4 Euler's Theorem

4.1 The Inclusion/Exclusion Principle

The "inclusion/exclusion principle" allows you to talk about the number of elements *included* in a large set, while *excluding* many of its subsets. In what follows:

"$\mathbf{A} \subset \mathbf{U}$" means "$\mathbf{A}$ is contained in $\mathbf{U}$"
"$\mathbf{U} \backslash \mathbf{A}$" means "$\mathbf{U}$ but not $\mathbf{A}$"
"$\mathbf{A} \cup \mathbf{B}$" means "the union of $\mathbf{A}$ and $\mathbf{B}$"
"$\mathbf{A} \cap \mathbf{B}$" means "the intersection of $\mathbf{A}$ and $\mathbf{B}$"
"$|\mathbf{U}|$" means "the number of elements in $\mathbf{U}$"

Q 4.1.1: $\mathbf{A} = \{\uparrow, \bowtie, \between, 7, \div\}$, $\mathbf{B} = \{\Delta, \square, \boxdot, \uparrow, 7\}$, and $\mathbf{C} = \{\boxdot, \Delta\}$
-$|\mathbf{A} \cup \mathbf{C}| =?$
-$|\mathbf{B} \cap \mathbf{C}| =?$
-$|\mathbf{A} \cap \mathbf{C}| =?$
-$|\mathbf{B} \cup \mathbf{C}| =?$
-$|\mathbf{A} \cup (\mathbf{B} \backslash \mathbf{C})| =?$
-$|(\mathbf{B} \cap \mathbf{C}) \cup (\mathbf{A} \cap \mathbf{B})| =?$
-$|(\mathbf{A} \cup \mathbf{B}) \backslash (\mathbf{A} \cap \mathbf{B})| =?$
-$|\mathbf{A} \cup \mathbf{B}| =?$
-$|\mathbf{A}| + |\mathbf{B}| - |\mathbf{A} \cap \mathbf{B}| =?$

Q 4.1.2: If $\mathbf{A} \subset \mathbf{U}$, then what is $|\mathbf{U} \backslash \mathbf{A}|$ in terms of $|\mathbf{A}|$ and $|\mathbf{U}|$?

Q 4.1.3: If $\mathbf{A} \subset \mathbf{U}$ and $\mathbf{B} \subset \mathbf{U}$, then what is $|\mathbf{U} \backslash (\mathbf{A} \cup \mathbf{B})|$ in terms of $|\mathbf{A}|$, $|\mathbf{B}|$, $|\mathbf{U}|$, and $|\mathbf{A} \cap \mathbf{B}|$? It may help to draw a venn diagram.

Q 4.1.4: If $\mathbf{A} \subset \mathbf{U}$, $\mathbf{B} \subset \mathbf{U}$, and $\mathbf{C} \subset \mathbf{U}$, then what is $|\mathbf{U} \backslash (\mathbf{A} \cup \mathbf{B} \cup \mathbf{C})|$ in terms of $|\mathbf{A}|$, $|\mathbf{B}|$, $|\mathbf{C}|$, $|\mathbf{U}|$, and their various intersections? Be careful to keep track of what your adding and subtracting.

Lets call an intersection of k different sets a "k-set". For example, $\mathbf{A} \cap \mathbf{B} \cap \mathbf{C}$, $\mathbf{A} \cap \mathbf{B} \cap \mathbf{D}$, $\mathbf{A} \cap \mathbf{C} \cap \mathbf{D}$, and $\mathbf{B} \cap \mathbf{C} \cap \mathbf{D}$ are all of the possible 3-sets involving $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, and $\mathbf{D}$. The "0-set" is just $\mathbf{U}$.

Q 4.1.5: If $x \in \mathbf{A} \cap \mathbf{B} \cap \mathbf{C} \cap \mathbf{D}$ (a 4-set), then
-How many 4-sets is x in, and what are they?
-How many 3-sets is x in, and what are they?
-How many 2-sets is x in, and what are they?
-How many 1-sets is x in, and what are they?

-How many 0-sets is x in, and what are they?
-What's the pattern?

Q 4.1.6: If, $j > k$ and x is in a j-set, then how many k-sets is x in?

Q 4.1.7: Say you count an element every time it shows up in an even k-set, and subtract it every time it shows up in an odd k-set. For example, if $x \in \mathbf{A} \cap \mathbf{B}$, you'd add it once for being in $\mathbf{U}$, subtract it twice for being in $\mathbf{A}$ and $\mathbf{B}$, and add it once more for being in $\mathbf{A} \cap \mathbf{B}$. That's 1-2+1=0. So if $x \in \mathbf{A} \cap \mathbf{B}$, it's counted a total of zero times.

