

X. Fermat and Euler on \mathbb{Z}_n

1 Fermat's Little Theorem

Theorem 1.1 : (Fermat's Little Theorem) Let p be prime. Then for any integer $a \in \mathbb{Z} - \{0\}$, either p divides a or else in \mathbb{Z}_p , $[a]^{p-1} = [1]$.

Proof: Suppose a is non-zero and is not divisible by p . Then in \mathbb{Z}_p we have $[a] \neq [0]$.

Because \mathbb{Z}_p is a field we know that the set $G := \{[1], [2], \dots, [p-1]\}$ is a multiplicative group with $p-1$ elements. Because $[a] \in G$ we know that $[a]^{p-1} = [1]$ as required. \square

Corollary 1.2 : Let p be a prime. For any $a \in \mathbb{Z}$, $a^p - a$ is divisible by p .

Proof: If a is not divisible by p then we already know that $[a]^{p-1} = [1]$ in \mathbb{Z}_p . Therefore $[a]^p = [a] * [1] = [a]$. And if a is divisible by p , then $[a] = [0]$ in \mathbb{Z}_p so that $[a]^p = [a]$. In any case, then $[a]^p = [a]$ so that $[0] = [a]^p - [a] = [a^p - a]$ and that is what we need in order to show that p must divide $a^p - a$. \square

2 Euler's Improvement

Consider any positive integer $n \geq 2$. We know that \mathbb{Z}_n is a commutative ring with identity and we know that if n is not prime, then \mathbb{Z}_n has non-zero zero-divisors. We need a preliminary result about the elements of \mathbb{Z}_n that are not zero-divisors.

Proposition 2.1 : Let $n \geq 2$ and let G_n be the set of all elements of $\mathbb{Z}_n - \{[0]\}$ that are not zero-divisors in \mathbb{Z}_n . Then G_n is a multiplicative group using the multiplication operation in \mathbb{Z}_n .

Proof: We must verify that $(G_n, *)$ is closed, has a multiplicative identity, and contains a multiplicative inverse of each of its elements.

Suppose $[a], [b] \in G_n$. Then neither $[a]$ nor $[b]$ is $[0]$ and neither is a zero-divisor in \mathbb{Z}_n . Therefore $[a] * [b] \neq [0]$. But could $[a] * [b]$ be a zero-divisor? Could there be some $[c] \in \mathbb{Z}_n - \{[0]\}$ with $([a] * [b]) * [c] = [0]$? If so, then $[0] = [a] * [bc]$. Because $[a]$ is not a zero-divisor, it must be true that $[0] = [bc] = [b] * [c]$. But because $[c] \neq [0]$ we are forced to conclude that $[b]$ is a zero-divisor, and that contradiction completes the proof that G_n is closed under $*$.

Is it true that $[1] \in G_n$? Yes, because if $[b] \neq [0]$ then $[1] * [b] = [b] \neq [0]$.

Is it true that if $[a] \in G_n$ then some $[b] \in G_n$ has $[a] * [b] = [1]$? Define a function $f : G_n \rightarrow \mathbb{Z}_n$ by the rule that $f([x]) = [a] * [x]$. We claim that f is 1-1. For suppose $f([x]) = f([y])$. Then $[a] * [x] = [a] * [y]$ so that $[0] = [a] * ([x] - [y])$. But $[a]$ is not a zero-divisor, so that we must have $[x] - [y] = [0]$, i.e., $[x] = [y]$. Also note that, because G_n is known to be closed under $*$, each $f([x])$ belongs to G_n so that $f[G_n] \subseteq G_n$. Therefore $f[G_n]$ is a subset of G_n with exactly as many elements as G_n , so that $f[G_n] = G_n$. In particular, because $[1] \in G_n$, some $[x] \in G_n$ must have $f([x]) = [1]$, i.e., $[a] * [x] = [1]$, and that $[x]$ is the multiplicative inverse of $[a]$ that we have been seeking. \square

Definition: Euler's phi-function is defined on the set of positive integers by the rule that $\phi(1) = 1$ and for $n \geq 2$, $\phi(n)$ is the number of integers in the list $1, 2, \dots, n$ that are relatively prime to n .

Therefore $\phi(2) = 1$, $\phi(3) = 2$, and $\phi(4) = 2$ because in the list $1, 2, 3, 4$ only 1 and 3 are relatively prime to 4 , and $\phi(5) = 4$.

