Euler's, Fermat's and Wilson's Theorems

R. C. Daileda

February 17, 2018

1 Euler's Theorem

Consider the following example.

Example 1. Find the remainder when 3^{103} is divided by 14.

We begin by computing successive powers of 3 modulo 14. The computations can easily be carried out in our heads since at each line we can always be sure we're never dealing with a number larger than 13, and the next line is simply obtained by multiplying the result of the previous line by 3.

$$\begin{aligned}
3^2 &\equiv 9 \equiv -5 \pmod{14},\\
3^3 &\equiv -15 \equiv -1 \pmod{14},\\
3^4 &\equiv -3 \pmod{14},\\
3^5 &\equiv -9 \equiv 5 \pmod{14},\\
3^6 &\equiv 15 \equiv 1 \pmod{14}.
\end{aligned}$$

Why did we stop here? Divide the real exponent we care about, 103, by 6: $103 = 17 \cdot 6 + 1$. We then have

$$3^{103} = 3^{17\cdot 6+1} = (3^6)17 \cdot 3 \equiv 1^{17} \cdot 3 \equiv 3 \pmod{14}$$

which means the remainder is $\boxed{3}$. We took advantage of the fact that $3^6 \equiv 1 \pmod{14}$ and that multiplication by 1 is trivial to convert the problem of reducing 3^{103} modulo 14 to the much more reasonable task of reducing the *exponent* 103 modulo 6. The reason we successively raised 3 to powers was to find the *smallest* exponent (namely 6) that would help us out. ♦

It turns out that what happened with the powers of 3 in the preceding example generalizes nicely to arbitrary moduli. As usual, we will introduce an abstract notion first and then return to congruences by applying it to $\mathbb{Z}/n\mathbb{Z}$.

Definition 1. Let G be a group, $g \in G$. If the set

$$\{n \mid n \in \mathbb{N} \text{ and } g^n = e\}$$

is nonempty, we define the *order of* g to be its least element. Otherwise we say the order of g is infinite. We denote the order of g by $\operatorname{ord}(g)$. So, $\operatorname{ord}(g)$ is the least $n \in \mathbb{N}$ so that $g^n = e$, if such an integer exists, and is infinite otherwise. ▲

Example 2.

- $\text{ord}(g) = 1$ if and only if $g = e$.
- In the example above, we see that $\text{ord}(3) = 6$ in $(\mathbb{Z}/14\mathbb{Z})^\times$.
- For $n \in \mathbb{Z}$, $\text{ord}(n)$ is infinite if $n \neq 0$ ($\text{ord}(0) = 1$ by our first observation). This is because if $n \neq 0$ and $k \in \mathbb{N}$, then $|kn| \geq 1$ so that $kn \neq 0$ (remember $\mathbb{Z}$ is additive, not multiplicative, so we don't use exponents).
- On the other hand, every element of $\mathbb{Z}/n\mathbb{Z}$ has finite order, since $n(a+n\mathbb{Z}) = na+n\mathbb{Z} = 0 + n\mathbb{Z}$.

♦

Lemma 1. *If G is a finite group and $g \in G$, then* $\text{ord}(g)$ *is finite.*

Proof. Since the list

$$g, g^2, g^3, g^4, \cdots$$

cannot contain infinitely many distinct elements, there exist exponents $i > j$ so that $g^i = g^j$. Cancelling we obtain $g^{i-j} = e$. Since $i - j \in \mathbb{N}$, this proves g has finite order.[1] □

Corollary 1. *Let $n \in \mathbb{N}$. Every element of $(\mathbb{Z}/n\mathbb{Z})^\times$ has finite order.*

Remark 1.

- $\mathbb{Z}/n\mathbb{Z}$ possesses two binary operations (although is only a group under one of them), hence has two notions of order. By caveat, from now on when we speak of order in $\mathbb{Z}/n\mathbb{Z}$ we will always mean *multiplicative order* (see below).
- When n is understood, we will write $\text{ord}(a)$ for $\text{ord}(a + n\mathbb{Z})$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. We will call it the *order of a modulo n*.
- If $g^n = e$ in G, then $g^{nm} = (g^n)^m = e^m = e$ for all $m \in \mathbb{Z}$.

▼

Proposition 1. *Let G be a group and $g \in G$ an element of finite order. Then*

$$\{n \,|\, n \in \mathbb{Z} \text{ and } g^n = e\} = \text{ord}(g)\mathbb{Z}.$$

Proof. The final remark above shows that we have the containment $\supseteq$. For the other, let n belong to the left hand side. Use the division algorithm to write $n = q \cdot \text{ord}(g) + r$ with $0 \leq r < \text{ord}(g)$. Then

$$e = g^n = (g^{\text{ord}(g)})^q g^r = e^q g^r = g^r.$$

This contradicts the minimality of $\text{ord}(g)$ unless $r = 0$, so that $n \in \text{ord}(g)\mathbb{Z}$, as claimed. □

In words, the proposition states that the only exponents that "annihilate" a group element are multiples of its order. Given a finite group G, a somewhat natural question to ask is if there is a *common* power that will annihilate *every* element. According to the proposition, an obvious, although probably cumbersome to compute, choice is the least common multiple of all of the orders of the elements of G. But there is a more natural choice, as the next result indicates.

