Summary of facts about orders

1. The facts

For simplicity, let’s write $\mathbb{Z}_m$ for $\mathbb{Z}/m\mathbb{Z}$ with $m > 0$. Let’s be casual about omitting brackets, writing $3 \in \mathbb{Z}_{10}$ instead of $[3]_{10}$. Also, $p$ will always refer to a prime.

(a) For $a \in \mathbb{Z}_m$, if $a^n = 1$ with $n \geq 1$ then $a(a^{n-1}) = 1$, so $a$ is invertible (i.e., $a$ is a unit).

(b) For $a \in \mathbb{Z}_m$, the list of powers $1, a, a^2, a^3, \ldots$ must start cycling at some point:

- If $a$ is a unit, then the first repeat is back to 1. The first $n > 0$ such that $a^n = 1$ is called the order of $a$.

  Example: For $3 \in \mathbb{Z}_{10}$ the list of powers is $1, 3, 9, 7, 1, 3, 9, 7, \ldots$ and the order of 3 is 4.

  Example: In a finite field, every nonzero element is a unit and so has an order.

- If $a$ is not a unit, then the first repeat is not back to 1, but the powers do get stuck in a cycle sooner or later.

  Example: For $2 \in \mathbb{Z}_{24}$, the list of powers is $1, 2, 4, 8, 16, 8, 16, 8, 16, \ldots$.

(c) If $a$ is a unit in $\mathbb{Z}_m$, with order $n$, then the powers equal to 1 are precisely $a^0, a^n, a^{2n}, a^{3n}, \ldots$.

  In other words, $a^i = 1 \Leftrightarrow n|i$.

(d) (i) If $p$ is prime and $a$ is a nonzero element of $\mathbb{Z}_p$, then Fermat’s Little Theorem says $a^{p-1} = 1$. Therefore the order of $a$ divides $p - 1$.

(ii) More generally, for any $m$, if $a$ is a unit of $\mathbb{Z}_m$, then Euler’s Theorem says $a^{\phi(m)} = 1$. Therefore the order of $a$ divides $\phi(m)$.

(iii) Even more generally, if $R$ is any commutative finite ring and $a$ is a unit of $R$, then the order of $a$ divides the number of units in $R$.

Example: In a finite field with $q$ elements, the order of each nonzero element divides $q - 1$. (As you know, $q$ has to be a prime power.)
(iv) Still more generally, if $G$ is any finite group, abelian (commutative) or not, then the order of each element divides the size of the group\footnote{The word “order” is also used to refer to the size of a finite group, so the statement is that the order of each element divides the order of the group.}.

(e) If $a$ has order $n$ and if $k$ and $n$ are coprime, then $a^k$ also has order $n$.
More generally, if $a$ has order $n$ then for any $k \geq 0$, $a^k$ has order \( \frac{n}{\gcd(n, k)} \).

Example: In $\mathbb{Z}_{11}$, 6 has order 10. Then $6^2$ has order 5, and so do $6^4$, $6^6$, and $6^8$, since all these exponents have 2 as their gcd with 10.

(f) (i) The units of a given finite ring might have a \textit{generator} or \textit{primitive element}, meaning an element $g$ for which the powers $1, g, g^2, \ldots$ are all the units. An equivalent statement is that the order of $g$ is the same as the number of units.
Example: The units of $\mathbb{Z}_{10}$ are 1, 3, 7, 9, with generator 3.
The units of $\mathbb{Z}_8$ are 1, 3, 5, 7; there is no generator since each of these elements has square $= 1$.
(ii) In a finite field, where all nonzero elements are units, there is always a generator. In fact, there are $\phi(p)$ generators of $\mathbb{Z}_p$ for $p$ prime.

(g) (i) In a commutative ring, if $a$ and $b$ are units and $a$ has order $m$ and $b$ has order $n$, where $m$ and $n$ are coprime, then $ab$ has order $mn$.
(ii) If a commutative ring $R$ has a unit $a$ of order $r$ and a unit $b$ of order $s$, then $R$ has a unit of order $d$ where $d = \text{lcm}(r, s)$.

