 is a factor of 6.

Warning. If $a^n \equiv 1 \bmod m$, this does not mean a mod m has order n, since the exponent might not be as small as possible. For example, $(-1)^4 \equiv 1 \bmod m$, but this doesn't mean $-1 \bmod m$ has order 4, and in fact it does not 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 $a^k \bmod m$. In Section 5 we will discuss the order of a product of two units if we know the order of each unit already. Some applications of orders, including to decimal periods, are in Section 4. Finally, in Section 6 we will show that for prime p there is a unit modulo p with order $p - 1$.

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 unit 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 looks 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. 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 $a^r \bmod m$ 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 $k \geq 0$, $a^k \equiv 1$ mod m if and only if $n \mid k$.*

Proof. If $n \mid k$, say $k = nn'$, then $a^k = a^{nn'} = (a^n)^{n'} \equiv 1$ mod m since $a^n \equiv 1$ mod m.

Now assume $a^k \equiv 1$ mod m. We want to prove $n \mid k$. Using division with remainder we can write $k = nq + r$ where q and r are integers and $0 \leq r < n$. Our goal is to show $r = 0$.

We have
$$a^k = a^{nq+r} = (a^n)^q a^r \implies a^k \equiv (a^n)^q a^r \text{ mod } m.$$
The left side of the congruence is 1 by hypothesis and $a^n \equiv 1$ mod m by part of the definition of n being the order of a mod m. Therefore the congruence becomes $1 \equiv a^r$ mod m. Since $0 \leq r < n$ and n is the *least* positive exponent that makes a power of a congruent to 1 mod m, r is not positive. Thus $r = 0$, so $k = nq$, which says $n \mid k$. $\square$

Corollary 2.2. *If $(a, m) = 1$ and a mod m has order n then $n \mid \varphi(m)$.*

Proof. By Euler's theorem, $a^{\varphi(m)} \equiv 1$ mod m. Now apply Theorem 2.1. $\square$

Example 2.3. Every unit a mod 19 satisfies $a^{18} \equiv 1$ mod 19, so its order must be a factor of 18, and hence is 1, 2, 9, or 18. Let's use this to determine the order of 2 mod 19. Certainly it is not 1. It is not 2 either, since $2^2 = 4 \not\equiv 1$ mod 19. Could the order be 9? We can find 2^9 by repeated multiplication by 2, starting from the familiar power 2^5:

$$2^5 = 32 \equiv 13 \equiv -6 \text{ mod } 19 \implies 2^6 \equiv -12 \equiv 7 \text{ mod } 19$$
$$\implies 2^9 = 2^3 \cdot 2^6 \equiv 8 \cdot 7 = 56 \equiv -1 \text{ mod } 19.$$

Thus $2^9 \not\equiv 1$ mod 19. The order of 2 mod 19 is not 1, 2, or 9, so it has to be 18. We don't have to check this directly since we have instead eliminated all the other potential options.

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

$$(2.1) \qquad a^{\ell+nq} = a^\ell a^{nq} = a^\ell (a^n)^q \equiv a^\ell (1^q) \equiv a^\ell \text{ mod } m.$$

This next theorem and corollary show this repetition doesn't happen more often than every n turns.

Theorem 2.4. *Let a mod m have order n. For integers k and $\ell \geq 0$, $a^k \equiv a^\ell$ mod m if and only if $k \equiv \ell$ mod n.*

Proof. Without loss of generality, $k \leq \ell$. Since a mod m is invertible,

$$(2.2) \qquad a^k \equiv a^\ell \text{ mod } m \iff a^k \equiv a^k a^{\ell-k} \text{ mod } m \iff a^{\ell-k} \equiv 1 \text{ mod } m,$$

and Theorem 2.1 says $a^{\ell-k} \equiv 1$ mod m if and only if $n \mid (\ell - k)$, or $k \equiv \ell$ mod n. $\square$

Corollary 2.5. *Let a mod m have order n. Then every power of a mod m is a^r mod 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 $a^k \equiv a^r$ mod m by (2.1) with $\ell = r$. Thus every power of a mod m is a^r mod m where $0 \leq r \leq n - 1$. If $0 \leq r < s \leq n - 1$ then we $a^r \not\equiv a^s$ mod m because $r \not\equiv s$ mod n (Theorem 2.4). $\square$

We have shown the powers $1, a, a^2, \ldots, a^{n-1}$ mod m are distinct from one another and describe all possible powers of a mod m without repetition. This gives a nice combinatorial interpretation of the order of a mod m: it is the number of distinct powers of a mod m. For example, 2 mod 7 has order 3 and there are 3 different powers of 2 mod 7.

