A modo de introducción: El pequeño teorema de Fermat

16.01.2023

Introducción

Bienvenidos a álgebra I. Yo soy Pablo Zadunaisky y voy a ser su profesor. Preferiría que me digan Pablo y me traten de vos, si les parece bien. Yo voy a estar a cargo de las clases teóricas de la materia, que van a ser en este aúla (el aúla 2 del pabellón 1), los martes y viernes de 14 a 16.

- Preguntar quiénes están estudiando la licenciatura en matemática, el profesorado, la licenciatura en computación, la licenciatura en ciencia de datos, alguna otra cosa.
- Preguntar para quiénes es la primera materia universitaria de la vida (sin contar el CBC u otras materias que hayan empezado ayer), quiénes ya cursaron alguna otra cosa, quiénes vienen de otras carreras.
- Preguntar quiénes van a una práctica por la mañana y quiénes van a la de la tarde. De paso preguntar quiénes saben cuál es la diferencia entre una teórica y una práctica.
- Preguntar quiénes saben dividir 1345 por 83.

Hablemos un poco sobre la materia. Esta es una materia que trata más bien sobre números ***enteros*** y números ***naturales***. Es más, trata sobre un montón de cosas que ya conocen, como contar, y sumar, y multiplicar y por sobre todas las cosas *dividir*. Eso quiere decir que ya tienen la mitad de la materia hecha. Felicitaciones, se suspenden las clases, los veo en el exámen final.

Más en serio, en la primera parte de la materia vamos a estudiar principalmente propiedades de dos familias de números:

$$\mathbb{N} = \{\text{pedir ejemplos y no ejemplos}\}$$
$$\mathbb{Z} = \{\text{pedir ejemplos y no ejemplos}\}.$$

La mayor parte de las cosas que vamos a ver ya se conocían a principios del siglo *XIX*, y casi que podríamos usar como libro de la materia las *Disquisitiones Arithmeticae* que escribió Gauss (recuerden el nombre) en 1798. Es todo muy accesible, tanto que podría ser un tema de matemática para fines del primario.

Hablando del primario, otro concepto super importante que vamos a estudiar es el de números primos. ¿Quién sabe lo que es un

número primo? (chistes sobre familiares son motivo de expulsión de la universidad).

anotar algunos ejemplos

¿Ven lo que hice acá? Escribí por separado una definición importante y resalté qué es lo que estoy definiendo.

Definición (Provisoria)**.** Un ***número primo*** es un número natural que solo es divisible por sí mismo y por 1.

¿Por qué estudiamos matemática tan antigua y tan básica? Porque es muy útil, porque es muy divertida, y porque es la base de un montón de cosas más recientes, pero por sobre todas las cosas porque nos permite aprender una nueva forma de hacer matemáticas, una en la que no solo aprendemos resultados (a los matemáticos les gusta decirles "teoremas") sino por qué esos resultado son ciertos.

Por ejemplo, ¿alguien sabe la regla de divisibilidad por 3? ¿cómo saber si el número 12984 es divisible por 3 sin hacer la cuenta? Bueno, si sumo los dígitos obtengo $1 + 2 + 9 + 8 + 4 = 24$, y si los sumo otra vez obtengo $2 + 4 = 6$ que es divisible por 3, y eso quiere decir que 12984 es divisible por 3. En cambio 12985 *no* es divisible por 3 porque el resultado final de esa cuenta es 7 y 7 no es divisible por 3.

¿Por qué? ¿qué tiene que ver la suma de los dígitos con dividir por 3? Y ya que estamos, ¿hay reglas parecidas para el 2, para el 11 o para el 113? Quizás las hay, quizás las conozcan. En esta materia vamos a aprender por qué funcionan esas reglas, cómo descubrir reglas nuevas, y por sobre todas las cosas, por qué el bendito algoritmo de división funciona. Cuando terminemos esta materia nunca más se van a olvidar del algoritmo de división, ni van a necesitar saberlo de memoria: van a saber por qué ese algoritmo funciona (y por qué la mejor forma de dividir 1345 por 83 es usando una calculadora).

El pequeño teorema de Fermat

En una carta del 18 de octubre de 1640, Pierre de Fermat le dijo a su amigo Frénicle de Bessy que había descubierto el siguiente hecho.

Los matemáticos le dicen ***teorema*** a los resultados que consideran más importantes o interesantes. Nos gusta usar el imperativo impersonal del verbo "ser" como una forma breve de decir "considero cosas con estas propiedades, y no voy a suponer ninguna otra, y les voy a poner este nombre para poder hablar de ellos con más comodidad". También nos gusta usar símbolos como $\in$ y $|$, y es importante usarlos pero no abusar.