Homework: Show that $\phi(n) = n - 1$ if and only if n is prime.

Lemma 2.2 : *With G_n as above, the order of G_n is $\phi(n)$.*

Proof: Let k be any positive integer that is less than n and relatively prime to n . We claim that $[k] \in G_n$. If not, then there is some non-zero $[b] \in \mathbb{Z}_n$ with $[k][b] = [0]$, i.e. having the property that kb is divisible by n . But $\gcd(k, n) = 1$ so that the only way for kb to be divisible by n is for n to divide b . But that makes $[b] = [0]$ in \mathbb{Z}_n and that is impossible. Therefore, $[k] \in G_n$ for each positive integer k that is less than or equal to n and relatively prime to n , and that shows that $\phi(n) \leq |G_n|$.

Next consider any integer m with $1 \leq m \leq n$ and $[m] \in G_n$. For contradiction, suppose that $\gcd(m, n) = d > 1$. Then there are integers i, j with $m = id$ and $n = jd$. Because $1 \leq j < n$ we see that in \mathbb{Z}_n , $[j] \neq [0]$. But $[j][m] = [jid] = [in] = [0]$ showing that $[m]$ is a zero-divisor in \mathbb{Z}_n and that is impossible because $[m] \in G_n$. Therefore, if $1 \leq m \leq n$ and $[m] \in G_n$, then $\gcd(m, n) = 1$ so that m is one of the integers counted when defining $\phi(n)$. Therefore $|G_n| \leq \phi(n)$. \square

Theorem 2.3 : *(Euler's Theorem) Suppose that $\gcd(a, n) = 1$. Then $a^{\phi(n)} - 1$ is divisible by n .*

Proof: It will be enough to show that if $\gcd(a, n) = 1$ then in \mathbb{Z}_n we have $[a]^{\phi(n)} = [1]$.

Let G_n be the group in the Proposition above. From the proof of the Lemma, we know that because $\gcd(a, n) = 1$, $[a] \in G_n$. Hence $[a]^{|G_n|} = [1]$. But $|G_n| = \phi(n)$ so we have $[a]^{\phi(n)} = [1]$ as required. \square

3 Solving first degree equations in the ring \mathbb{Z}_n

Consider \mathbb{Z}_6 . In that ring, the equation $[3] * [x] = [2]$ has no solution, as one can see by checking all possible values of $[x]$, but the equation $[5][x] = [b]$ has a solution for any given $[b]$, namely $[x] = [5b]$. The theorems above can be used to explain why.

Proposition 3.1 : *Let n be a positive integer and suppose $\gcd(a, n) = 1$. Then the equation $[a][x] = [b]$ can be solved for $[x]$ for every possible $[b] \in \mathbb{Z}_n$ in one and only one way.*

Proof: Because $\gcd(a, n) = 1$ we know that $[a] \in G_n$ where G_n is the group of all elements of \mathbb{Z}_n that are not zero-divisors. Then there is some $[c] \in \mathbb{Z}_n$ with $[a][c] = [1]$ and if we use $[x] = [c][b]$, we have $[a][x] = [a][c][b] = [1][b] = [b]$. Hence the equation $[a][x] = [b]$ has at least one solution in \mathbb{Z}_n . To see that there is only one solution of the equation, suppose that $[y] \in \mathbb{Z}_n$ and $[a][y] = [b]$. Then $[a][y] = [a][x]$ so that because $[a]$ is not a zero-divisor, cancellation applies and we get $[y] = [x]$. \square

Theorem 3.2 : Suppose n is a positive integer and let $a, b \in \mathbb{Z}$. Compute $d = \gcd(a, n)$. Then the following are equivalent:

- (i) the equation $[a][x] = [b]$ has at least one solution in \mathbb{Z}_n ;
- (ii) the number $d = \gcd(a, n)$ divides b ;
- (iii) the equation $[a][x] = [b]$ has exactly d many solutions in \mathbb{Z}_n .

Proof: Because (iii) clearly implies (i), it will be enough to show (i) implies (ii) and (ii) implies (iii).