3. Orders of powers

When $a \bmod m$ has order n, what is the order of a power $a^k \bmod m$? Since $(a^k)^n = (a^n)^k \equiv 1^k \equiv 1 \bmod m$, the order of $a^k \bmod m$ divides n by Theorem 2.1. 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 $k \mid n$ 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 $k \mid n$ 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 Theorem 2.1.

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 $k \mid n$, $t = n$ if $(k, n) = 1$, and $t = n/(k, n)$ in general.

1) We assume $k \mid n$. The condition $(a^k)^t \equiv 1 \bmod m$ is the same as $a^{kt} \equiv 1 \bmod m$, so $n \mid kt$ by Theorem 2.1. 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 a unit is. 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 $n \mid kt$ by Theorem 2.1. Since n and k are relatively prime, from $n \mid kt$ we conclude that $n \mid t$, 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 a unit. Therefore $t = n$.

3) In the general case, for each $k \geq 1$ we want to show $t = n/(k, n)$. The congruence $(a^k)^t \equiv 1 \bmod m$ is the same as $a^{kt} \equiv 1 \bmod m$, which is the same as $n \mid kt$ by Theorem 2.1. So t is the smallest positive integer such that $n \mid kt$.

Factor (k, n) out of both k and n: set $k = (k, n)k'$ and $n = (k, n)n'$ with $k', n' \in \mathbf{Z}$. Then $(k', n') = 1$. We have

$$n \mid kt \implies (k, n)n' \mid (k, n)k't \implies n' \mid k't.$$

Since $(k', n') = 1$, we get $n' \mid t$, so $n' \leq t$.

We have the reverse inequality too:

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

Let's explain the equality with the exclamation point: $kn' = nk'$ since both products equal $kn/(k,n)$. 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. $\qquad\square$

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.

4. Applications of orders

As a first application of orders, we determine all consecutive powers of 2 and 3.

Theorem 4.1. *The consecutive powers of 2 and 3 in* $\mathbf{Z}^+$ *are* $(1,2),(2,3),(3,4)$, *and* $(8,9)$.

Proof. The condition that 2^m and 3^n (where m and n are nonnegative integers) are consecutive is that $2^m - 3^n = 1$ or $3^n - 2^m = 1$. In both cases we will list the solutions for small m and then prove there are no solutions for larger m.

Case 1: $2^m - 3^n = 1$. Letting $m = 0,1,2$ and trying to solve for n, the only solutions are $(2^m, 3^n) = (2,1)$ and $(4,3)$. We want to show there is no solution when $m \geq 3$. If $m \geq 3$ then 2^m is divisible by 8, so

$$3^n = 2^m - 1 \equiv -1 \equiv 7 \bmod 8.$$

This is impossible: since $3^2 \equiv 1 \bmod 8$, we have $3^{\text{even}} \equiv 1 \bmod 8$ and $3^{\text{odd}} \equiv 3 \bmod 8$, so the powers of 3 mod 8 do not include 7 mod 8. (This did not use anything about orders. The next case will.)

Case 2: $3^n - 2^m = 1$. Letting $m = 0,1,2,3$ and trying to solve for n, the only solutions are $(2^m, 3^n) = (2,3)$ and $(8,9)$. To show there are no solutions when $m \geq 4$, write

$$3^n = 1 + 2^m \equiv 1 \bmod 16.$$

Check yourself that the order of 3 mod 16 is 4. Then $4 \mid n$, say $n = 4\ell$, so

$$(4.1) \qquad\qquad 2^m = 3^n - 1 = 3^{4\ell} - 1 = 81^\ell - 1.$$

However, $81^\ell - 1$ is divisible by 5 (indeed, $81 \equiv 1 \bmod 5 \Rightarrow 81^\ell \equiv 1 \bmod 5$), so (4.1) is impossible because the right side is divisible by 5 and the left side is a power of 2. $\qquad\square$

Fermat's little theorem and its consequences (like the Fermat test) show the importance of considering $a^{n-1} \equiv 1 \bmod n$. Could we ever have $a^n \equiv 1 \bmod n$? Using a computer it's not hard to find $3^n \equiv 1 \bmod n$ when $n = 1,2,4,8,16,20,32,40,\ldots$, $4^n \equiv 1 \bmod n$ when $n = 1,3,9,21,27,63,81,147,\ldots$, and $5^n \equiv 1 \bmod n$ when $n = 1,2,4,6,8,12,16,18,\ldots$, but the case $a = 2$ is different and this will be our second application of orders.