Teorema. *Sean $a \in \mathbb{Z}$ y $p \in \mathbb{N}$ con p primo. Entonces $p \mid a^p - a$.*

Este resultado se conoce es el *pequeño teorema de Fermat* (para distinguirlo del más famoso y popular último teorema de Fermat). Esta es la clase de resultado que vamos a estudiar en esta materia, al menos en su primera parte. La forma medio rara en que está presentado esto es la forma que tienen les matemátiques de decir que no importa qué número elijamos para jugar el rol de a o p, siempre que a sea entero y p sea primo. Por ejemplo

- Si $a = 5$ y $p = 3$ entonces $a^p - a = 5^3 - 5 = 125 - 5 = 120$, que es divisble por 3 porque $120/3 = 40$.
- Si $a = 7$ y $p = 2$ entonces $a^p - a = 7^2 - 7 = 49 - 7 = 42$, que claramente es par así que es divisible por 2.
- Si $a = 0$ y $p = 5$ entonces $a^p - a = 0^5 - 0 = 0$, que es divisible por 5... ¿no?
- Si $a = -3$ y $p = 7$ entonces $a^p - a = -2187 + 3 = -2184$, que mágicamente es divisible por 7 porque $-2184 = -312 \cdot 7$.
- Si $a = 3$ y $p = 4$ entonces $a^p - a = 81 - 3 = 78$ que no es divisible por 4, pero a nadie le importa porque p no es primo.

Una versión menos resumida, menos compacta y más explícita del teorema es la siguiente.

TEOREMA. *~~Sean~~ Supongamos que ~~$a \in \mathbb{Z}$~~ tenemos un número entero cualquiera a y ~~$p \in \mathbb{N}$ con p primo~~ un entero positivo primo p. Entonces ~~$p \mid a^p - a$~~ el número $a^p - a$ es divisible por p.*

Hay que elegir un balance entre cuán explícito y cuán resumido es un enunciado. Si me preguntan por qué no simplemente escribir este segundo enunciado, les comento que Fermat originalmente escribió una versión más explícita aún.

TEOREMA. *Todo número primo mide una de las potencias menos uno de cualquier progresión en la que el exponente es un múltiplo del primo dado menos uno. (...) Y esta proposición es generalmente cierta para todas las progresiones y todos los números primos.*

Después de un par de años de estudiar matemática, la primera versión es tanto mejor que la segunda como la segunda de la tercera.

Demostrando el teorema

La estrategia

Veamos una demostración del pequeño teorema de Fermat. La idea de la demostración va a ser la siguiente. Vamos a comenzar suponiendo que conocemos los números a y p (a natural, p primo)

- Vamos a encontrar un ***conjunto*** con $a^p - a$ ***elementos***.
- Vamos a probar que podemos dividir esos elementos en grupos de p elementos cada uno.

Con estos dos resultados, podemos hacer el siguiente razonamiento: si tenemos n grupos con p elementos, sabemos que el total de elementos en nuestro conjunto es np; como además el conjunto tenía

$a^p - a$ elementos, sabemos que $a^p - a = np$, es decir que p divide a $a^p - a$. Antes de seguir, asegúrense de que este argumento los convence. El resto es coser y cantar.

El conjunto

Imaginemos que tenemos una colección de perlas. Tenemos muchas perlas de distintos colores, de hecho tenemos en total a colores (si los deja tranquilos, piensen por ahora que a es 2 o 3). Podemos armar cadenas de perlas, y de hecho vamos a pensar en cadenas que tengan p perlas. ¿Cuántas cadenas distintas podemos formar? Cada una de las p perlas puede elegirse de a colores distintos, así que tenemos a posibilidades para la primera, a posibilidades para la segunda, y así, hasta la p-ésima, es decir, tenemos a^p cadenas posibles.

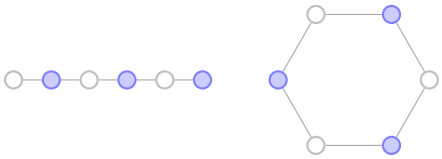
Ahora, entre esas cadenas hay a cadenas cuyas perlas son todas del mismo color. Por ejemplo, si mis perlas son azules, blancas y grises (o sea, $a = 3$), hay una cadena con perlas todas azules, una cadena con perlas todas blancas, y una cadena con perlas todas grises; es decir, tres cadenas formadas por perlas del mismo color. Todas las otras cadenas tienen al menos dos perlas de colores distintos, y de esas hay exactamente $a^p - a$.