Note: This element is not necessarily $ab$, since for example if $b = a^{-1}$ then $a$ and $b$ have the same order $r$ and $\text{lcm}(r, r) = r$, but $ab = 1$, which is an element of order 1.

(h) If $m$ and $n$ are coprime, then the order of an element $a$ of $\mathbb{Z}/mn\mathbb{Z}$ is the lcm of the orders of the images of $a$ in $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.
In other words, if $a \leftrightarrow (a_1, a_2)$ under the isomorphism of $\mathbb{Z}/mn\mathbb{Z}$ with $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ according to the Chinese Remainder Theorem, then the order of $a$ is the lcm of the orders of $a_1$ and $a_2$.

2. Problems

Problem H-1. Explain: The order of $a$ is also the number of distinct elements (including 1) that are powers of $a$. 

Problem H-2. (i) Which of the statements in §1 are true in any finite ring with 1? (ii) Which statements are true in any finite field?

Problem H-3. (i) Show that \(a^p \equiv a \mod p\), whether or not \(p\) divides \(a\).

(ii) More generally, invent and prove a similar statement for a power of \(a\) in \(\mathbb{Z}_m\), involving \(\phi(m)\).

Problem H-4. If the units of \(\mathbb{Z}_m\) have a generator, show that there are \(\phi(\phi(m))\) units in all.

Problem H-5. Show that in the field \(\mathbb{Z}_p\) (for a prime \(p\)), if \(a\) is any nonzero element then \(a^{\frac{p-1}{2}} = \pm 1\).

(Method: Let \(b = a^{\frac{p-1}{2}}\) and observe that \(b^2 = 1\). Solve for \(b\) as in high-school algebra.)

Problem H-6. (i) Show that for positive integers \(d\) and \(n\), if \(d|n\) and \(d \neq n\), then \(d\frac{\frac{n}{q}}{q}\) for some prime divisor \(q\) of \(n\). (Suggestion: Think in terms of the prime factorization of \(n\).)

Example\(^2\): 4|60 so 4| (at least) one of \(\frac{60}{2}, \frac{60}{3}, \frac{60}{5}\), of which the last two work.

(ii) Apply this idea to show that an element \(a\) in \(\mathbb{Z}_p\) is not a generator of the units if and only if \(a^{(p-1)/q} = 1\) for some prime factor \(q\) of \(p - 1\).

In other words, if the powers of \(a\) return to 1 too soon, then one of the places they return to 1 is a power of the form given.

This provides a quick test for whether an element is a generator!

Example: In \(\mathbb{Z}_{17}\), the only prime factor of \(p - 1 = 16\) is 2 and \(\frac{16 - 1}{2} = 8\), so an element \(a\) is not a generator if and only if \(a^8 = 1\). Testing 2: \(2^4 = -1\) so \(2^8 = 1\), not a generator. Testing 3: \(3^4 = 81 = -4\) and \(3^8 = 16 = -1\), so 3 is a generator. In fact, in \(\mathbb{Z}_{17}\) all nonzero elements will have 8th power equal to \(\pm 1\), by Problem H-5; therefore the generators are the elements, such as 3, whose 8th power is \(-1\).

(iii) Use the calculators on the course home page to find a generator for (a) \(\mathbb{Z}_{31}\); (b) \(\mathbb{Z}_{151}\) (which you can see is prime by using the factoring routine). Say what you did.

Note: The calculators will accept simple expressions such as 150/3 in place of an explicit integer.

\(^2\text{not to do}\)
Problem H-7. Let $p$ be the first prime past 10 million. Find the smallest generator of the units of $\mathbb{Z}_p$.

(Use the calculators on the home page for testing primality, for factoring $p - 1$, and for residues of powers. Be careful about the numbers of zeros in integers! Include a record of the calculations you tried.)

Problem H-8. Use the Chinese Remainder Theorem to explain why the powers of 2 in $\mathbb{Z}_{24}$ cycle the way they do.


Problem H-10. Prove (g)-(i) in §1.