Find how many times is x counted, total, if x is in each of the following sets. Write the equation you used.

- 0-set
- 1-set
- 2-set
- 3-set
- 4-set
- m-set

Q 4.1.8: Using the binomial expansion theorem (if you know it), show that if $x \in \mathbf{U}$ it's counted once, and that if x is in any of the subsets, $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, etc, then it's counted a total of zero times.

Q 4.1.9: Without actually writing it out, describe the equation for what $|\mathbf{U} \setminus (\mathbf{A} \cup \mathbf{B} \cup \cdots \cup \mathbf{Y} \cup \mathbf{Z})|$ is equal to.

4.2 $\varphi(N)$

$\varphi(N)$ is the "number of numbers less than N that are coprime to N". As a direct result of this definition, the number of elements in $\mathbb{Z}_N$ is equal to $\varphi(N)$, since $\mathbb{Z}_N$ is made up only of those numbers coprime to N. If you know the prime factorization of N, then you can find $\varphi(N)$ quickly.

Define the set $\mathbf{A}$ as the set of all numbers smaller than or equal to N that are multiples of the prime a, $\mathbf{B}$ as the set of all numbers smaller than or equal to N that are multiples of the prime b, etc.

Define $\mathbf{U}$ as the set of numbers less than or equal to N. Clearly, $|\mathbf{U}| = N$.

If $N = a^4b^3c^2$, for example, then you can find $\varphi(N)$ by finding the number of numbers in $\mathbf{U}$ that aren't in $\mathbf{A}$, $\mathbf{B}$, or $\mathbf{C}$. After all, if a number is not coprime to N, then it must be a multiple of one of N's prime factors. So finding $\varphi(N)$ amounts to finding $|\mathbf{U}\backslash(\mathbf{A}\cup\mathbf{B}\cup\mathbf{C})|$.

Q 4.2.1: How big is $|\mathbf{A}|$ when a is a prime factor of N? That is, how many numbers are less than or equal to N that are multiples of a?

Q 4.2.2: If a is a prime factor of N, what is $|\mathbf{U}\backslash\mathbf{A}| =$?
-Use the result to find the formula for $\varphi(N)$ when $N = a, a^j$, for prime a.

Q 4.2.3: -$\varphi(13) =$?
-$\varphi(64) =$?
-$\varphi(343) =$?

Q 4.2.4: What does it mean when $x \in \mathbf{A}\cap\mathbf{B}$?
-If a and b are prime factors of N, then $|\mathbf{U}\backslash(\mathbf{A}\cup\mathbf{B})| =$?
-Use the result to find a formula for $\varphi(N)$, when $N = ab, a^kb, a^jb^k$, for primes a and b. To simplify the equation, it may help to factor out a, then b.

Q 4.2.5: -$\varphi(15) =$?
-$\varphi(77) =$?
-$\varphi(63) =$?
-$\varphi(15125) =$?

Q 4.2.6: If a, b, and c are prime factors of N, then $|\mathbf{U}\backslash(\mathbf{A}\cup\mathbf{B}\cup\mathbf{C})| =$?
-Use the result to find a formula for $\varphi(N)$, when $N = abc, a^jb^kc^\ell$, for primes a, b, and c.

Q 4.2.7: -$\varphi(30) =$?
-$\varphi(195) =$?
-$\varphi(180) =$?

-$\varphi(1575) =?$

Q 4.2.8: A very important property of $\varphi(M)$ is that it's multiplicative. If $gcd(X, Y) = 1$, then $\varphi(XY) = \varphi(X) \cdot \varphi(Y)$. From what you've found so far show that:
-$\varphi(a^j b^k) = \varphi(a^j) \cdot \varphi(b^k)$
-$\varphi(a^j b^k c^\ell) = \varphi(a^j) \cdot \varphi(b^k) \cdot \varphi(c^\ell)$

To sum up: When p and$q$ are primes:

$$\varphi(N) = \begin{cases} p-1 & , N = p \\ p^{k-1}(p-1) & , N = p^k \\ (p-1)(q-1) & , N = pq \\ p^{k-1}(p-1)q^{j-1}(q-1) & , N = p^k q^j \end{cases}$$

This pattern continues, no matter how many primes factors N has.

Q 4.2.9: $\varphi(630) =?$

Q 4.2.10: How many elements do $\mathbb{Z}_{107}$ and $\mathbb{Z}_{107}^{\times}$ have?

4.3 The Theorem

A quick reminder, $\mathbb{Z}_M^\times$ is the set of numbers in $\mathbb{Z}_M$ that are coprime to M. This set is useful because everything in it has an inverse and you don't have to worry about zeros.