> Llamamos C al conjunto de cadenas de p perlas con al menos dos perlas de distinto color.

Y ese es nuestro conjunto.

La división

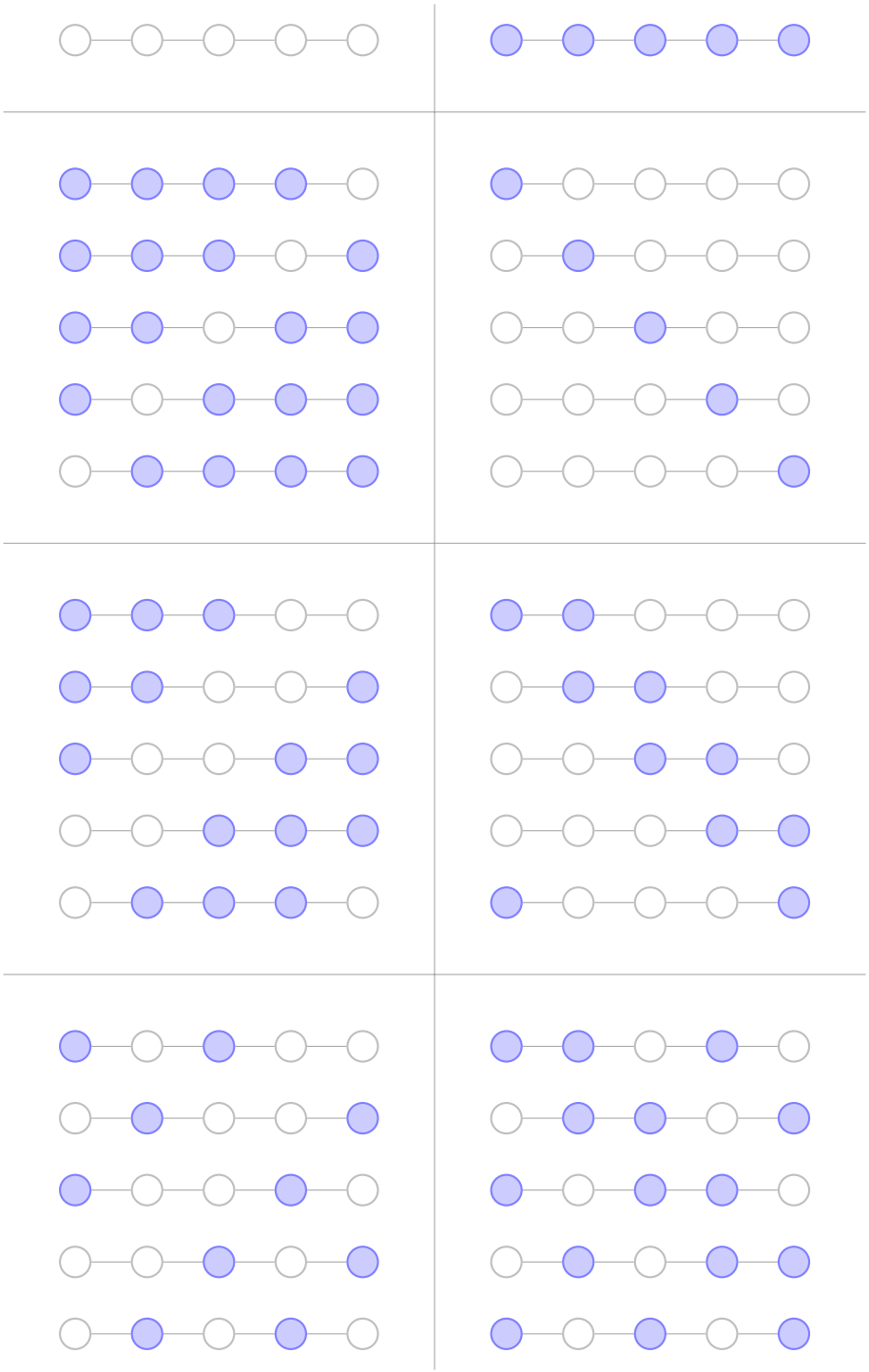
Si nos dan una cadena, podemos formar un collar cerrándola, como en el dibujo.



Las cadenas amigas son un ejemplo de ***clase de equivalencia***, otra idea que vamos a ver varias veces en la materia.