Theorem 4.2. *There is no* $n > 1$ *for which* $2^n \equiv 1 \bmod n$.

Proof. Suppose $2^n \equiv 1 \bmod n$. Let p be the smallest prime factor of n, so p is the smallest factor of n that's greater than 1.

Let m be the order of 2 mod p. Since $2^n \equiv 1 \bmod n \implies 2^n \equiv 1 \bmod p$ we have $m \mid n$. Also $m \mid (p-1)$, so $m \leq p-1$. The only factor of n less than p is 1, so $m = 1$. Thus the condition $2^m \equiv 1 \bmod n$ becomes $2 \equiv 1 \bmod n$, so $n = 1$. $\qquad \square$

The base 2 in this theorem is the only one that fits: for each $a > 2$ there are infinitely many $n > 1$ for which $a^n \equiv 1 \bmod n$: use $n = (a-1)^k$ for all $k \geq 1$.

Our next application of orders, which is the original reason mathematicians became interested in them, is their link to periodic decimal expansions. A decimal expansion is called *periodic* if from some point onwards it has a repeating block of digits, and *purely periodic* if the repeating block occurs right from the start. For example, $4/27 = .148148148\ldots$ is purely periodic while $19/54 = .3518518518\ldots$ is periodic but not purely periodic. The *period length* of a repeating decimal is the number of digits in its smallest repeating block, so the decimal expansions of $4/27$ and $19/54$ have period length 3.[1]

Theorem 4.3. *Every purely periodic decimal expansion is a rational number between 0 and 1 with denominator relatively prime to 10, and conversely all such rational numbers have purely periodic decimal expansions. Moreover, if a/b is in reduced form between 0 and 1 with $(10, b) = 1$ then the period length of its decimal expansion is the order of 10 mod b. In particular, the period length of a/b divides $\varphi(b)$ and is independent of a.*

Proof. We start by writing a purely periodic decimal as a fraction. If $x = .\overline{c_1 c_2 \ldots c_d}$ has a periodic block of d terms then the digit c_1 occurs in positions for 10^{-1}, $10^{-(d+1)}$, $10^{-(2d+1)}$, and so on, the digit c_2 occurs in positions 10^{-2}, $10^{-(d+2)}$, $10^{-(2d+2)}$, and so on, so

$$
\begin{aligned}
x &= c_1 \sum_{k\geq 0} \frac{1}{10^{dk+1}} + c_2 \sum_{k\geq 0} \frac{1}{10^{dk+2}} + \cdots + c_d \sum_{k\geq 0} \frac{1}{10^{dk+d}} \\
&= \left(\frac{c_1}{10} + \frac{c_2}{10^2} + \cdots + \frac{c_d}{10^d} \right) \sum_{k\geq 0} \frac{1}{10^{dk}} \\
&= \left(\frac{c_1}{10} + \frac{c_2}{10^2} + \cdots + \frac{c_d}{10^d} \right) \frac{1}{1 - 1/10^d},
\end{aligned}
$$

by the formula for the sum of a geometric series. Rewriting $1/(1 - 1/10^d)$ as $10^d/(10^d - 1)$ and multiplying through the first factor in the numerator with the 10^d, we get

$$
x = \frac{c_1 10^{d-1} + c_2 10^{d-2} + \cdots + c_d}{10^d - 1}.
$$

This is a fraction between 0 and 1 with denominator relatively prime to 10.

Conversely, suppose a/b is rational between 0 and 1 with $(10, b) = 1$. If $b = 10^d - 1$ for some d then we could run the calculations above in reverse to show a/b has a purely periodic decimal expansion. Most denominators relatively prime to 10 are not $10^d - 1$, but we can rewrite the fraction to have such a denominator using Euler's theorem: since $10^{\varphi(b)} \equiv 1 \bmod b$, we have $10^{\varphi(b)} - 1 = bc$ for some integer c, so

$$
\frac{a}{b} = \frac{ac}{bc} = \frac{ac}{10^{\varphi(b)} - 1}.
$$

---

[1]Logically speaking, $4/27 = .148148\ldots$ could be said to have a repeating block "148148" of length 6. The period length is the *minimal* possible size of a repeating part.