Example: Going from the $\mathbb{Z}_9$ table to the $\mathbb{Z}_9^\times$ table.

$\times$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

$\rightarrow$

$\times$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

$\rightarrow$

$\times$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

All that's needed is to construct the $\mathbb{Z}_9$ table, then locate all of the rows and columns not coprime to 9 (3 and 6) and remove them.

We've already learned that every row in the multiplicative table of $\mathbb{Z}_M^\times$ contains every number in $\mathbb{Z}_M^\times$, but in different orders. It may help to take a moment to look at the $\mathbb{Z}_9^\times$ example to check this.

Define E as the product of every number in a row, mod M. For example, for $\mathbb{Z}_9^\times$:

$E = [1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8]_9$
$= [2 \cdot 4 \cdot 5 \cdot 7 \cdot 8]_9$
$= [2 \cdot 4 \cdot 5 \cdot 2]_9$
$= [2 \cdot 4 \cdot 1]_9$
$= [2 \cdot 4]_9$
$= [8]_9$

It doesn't matter what row you're looking at, since the only difference between them is the order of the numbers.

$\times$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

The rows are related to each other in a pretty straight forward way. For example, to go from row 1 to row 4 in the multiplication table for $\mathbb{Z}_9^\times$, you just multiply every entry by 4:

$\times$	1	2	4	5	7	8
1	1	2	4	5	7	8
4	4	8	7	2	1	5

It's worth taking a moment to double check this.

Q 4.3.1: -Show that to transform row 1 into row a in the $\mathbb{Z}_M^\times$ table, all you have to do is multiply every term by a. If this is so obvious you don't know why I'm asking, then move on.

-Show that to go from row a to row b in $\mathbb{Z}_M^\times$, all you have to do is multiply every entry by some number, and find what that number is.

Q 4.3.2: -Construct the multiplication table for $\mathbb{Z}_{15}$.

-Do 3 and 5 have inverses? Where are all of the zeros?

-Construct the multiplication table for $\mathbb{Z}_{15}^\times$ by removing all the rows and columns not coprime to 15.

-How many rows are left?

-Is the table for $\mathbb{Z}_{15}^\times$ closed? That is; is there a combination of numbers in $\mathbb{Z}_{15}^\times$ that you can multiply together to get something not in $\mathbb{Z}_{15}^\times$? (consider what it means to be in $\mathbb{Z}_{15}^\times$)

Q 4.3.3: Show that $\mathbb{Z}_M^\times$ is closed in general. This amounts to showing that the product of two numbers that are coprime to M is another number coprime to M.

Q 4.3.4: Define E to be the product of every number in $\mathbb{Z}_M^\times$. For example, for $\mathbb{Z}_9^\times$, $E = [1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8]_9 = [8]_9$.

-The number of numbers in $\mathbb{Z}_M^\times$ is $\varphi(M)$, by definition. Show that the product, mod M, of every number in row a is $a^{\varphi(M)}E$.

Q 4.3.5: Using the fact that the product of every entry in a row always gives you the same thing, E, show that $[a^{\varphi(M)}]_M = 1$.

Q 4.3.6: You've just proven "Euler's theorem". Be very excited.

Euler's theorem states that, if $a \in \mathbb{Z}_M^\times$ (in other words, if $gcd(a, M) = 1$), then $[a^{\varphi(M)}]_M = 1$.

Euler's theorem, among other things, allows you to fix the "problem of exponents" that we saw in section 2.2. Since $[a^{\varphi(M)}]_M = 1$ for any $a \in \mathbb{Z}_M^\times$, we now have a way to "mod the exponent".

Example: $[4^{746}]_7 =?$

Since 7 is prime, $\varphi(7) = 7 - 1 = 6$. Therefore, by Euler's theorem, $[4^6]_7 = 1$.

$[4^{746}]_7$
$= [4^{744+2}]_7$
$= [4^{744}4^2]_7$
$= [\left(4^6\right)^{124} 4^2]_7$
$= [(1)^{124} 4^2]_7$
$= [4^2]_7$
$= [16]_7$
$= [2]_7$

So, finding that $[4^{746}]_7 = [4^2]_7$ is easy, because we can take advantage of the fact that $[746]_{\varphi(7)} = [2]_{\varphi(7)}$.

Q 4.3.7: $[3^{291}]_5 =?$

Q 4.3.8: $[7^{4673}]_{22} =?$

Q 4.3.9: $[13^{3067}]_{48} =?$

Euler's theorem also gives us a way of finding inverses.

$[a^{\varphi(M)}]_M = 1 \Rightarrow [a \cdot a^{\varphi(M)-1}]_M = 1 \Rightarrow a^{\varphi(M)-1}$ is the inverse of a. This provides a welcome relief to anyone tired of solving Diophantine equations.