[1] Note that we are not claiming that $\text{ord}(g) = i - j$, just that the set of positive powers of g equal to e is nonempty.

Theorem 1. *Let G be a finite abelian group, $g \in G$. Then*

$$g^{|G|} = e.$$

In particular, $\mathrm{ord}(g)$ *divides* $|G|$.

Proof. Recall from HW that the left translation $L_g : G \to G$, given by $x \mapsto gx$, is a bijection. Hence[2]

$$\prod_{x \in G} x = \prod_{x \in G} L_g(x) = \prod_{x \in G gx} = g^{|G|} \prod_{x \in G} x \;\; \Rightarrow \;\; e = g^{|G|},$$

by cancellation of the product from both sides. □

Remark 2. The preceding result holds for *all* finite groups G, although the proof, while still very elegant, is not quite as simple. It requires a fundamental group-theoretic result known as *Lagrange's Theorem.* ▼

We are almost ready to state Euler's Theorem, which is simply the theorem above couched in the language of congruences. To simplify its statement somewhat, and because it will later be of independent interest, we introduce our first number-theoretic function.

Definition 2. The *Euler φ function* (or *totient function*), $\varphi : \mathbb{N} \to \mathbb{N}$, is defined by

$$\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \left|\{a \in \mathbb{N} \,|\, 1 \le a \le n \text{ and } (a, n) = 1\}\right|.$$

▲

Remark 3. Since $\mathbb{Z}/\mathbb{Z}$ consists of a single element, it isn't technically a ring, so we can't talk about its unit group, meaning $\varphi(1) = |(\mathbb{Z}/\mathbb{Z})^\times|$ doesn't make sense. However, the alternate characterization given above does make sense when $n = 1$ and shows that we should take $\varphi(1) = 1$. ▼

Example 3.

n	$(\mathbb{Z}/n\mathbb{Z})^\times$	$\varphi(n)$
1	-	1
2	$\{1\}$	1
3	$\{1, 2\}$	2
4	$\{1, 3\}$	2
5	$\{1, 2, 3, 4\}$	4
6	$\{1, 5\}$	2
7	$\{1, 2, 3, 4, 5, 6\}$	6
8	$\{1, 3, 5, 7\}$	4
9	$\{1, 2, 4, 5, 7, 8\}$	6
10	$\{1, 3, 7, 9\}$	4
11	$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$	10
12	$\{1, 5, 7, 11\}$	4

[2]The products below are well-defined since G is abelian so we need not specify an order of multiplication.

♦

Remark 4. *Carmichael's conjecture* is that φ is always at least 2-to-1, i.e. given any $n \in \mathbb{N}$ there exists an $m \in \mathbb{N}$, $m \neq n$, so that $\varphi(m) = \varphi(n)$. ▼

Corollary 2 (Euler's Theorem)**.** *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. If $(a, n) = 1$, then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

In particular, the order of a modulo n divides $\varphi(n)$.

Proof. If $(a, n) = 1$, then $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Since $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, the theorem implies that

$$(a + n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z} \;\Rightarrow\; a^{\varphi(n)} + n\mathbb{Z} = 1 + n\mathbb{Z} \;\Rightarrow\; a^{\varphi(n)} \equiv 1 \pmod{n}.$$

The equation $(a + n\mathbb{Z})^{\varphi(n)} = 1 + n\mathbb{Z}$ also shows that the order of a modulo n divides $\varphi(n)$, since it implies the order of $a + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ divides $\varphi(n)$. □

Remark 5. Note that if $n \in \mathbb{N}$, $a \in \mathbb{Z}$ with $(a, n) = 1$ and $s \equiv t \pmod{\varphi(n)}$, then $a^s \equiv a^t \pmod{n}$. Indeed, we have $s = t + k \cdot \varphi(n)$ for some k so that by Euler's theorem

$$a^s = (a^{\varphi(n)})^k a^t \equiv 1^k a^t \equiv a^t \pmod{n}.$$

Hence we can reduce the exponent modulo $\varphi(n)$ in order to reduce the overall power modulo n. ▼

Example 4. Find the remainder when 7^{2018} is divided by 20.

Rather than compute the order of 7 modulo 20 as we did with our initial example, we use Euler's theorem as a substitute. Since $\varphi(20) = 8$ and $2018 \equiv 2 \pmod{8}$, we have

$$\begin{aligned} 7^{2018} &\equiv 7^2 \pmod{20} \\ &\equiv 9 \pmod{20} \end{aligned}$$

so that the remainder is $\boxed{9}$. ♦

Remark 6. In the preceding example, the actual order of 7 modulo 20 is 4, which probably is no harder to compute directly than $\varphi(20)$. However, once we have some rules for computing $\varphi(n)$ we will see that it is frequently much easier to find than the order of a given element and therefore much more convenient to work with in problems like the one above. ▼

We conclude this section with *Fermat's Little Theorem*. Historically Fermat's theorem preceded Euler's, and the latter served to generalize the former. However, in our presentation it is more natural to simply present Fermat's theorem as a special case of Euler's result. Nonetheless, it is a valuable result to keep in mind.