This fraction is between 0 and 1 with denominator $10^{\varphi(b)} - 1$, so calculations at the start of the proof can be read in reverse to show the fraction has a purely periodic decimal expansion with a repeating part of $\varphi(b)$ digits. (If ac has fewer than $\varphi(b)$ base 10 digits, append 0's to the front of it; see Examples 4.5 and 4.6.)

This repeating part may not be as small as possible. The smallest repeating part has d digits where d is the smallest positive integer for which a/b can be written with denominator $10^d - 1$. Since a/b is in reduced form, its possible denominators are multiples of b, so its decimal period length is the smallest $d \geq 1$ for which $10^d - 1$ is a multiple of b, or equivalently $10^d \equiv 1 \bmod b$. The least d is the order of 10 mod b, which divides $\varphi(b)$ by Theorem 2.1. $\square$

Example 4.4. The order of 10 mod 27 is 3: $10^1 \equiv 10 \bmod 27$, $10^2 = 100 \equiv 19 \bmod 27$, $10^3 = 190 \equiv 1 \bmod 27$. Therefore every reduced fraction $a/27$ has a decimal period length 3. For example, to find the decimal of $20/27$ we rewrite the fraction to have denominator $10^3 - 1$:

$$\frac{20}{27} = \frac{20(10^3 - 1)/27}{10^3 - 1} = \frac{20(37)}{10^3 - 1} = \frac{740}{10^3 - 1}.$$

Since the numerator is 740, the proof of Theorem 4.3 tells us $20/27 = .\overline{740}$.

Example 4.5. The order of 10 mod 57 is 18, so $1/57$ has decimal period length 18. Explicitly,

$$\frac{1}{57} = \frac{(10^{18} - 1)/57}{10^{18} - 1} = \frac{\overbrace{17543859649122807}^{17 \text{ digits}}}{10^{18} - 1} = .\overline{017543859649122807}.$$

The initial 0 occurs since the decimal period length is 18 but $(10^{18} - 1)/57$ has 17 digits.

Example 4.6. The order of 10 mod 239 is 7, so $2/239$ has decimal period length 7. Explicitly,

$$\frac{2}{239} = \frac{2(10^7 - 1)/239}{10^7 - 1} = \frac{83682}{10^7 - 1} = .\overline{0083682}.$$

Two initial 0's occur since the decimal period length is 7 while $2(10^7 - 1)/239$ has 5 digits.

Remark 4.7. Fractions a/b and a'/b with the same denominator are guaranteed to have the same decimal period length when they are both in reduced form[2] but reduced and non-reduced fractions with the same denominator could have different decimal periods: $1/21 = .\overline{047619}$ has decimal period 6 while $7/21 = 1/3 = .\overline{3}$ does not.

If $(10, b) = 1$ then the decimal period length of $1/b$ divides $\varphi(b)$. Since $\varphi(b) = b - 1$ if b is prime and $\varphi(b) < b - 1$ if b is composite, the decimal period length of $1/b$ can be $b - 1$ only for prime b (other than 2 and 5), and this happens if and only if 10 mod b generates the units mod b. When $b < 100$, this occurs for $b = 7, 17, 19, 23, 29, 47, 59, 61, 97$. For example,

$$\frac{1}{7} = .\underbrace{\overline{142857}}_{6\,\text{digits}}, \quad \frac{1}{17} = .\underbrace{\overline{0588235294117647}}_{16\,\text{digits}}, \quad \frac{1}{19} = .\underbrace{\overline{052631578947368421}}_{18\,\text{digits}}.$$

It is believed that 10 mod p has order $p - 1$ for infinitely many primes p, or equivalently $1/p$ has decimal period length $p - 1$ for infinitely many primes p. This is a special case of Artin's primitive root conjecture, which will be described at the end of Section 6.

---

[2]More generally, the decimal period lengths are equal when $(a, b) = (a', b)$.

Everything we have done with decimal expansions in base 10 can be carried over with no essential changes to others bases, provided the fraction has a denominator relatively prime to the base. For example, using base 2, a reduced fraction a/b with odd denominator has binary period length equal to the order of 2 mod b.