Example: $[3^{-1}]_{35} =?$

$\varphi(35) = \varphi(5)\varphi(7) = (4)(6) = 24$. So $[3^{-1}]_{35} = [3^{23}]_{35}$. We can use fast exponentiation to do this quickly.

$[3^2]_{35} = 9$
$[3^4]_{35} = 11$
$[3^8]_{35} = 16$
$[3^{16}]_{35} = 11$

With this in hand, and using the fact that 23=16+4+2+1:

$[3^{-1}]_{35}$
$= [3^{23}]_{35}$
$= [(3^{16})(3^4)(3^2)(3)]_{35}$
$= [(11)(11)(9)(3)]_{35}$
$= [3267]_{35}$
$= [12]_{35}$
$= 12$
This is easy enough to double check: $[3 \cdot 12]_{35} = [36]_{35} = 1$.

Q 4.3.10: Find 5^{-1} in $\mathbb{Z}_{13}^{\times}$ using
-A Diophantine equation.
-Euler's theorem.

Q 4.3.11: $[3^{-1}]_{325} =?$

Q 4.3.12: Carefully consider how to find the decimal expansion of a fraction.
-*At least*, how often does a decimal expansion of a fraction with 7 in the denominator repeat?
-27 in the denominator?

Q 4.3.13: Prove that $300^{3000} - 1$ is divisible by 1001.

Q 4.3.14: We take any number a, and consider the set D of its divisors. Show that the sum of the values of $\varphi(d)$ for d in D is just a. For example, when $a = 10$: $\varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 4 = 10$.

4.4 Fermat's Little Theorem

Euler's theorem is a powerful than Fermat's Little theorem. While Fermat is a statement about primes, Euler is a statement about any number.

Q 4.4.1: Use Euler's theorem to show that for any $x \in \mathbb{Z}_p^\times$, $[x^{p-1}]_p = 1$, when p is prime.

That's Fermat's Little Theorem. When n is prime, $[x^{n-1}]_n = 1$, so when $[x^{n-1}]_n \neq 1$, n is composite.

The full statement of the theorem is:

If $[x^{n-1}]_n \neq 1$, then n is composite.

If $[x^{n-1}]_n = 1$, then n is *probably* prime.

Q 4.4.2: Use Fermat's little theorem to test 22, 65, 1027. Are these numbers prime?

Q 4.4.3: Use Fermat's little theorem to test 53, 101, and 1031. Are these numbers prime?

Q 4.4.4: Use Fermat's little theorem to test 561. Is 561 prime?

Numbers that past the test of Fermat's little theorem, but are not actually prime, are called "Carmichael numbers". 561 is the smallest. Carmichael numbers are pretty rare, so if Fermat's little theorem says that a number is prime, it *almost* always is. But not always.

Q 4.4.5: For any prime number p, and any two integers a, b, show that p divides $ab^{p-1} - a^{p-1}b$

Q 4.4.6: For any prime number $p > 7$, show that the number $1111\ldots111$ (which contains $p-1$ digits 1) is a multiple of p.

Q 4.4.7: (Difficult) Find an infinite non-constant arithmetic progression which contains no term that can be represented as the sum of two cubes.

Fermat's Little theorem is a special case of Euler, because it only works for prime moduli ($\mathbb{Z}_M$, when M is prime). When proving Euler we restricted our attention to $\mathbb{Z}_M^\times$, the set of numbers in $\mathbb{Z}_M$ that are coprime to M, and then looked at the product of the numbers in each row.

But if you're just given some number M, you may not be able to factor it, so you may not be able to figure out what's in $\mathbb{Z}_M^\times$.

Q 4.4.8: Excluding the zero row and column;

-what's the difference between the multiplication tables for $\mathbb{Z}_M^\times$ and $\mathbb{Z}_M$, when M is prime?

-what's the difference between the multiplication tables for $\mathbb{Z}_M^\times$ and $\mathbb{Z}_M$ when M is composite?

-when M is prime, what is the product of the numbers in each row?

-when M is composite, what is the product of the numbers in each row? Prove it.

Q 4.4.9: In order to be "fooled" by Fermat's Little theorem, $[x^{M-1}]_M = 1$, even though M is composite.

-Fermat sees composites automatically for some values of x. What does Fermat say if $gcd(x, M) \neq 1$? What does Fermat say if $gcd(x, M) = 1$?

-Looking at Euler's theorem, what can you say about M, if Fermat says M is prime, for every x that works?

-Does your answer work for the first two Carmichael numbers: $M = 561$ and $M = 1105$?