Corollary 3 (Fermat's Little Theorem)**.** *Let p be a prime and $a \in \mathbb{Z}$. If $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Since p is prime, $\varphi(p) = p - 1$ and $p \nmid a$ implies $(a, p) = 1$. The result then follows immediately from Euler's theorem. □

2 Wilson's Theorem

Let G be an abelian group and consider the product that occurred in the proof of Theorem 1:

$$P = \prod_{x \in G} x.$$

Notice that if p is prime and $G = (\mathbb{Z}/p\mathbb{Z})^\times$, then this product is just the congruence class

$$(p-1)! + p\mathbb{Z}.$$

It is natural to ask how this product depends on the group G. To answer this question we define

$$G(2) = \{g \in G \,|\, g^2 = e\}.$$

Note that $G(2)$ consists of the identity element and the elements of G of order 2 (if there are any).

Remark 7.

- Let G be a group and suppose $g \in G$ has order 2. Then $g^2 = e$ which implies $g^{-1} = g$. So $G(2)$ can also be thought of as the set of all elements of G that are their own inverses.
- For an abelian group G, the subset $G(2)$ is closed under the binary operation on G and itself satisfies the axioms of a group, i.e. is a *subgroup* of G. It is called the *2-torsion subgroup* of G.

▼

Example 5.

- If $G = (\mathbb{Z}/n\mathbb{Z})^\times$, then $x + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ belongs to $G(2)$ if and only if $x^2 + n\mathbb{Z} = 1 + n\mathbb{Z}$ if and only if $x^2 \equiv 1 \pmod{n}$.
- In the homework you found that $x^2 \equiv 1 \pmod{35}$ if and only if $x \equiv \pm 1, \pm 6 \pmod{35}$. Hence, if $G = \mathbb{Z}/35\mathbb{Z}$, then $G(2) = \{\pm 1 + 35\mathbb{Z}, \pm 6 + 35\mathbb{Z}\}$.
- If p is prime, then $x^2 \equiv 1 \pmod{p}$ if and only if $p | x^2 - 1 = (x-1)(x+1)$ if and only if $p|(x-1)$ or $p|(x+1)$ if and only if $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. Hence, for the group $G = (\mathbb{Z}/p\mathbb{Z})^\times$

$$G(2) = \{\pm 1 + p\mathbb{Z}\}.$$

⧫

We now prove our primary abstract result.

Theorem 2. *Let G be an abelian group. Then*

$$P = \prod_{x \in G} x = \prod_{x \in G(2)} x.$$

Proof. In the product P pair each element with its inverse, when its inverse is distinct from itself. This leaves behind only those elements that are their own inverses. □

Corollary 4 (Wilson's Theorem)**.** *If p is prime, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Let $G = (\mathbb{Z}/p\mathbb{Z})^\times$. We have already observed that

$$\prod_{x \in G} x = (p-1)! + p\mathbb{Z}.$$

We have also seen that $G(2) = \{\pm 1 + p\mathbb{Z}\}$ so that

$$\prod_{x \in G(2)} x = (1 + p\mathbb{Z})(-1 + p\mathbb{Z}) = -1 + p\mathbb{Z}.$$

By the theorem, we therefore have $(p-1)! + p\mathbb{Z} = -1 + p\mathbb{Z}$ which is equivalent to the statement of the corollary. □

Remark 8. The converse of Wilson's theorem is also true. So given $n \in \mathbb{N}$, determining the congruence class of $(n-1)!$ modulo n serves as a *primality test* for n. Unfortunately it is extremely inefficient. ▼

Example 6. Find the remainder when 99! is divided by 103.

We note that 103 is prime and so by Wilson's theorem

$$-1 \equiv 102! \equiv 99! \cdot 100 \cdot 101 \cdot 102 \equiv 99!(-3)(-2)(-1) \equiv -99! \cdot 3 \cdot 2 \pmod{103}.$$

Hence

$$99! \equiv 2^{-1}3^{-1} \pmod{103}$$

where the the negative exponents indicate inverses modulo 103 (i.e. in $(\mathbb{Z}/103\mathbb{Z})^\times$). The extended Euclidean algorithm takes a single step for both 2 and 3 and immediately yields the inverses 52 and 69, respectively. Hence

$$99! \equiv 52 \cdot 69 \equiv 3588 \equiv 86 \pmod{103}$$

so that the remainder is $\boxed{86.}$ Given that 99! has 156 digits, the fact that we were able to compute its remainder so easily (by hand!) demonstrates the utility of Wilson's theorem. ♦