Example 4.8. The order of 10 mod 11 is 2 while the order of 2 mod 11 is 10, so $1/11$ has decimal period length 2 and binary period length 10:

$$\frac{1}{11} = \frac{(10^2 - 1)/11}{10^2 - 1} = \frac{9}{10^2 - 1} = .\overline{09}$$

and

$$\frac{1}{11} = \frac{(2^{10} - 1)/11}{2^{10} - 1} = \frac{93}{2^{10} - 1} = \frac{\overbrace{1011101_2}^{7\,\text{digits}}}{2^{10} - 1} = .\overline{0001011101}.$$

5. Order of products

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

Example 5.1. Suppose a mod m has order 5. Then a^4 mod m, the inverse of a mod m, has order 5 and a^2 mod m also has order 5, but the product $aa^4 \equiv 1$ mod m has order 1 while the product $aa^2 = a^3$ mod m has order 5.

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

Theorem 5.2. *Let a_1 mod m and a_2 mod m have respective orders n_1 and n_2. If $(n_1, n_2) = 1$ then $a_1 a_2$ mod m has order $n_1 n_2$.*

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

Proof. Since

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

we see $a_1 a_2$ mod m has order dividing $n_1 n_2$ by Theorem 2.1.

Let n be the order of $a_1 a_2$ mod m. In particular, $(a_1 a_2)^n \equiv 1$ mod m. From this we will show $n_1 \mid n$ and $n_2 \mid n$. Since

$$(5.1) \qquad\qquad a_1^n a_2^n \equiv 1 \cdot 1 \equiv 1 \bmod m,$$

raising both sides of (5.1) to the power n_2 (to kill off the a_2 factor) gives us

$$a_1^{n n_2} \equiv 1 \bmod m.$$

Therefore $n_1 \mid nn_2$ by Theorem 2.1. Since $(n_1, n_2) = 1$, we conclude $n_1 \mid n$. Now raising both sides of (5.1) to the power n_1 gives $a_2^{n n_1} \equiv 1$ mod m, so $n_2 \mid nn_1$ by Theorem 2.1, and thus $n_2 \mid n$.

Since $n_1 \mid n$, $n_2 \mid n$, *and* $(n_1, n_2) = 1$, we conclude that $n_1 n_2 \mid n$. Since we already showed $n \mid n_1 n_2$ (in the first paragraph of the proof), we conclude $n = n_1 n_2$. $\qquad\square$

Example 5.3. Mod 21, -1 has order 2 and 4 has order 3. Therefore $-4 = 17$ has order 6.

Example 5.4. If a_1 mod m has order 5 and a_2 mod m has order 8, then $a_1 a_2$ mod m has order 40.

Corollary 5.5. *If $a_1, \ldots, a_r$ mod m are units with orders $n_1, \ldots, n_r$ and the n_i are pairwise relatively prime, then the product $a_1 \cdots a_r$ mod m has order $n_1 \cdots n_r$.*

Proof. Induct on r, with Theorem 5.2 being the case $r = 2$. Details are left to the reader. $\square$

Remark 5.6. While Theorem 5.2 shows that a product of units with relatively prime orders has a predictable order, what can be said if we *start* with a mod m of order n and write $n = n_1 n_2$ where $(n_1, n_2) = 1$: is a mod m a product of units with orders n_1 and n_2? The answer is yes, and those units are unique.

Suppose $a \equiv a_1 a_2$ mod m where a_1 mod m has order n_1 and a_2 mod m has order n_2. Therefore $a^{n_1} \equiv a_2^{n_1}$ mod m and $a^{n_2} \equiv a_1^{n_2}$ mod m. To remove the exponents on a_2 and a_1 we want to raise to an additional power that is an inverse of the exponent modulo the order of a_2 or a_1. In powers of a_1 the exponent only matters modulo n_1, and in powers of a_2 the exponent only matters modulo n_2. Since $(n_1, n_2) = 1$, $n_1 x + n_2 y = 1$ for some $x, y \in \mathbf{Z}$, so $n_1 x \equiv 1$ mod n_2 and $n_2 y \equiv 1$ mod n_1. Thus

$$a^{n_1} \equiv a_2^{n_1} \text{ mod } m \implies a^{n_1 x} \equiv a_2^{n_1 x} \equiv a_2 \text{ mod } m,$$

$$a^{n_2} \equiv a_1^{n_2} \text{ mod } m \implies a^{n_2 y} \equiv a_1^{n_2 y} \equiv a_1 \text{ mod } m,$$

so we solved for a_1 mod m and a_2 mod m as particular powers of a mod m. Conversely, $a = a^1 = a^{n_1 x + n_2 y} = (a^{n_2 y})(a^{n_1 x})$ where $a^{n_2 y}$ mod m has order n_1 while $a^{n_1 x}$ mod m has order n_2.