Digamos que dos cadenas de nuestro conjunto C son ***amigas*** si al cerrarlas obtenemos el mismo collar, y agrupamos las cadenas según si son amigas o no. Esto divide el conjunto C en varios ***subconjuntos***. Ahora digo que si tenemos muchas cajas, y vamos separando las cadenas según si son amigas o no, eventualmente cada caja que use va a tener p cadenas. Si las cadenas de C ocupan n cajas, cada una con p cadenas, $a^p - a = np$.

Ejemplo. Por ejemplo en la imagen de abajo vemos los subconjuntos de cadenas amigas cuando $a = 2$ y $p = 5$. Tenemos entonces 32 cadenas (incluyendo las que quedaron afuera de C, que aparecen en la primera fila del dibujo).



La tabla está organizada de forma que dos cadenas están en el mismo casillero si y solo si se cierran para formar el mismo collar. Si excluimos las $a = 2$ cadenas que no están en C, nos quedan $a^p - a = 2^5 - 2 = 30$ cadenas que forman collares que vienen de cadenas de C. Ahora notamos que cada celda restante contiene $p = 5$ cadenas, es decir, cada collar proviene de cerrar p cadenas distintas. Esto dice que hay $(a^p - a)/p = 30/5 = 6$ collares distintos con al menos dos colores de perlas. Esta es una manera bastante complicada de probar que 30 es divisible por 5, pero la gracia es que, como vamos a ver pronto, este mismo argumento funciona siempre que a sea un número entero y p un número primo.

Ejemplo. Puede ocurrir que una cadena tenga menos de p amigas. Por ejemplo, una cadena donde todas las perlas son del mismo color tiene una sola amiga: sí misma. Hay casos más sutiles. Por ejemplo, la cadena  tiene dos amigas: sí misma y  . La cadena  tiene *tres* amigas: sí misma,  y  . Lo que *nunca* ocurre es que una cadena de seis perlas tenga cuatro o cinco amigas.

Ahora sí estamos listos para probar que todo collar proviene de exactamente p cadenas.

Los matemáticos llaman *lema* a observaciones interesantes o útiles que aparecen en el camino de la prueba de un resultado más importante

LEMA. *Cada collar con al menos dos perlas de distinto color proviene de cerrar exactamente p cadenas distintas.*

Demostración. Si tengo una cadena y formo el collar correspondiente, puedo recuperar la cadena cortando el collar en un punto entre dos perlas. Así, si dos cadenas son amigas entonces ambas aparecen cortando el mismo collar en distintos puntos. Esto muestra que cada cadena tiene a lo sumo p amigas.

Digamos que la distancia entre dos puntos de corte es el número de perlas entre ambos puntos, yendo por el camino más corto. Tomemos un collar cualquiera, y estudiemos las p cadenas distintas que se obtienen de cortarlo en los p puntos posibles. Si no hay repeticiones, este collar efectivamente proviene de p cadenas distintas. Si obtenemos repeticiones hacemos lo siguiente: armamos la lista completa de todos los pares de puntos (P, Q) distintos tales que al cortar en P obtenemos la misma cadena que al cortar en Q. Ahora elijamos un par que (P, Q) que esté a la menor distancia posible, digamos d.

- (P, Q) es un par de puntos de corte que producen la misma cadena y están lo más cerca posible
- d es la distancia mínima entre dos puntos de corte que producen la misma cadena.

Como al cortar en P y en Q obtenemos la misma cadena, la primera perla que viene después de P cuando avanzamos en dirección a Q por el camino más corto es igual a la primera perla que viene después de Q, es decir, la perla que está d pasos más adelante. Lo mismo vale para la segunda, la tercera, y así hasta la p-ésima. Eso dice en particular que los colores de las perlas se deben ir repitiendo cada d pasos.

Los colores de las perlas se repiten cada d pasos. Esto no es obvio de la definición de d

Ahora, los d cortes entre P (incluido) y Q (excluido) producen cadenas distintas, porque están a distancia menor a d. Por otro lado, como el patrón de colores del collar se repite cada d pasos, no obtenemos cadenas distintas al hacer nuevos cortes, así que d es también el número de cadenas distintas que se obtienen cortando el collar.

d es el número de cadenas distintas que se obtienen cortando el collar. Esto es menos obvio aún

Partiendo desde P avancemos d pasos, $2d$ pasos, $3d$ pasos, etc., finalmente llegamos a un corte en la posición kd, donde kd difiere de p en menos que d. En otras palabras, llegamos a un corte que está a distancia menor a d de nuestro corte inicial P, y que produce la misma cadena que P. Pero si dos cortes distintos producen la misma cadena, entonces deben estar a distancia mayor o igual a d, así que esto es solo posible si el nuevo corte coincide con P, o en otras palabras, $p = kd$. Esto no es posible, porque p es un número primo y no puede escribirse como el producto de dos números más pequeños. □