(i) \Rightarrow (ii): Because $d = \gcd(a, n)$ we know that for some integers i, j , $a = id$ and $n = jd$. Because $[x]$ is a solution of $[a][x] = [b]$ we know that there is an integer k with $ax = b + kn$. In order to show that d divides b , apply the division algorithm to find integers q, r with $b = qd + r$, where $0 \leq r < d$. Our goal is to show that $r = 0$. For contradiction, suppose that $r > 0$. We substitute into the equation $ax = b + kn$ to get $idx = (qd + r) + kjd$ and rearrange to obtain $idx - qd - kjd = r$ which we factor as $d(ix - q - kj) = r$. But that is impossible because $0 < r < d$. This contradiction shows that $r = 0$ so that d divides b .

(ii) \Rightarrow (iii): In this part of the proof, we know that d divides b , where $d = \gcd(a, n)$, and we must show that the equation $[a][x] = [b]$ has exactly d different solutions in \mathbb{Z}_n . This will involve exhibiting d many solutions, and then showing that any solution must be one of those solutions.

In a moment, we will begin using equations in a different ring \mathbb{Z}_m to study equations in \mathbb{Z}_n . Consequently, we will begin putting subscripts on our equivalence classes to keep track of that fact that, for example, the equivalence class $[1]_m \in \mathbb{Z}_m$ is quite different from the equivalence class $[1]_n \in \mathbb{Z}_n$. Therefore, in this new notation, our goal is to show that the equation

$$(*) \quad [a]_n[x]_n = [b]_n$$

has exactly d many solutions in \mathbb{Z}_n .

Because $d = \gcd(a, n)$ we know that there are integers i, j with $a = id$ and $n = jd$, and furthermore that $\frac{a}{d} = i$ and $\frac{n}{d} = j$ are relatively prime integers. Write $m = \frac{n}{d}$. Then according to the previous proposition, the equation

$$(**) \quad \left[\frac{a}{d} \right]_m [x]_m = \left[\frac{b}{d} \right]_m$$

has exactly one solution. Choose the unique integer x with $0 \leq x < m = \frac{n}{d}$ that satisfies equation (**) and consider the list of integers $x, x + \frac{n}{d}, x + \frac{2n}{d}, x + \frac{3n}{d}, \dots, x + \frac{(d-1)n}{d}$. There are exactly d many entries in that list, and each of them lies between 0 and $\frac{dn}{d} = n$. Consequently, there are exactly d many distinct equivalence classes $[x + \frac{kn}{d}]_n$ in \mathbb{Z}_n .

First we show that any $[y]_n = [x + \frac{nk}{d}]_n$ will have $[a]_n[y]_n = [b]_n$. Because x solves equation (**) we know that $\frac{a}{d} * x = \frac{b}{d} + t\frac{n}{d}$ for some integer t . Multiply by d to get $ax = b + tn$. Then note that

$$a * \left(x + \frac{nk}{d} \right) = ax + a * \frac{nk}{d} = b + tn + (di) * \frac{nk}{d} = b + tn + ink$$

and therefore $[a]_n * [x + \frac{nk}{d}]_n = [b]_n$. It follows that we have at least d many solutions of our equation (*) in \mathbb{Z}_n .

Finally we show that any solution of the equation (*) in \mathbb{Z}_n must belong to the list above. Any solution of (*) has an alias lying between 0 and $n - 1$ and so we may assume that $0 \leq z < n$. Because $[z]_n$ solves equation (*), we know that

$$(***) \quad az = b + vn$$

for some integer v . Recall that a, n and b are each divisible by d , so that each of $\frac{a}{d}$, $\frac{n}{d}$ and $\frac{b}{d}$ is an integer. Therefore when we divide through equation (***) by d we get an equation $\frac{a}{d} * z = \frac{b}{d} + v\frac{n}{d}$. Recalling that $\frac{n}{d} = m$ we see that z must be a solution of equation (**) in \mathbb{Z}_m . But we already know that the unique solution of that equation in \mathbb{Z}_m is $[x]_m$. Therefore we must have $[z]_m = [x]_m$ and hence $z = x + wm = x + w\frac{n}{d}$ for some integer w . But then $[z]_n = [x + \frac{kn}{d}]_n$ already appears in our list of d many solutions. Hence our list of d many solutions contains every solution. \square

The previous theorem shows how much of a contrast exists between rings in general and the field of rational (or real) numbers. In the latter, every first degree equation has exactly one solution. In arbitrary rings, some first degree equations can have no solutions, while others have multiple solutions.