Dropping the assumption that n_1 and n_2 are relatively prime, $a_1 a_2$ mod m has order dividing $n_1 n_2$ since $(a_1 a_2)^{n_1 n_2} = a_1^{n_1 n_2} a_2^{n_1 n_2} \equiv 1 \cdot 1 \equiv 1$ mod m. More precisely, the order of $a_1 a_2$ mod m divides the least common multiple $[n_1, n_2]$: $(a_1 a_2)^{[n_1, n_2]} = a_1^{[n_1, n_2]} a_2^{[n_1, n_2]} \equiv 1 \cdot 1 \equiv 1$ mod m. For example, if a_1 mod m has order 6 and a_2 mod m has order 4, then $a_1 a_2$ mod m has order dividing 12, not just 24.

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 5.7. *Let a_1 mod m and a_2 mod 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 $a_1^{k_1}$ mod m and $a_2^{k_2}$ mod m have orders equal to those factors. Then the order of $a_1^{k_1}$ mod m and $a_2^{k_2}$ mod m will be equal to the product of the factors (Theorem 5.2), 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, $\ell_1 \mid n_1$ and $\ell_2 \mid n_2$. 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 $\ell_1 \ell_2 = [n_1, n_2]$. $\qquad\square$

Example 5.8. 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 $2^2 \cdot 3^2 \cdot 5 \cdot 7 = [n_1, n_2]$.

6. Units modulo a prime

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

Example 6.1. The order of 3 mod 7 is $6 = \varphi(7)$ and every unit mod 7 is a power of 3. We can see this in the row of powers of 3 mod 7 in the table in Example 1.1.

Example 6.2. 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.

A unit mod m whose order is $\varphi(m)$ is called a *generator* or *primitive root* mod m. For instance, Examples 6.1 and 6.2 tell us that 3 is a generator mod 7 and 2 is a generator mod 9. Example 1.2 shows there is no generator for modulus 15 since there are 8 units modulo 15 and their orders are 1, 2, or 4.

In a 1769 paper on decimal expansions, Lambert [5] conjectured that the units modulo a prime always have a generator. A proof was given by Euler in 1774 [2, Art. 37, 38], Legendre in 1785 [6, pp. 471–473], and Gauss in 1801 [3, Art. 52–55]. Gauss went farther than anyone else by classifying *all $m \geq 2$* such that the units mod m have a generator: $2, 4, p^k$, and $2p^k$ for odd primes p. We will focus just on the case of a prime modulus.

Theorem 6.3. *When p is a prime, there is a unit mod p with order $p - 1$.*

A common feature of all proofs of this theorem is that they are not constructive. There is no algorithm known for finding a generator of $(\mathbf{Z}/(p))^\times$ that is substantially faster than a brute force search: try $a = 2, 3, \ldots$ until you find an element with order $p - 1$. What makes Theorem 6.3 important, despite its nonconstructive nature, is that it guarantees a brute force search *will* eventually succeed.[3]

Theorem 6.3 is important not only in pure mathematics, but also in cryptography. A choice of generator for $(\mathbf{Z}/(p))^\times$ is one of the ingredients in two public key cryptosystems: Diffie-Hellman (this is the original public key system, if we discount earlier classified work by British intelligence) and ElGamal. You can look up these cryptosystems online.

We are now ready to prove Theorem 6.3.

---

[3] The Generalized Riemann Hypothesis implies a brute force search runs in polynomial time in $\log p$.

Proof. **Step 1**: We have the following equality in $(\mathbf{Z}/(p))[T]$:

$$T^{p-1} - 1 = (T-1)(T-2)\cdots(T-(p-1)).$$

Fermat's little theorem tells us $T^{p-1} - 1$ has roots $1, 2, \ldots, p-1 \mod p$. Therefore in $(\mathbf{Z}/(p))[T]$, $T^{p-1} - 1$ is divisible by $T-1, T-2, \ldots, T-(p-1)$. These linear factors are pairwise relatively prime, so in $(\mathbf{Z}/(p))[T]$

$$T^{p-1} - 1 = (T-1)(T-2)\cdots(T-(p-1))h(T)$$

for some polynomial $h(T)$. Computing the degrees of both sides shows $\deg h = 0$, so $h(T)$ is a nonzero constant. Then looking at leading coefficients on both sides shows $h(T) = 1$, and we're done.

Step 2: If d and n are positive integers with $d \mid n$ then $(T^d - 1) \mid (T^n - 1)$.

Let $n = dd'$. Then $T^n - 1 = T^{dd'} - 1 = (T^d)^{d'} - 1$.

The polynomial $T^{d'} - 1$ has 1 as a root, so it is divisible by $T - 1$:

$$T^{d'} - 1 = (T-1)g(T).$$

(Explicitly, $g(T) = T^{d'-1} + T^{d'-2} + \cdots + T + 1$.) Substituting T^d for T in this polynomial equation, we get

$$T^n - 1 = (T^d - 1)g(T^d),$$

showing $T^d - 1$ is a factor of $T^n - 1$.

Step 3: For each prime power q^e that divides $p-1$, there is a unit mod p with order q^e.

That a unit $a \mod p$ has order q^e is is the same as saying

$$a^{q^e} \equiv 1 \mod p, \quad a^{q^{e-1}} \not\equiv 1 \mod p.$$

This means $a \mod p$ is a root of $T^{q^e} - 1$ and is *not* a root of $T^{q^{e-1}} - 1$. And that is what we will do: show $T^{q^e} - 1$ has a root in $\mathbf{Z}/(p)$ that is not a root of $T^{q^{e-1}} - 1$.

From Step 2, with $d = q^e$ and $n = p-1$, $T^{p-1} - 1$ is divisible by $T^{q^e} - 1$. Since $T^{p-1} - 1$ in $(\mathbf{Z}/(p))[T]$ is a product of $T-1, T-2, \ldots, T-(p-1)$ by Step 1, any monic factor of $T^{p-1} - 1$ in $(\mathbf{Z}/(p))[T]$ must be a product of some of these linear factors (unique factorization!). Therefore $T^{q^e} - 1$ has q^e distinct roots in $\mathbf{Z}/(p)$, and by similar reasoning $T^{q^{e-1}} - 1$ has q^{e-1} distinct roots in $\mathbf{Z}/(p)$. As $q^e > q^{e-1}$, there must be an integer mod p that is a root of $T^{q^e} - 1$ and not a root of $T^{q^{e-1}} - 1$.

Step 4: There is an integer mod p that has order $p-1$.

Write $p-1$ as a product of primes:

$$p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}.$$

By Step 3, there is a unit $a_i \mod p$ with order $q_i^{e_i}$. Then Corollary 5.5 tells us $a_1 \cdots a_r \mod p$ has order $q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r} = p-1$. $\square$

Is each integer a other than $0, 1, -1$ a generator modulo p for infinitely many primes p? Not if a is a perfect square: for odd primes p, if $a = b^2$ in $\mathbf{Z}$ then $a^{(p-1)/2} = b^{p-1} \equiv 1 \mod p$, so $a \mod p$ has order at most $(p-1)/2$. Emil Artin conjectured in 1927 that for all other integers a (not $0, \pm 1$, or perfect squares) the answer is *yes*. This is called Artin's primitive root conjecture, and Hooley [4] showed in 1967 that this conjecture is a consequence of the Generalized Riemann Hypothesis.

References

[1] M. Bullynck, Decimal periods and their tables: a German research topic (1765–1801), *Historia Mathematica* **36** (2009), 137–160. Online at https://halshs.archives-ouvertes.fr/halshs-00663295/document.

[2] L. Euler, "Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia," Novi Commentarii academiae scientiarum Petropolitanae **18** (1773), pp. 85-135. Online at http://eulerarchive.maa.org//docs/originals/E449.pdf

[3] C. F. Gauss, *Disquisitiones Arithmeticae*, translated by A. A. Clarke, Yale Univ. Press, New Haven, 1966.

[4] C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.

[5] J. H. Lambert, "Adnotata quaedam de numeris eorumque anatomia," *Nova Acta Eruditorum* LXIX (1769), 107–128.

[6] A. M. Legendre, "Recherches d'Analyse Indéterminée," Mémoires de Mathématiques et de Physique de l'Académie Royale des Sciences de Paris (1785), 465–559. Online at https://gallica.bnf.fr/ark:/12148/bpt6k35847/f649.image.