Avanzando de a d perlas en el collar, finalmente debemos volver al punto de corte P, pero para volver al mismo punto en el collar tenemos que avanzar p perlas. Así p es un múltiplo de d

Volviendo al pequeño teorema de Fermat, tenemos $a^p - a$ cadenas con al menos dos colores distintos. El lema que acabamos de demostrar dice que si separamos estas cadenas en grupos de amigas, es decir en grupos de cadenas que se cierran en el mismo collar, cada grupo tendrá p cadenas. Notar que hay tantos grupos como collares, así que si el número de collares distintos que obtenemos es n, tenemos que $pn = a^p - a$, y en particular p divide a $a^p - a$.□

En la clase alguien preguntó que ocurre si p no es primo, sino un número cualquiera. En ese caso nuestro razonamiento funciona exactamente igual, pero la conclusión es que nuestro collar proviene de d cadenas distintas y que $p = kd$, es decir que en general d debe dividir a p; en el caso en que p es primo, sus únicos divisores son 1 y p, y por lo tanto $d = 1$ o $d = p$. El caso $d = 1$ corresponde a los collares con perlas de un solo color y queda descartado, por eso tenemos $d = p$.

Volviendo al principio...

Como les dije, esta materia se va a tratar de las propiedades de los números enteros, como el teorema que acabamos de demostrar. El objetivo de la materia no es solamente que conozcan estas propiedades, ni conocer sus demostraciones, sino que ustedes sean capaces de descubrir propiedades por su cuenta y dar sus propias demostraciones.

¿Cómo descubre uno propiedades de los números? No hay una receta, la mejor forma es: hacer una prueba, adivinar, hacer más pruebas, adivinar, hace más pruebas... es más facil de lo que uno cree. Y en todo caso, ustedes ya conocen un montón de cosas sobre

los números naturales: está la regla de divisibilidad por 3, y también saben que todos se escriben como producto de números primos, y también saben que no hay un número natural más grande... si no se les ocurre nada, hay una guía de ejercicios con muchas propiedades interesantes para probar.

El verdadero problema es, ¿cómo aprender a demostrar cosas? La prueba esta de contar collares es muy bonita y, con el tiempo, debería resultarles muy clara, pero ¿a quién se le ocurre contar collares para demostrar teoremas? Aunque esta prueba es "elemental" (no usamos integrales de funciones trigonométricas ni espacios vectoriales de polinomios, solamente contamos "de manera inteligente"), es la más complicada que conozco en el sentido de que es muy dificil explicar cómo se nos puede ocurrir esta demostración. Más adelante vamos a ver dos demostraciones un poco menos "brillantes" y más accesibles.

El programa de la materia

Hablemos sobre el programa de esta primera parte de la materia.

1. **Conjuntos y funciones:** En esta primera parte vamos a aprender un poco de lenguaje novedoso. Vamos a hablar de conjuntos (como el conjunto de todas las cadenas, y todos los collares), subconjuntos (como el de las cadenas con perlas de un solo color) y funciones (como la que asigna a cada cadena el collar correspondiente). Vamos a hablar de operaciones como uniones, intersecciones, diferencias (como la de sacar de entre todas las cadenas las que tienen un solo color). Vamos a ver que la idea de "separar cadenas en amigas" es un ejemplo de *relación de equivalencia*, que es de lo más nuevo que vamos a ver acá.
2. **Números naturales e inducción:** Acá arranca de verdad la materia. Usando solo ideas sobre conjuntos, y partiendo de unas pocas propiedades básicas, vamos a ir demostrando un montón de cosas que ya sabíamos sobre los números naturales, pero que no sabíamos por qué son ciertas. Vamos a hablar de un método de demostración, llamado inducción; a partir de este punto, cada vez que querramos demostrar algo, siempre podemos al menos intentar demostrarlo por inducción.
3. **Combinatoria:** ¿Vieron eso de "contar de manera inteligente"? Es muy complicado, tanto que hay toda una rama de la matemática dedicada a ello llamada combinatoria. Contar en este caso es contar los elementos de un conjunto (el ***cardinal*** del conjunto), y vamos a ver cómo las operaciones de conjuntos se relacionan con las cardinalidades. Ejemplo: si X es un conjunto con n elementos, ¿cuántos subconjuntos distintos tiene?

4. **Números enteros:** Vamos a darle a los números enteros el mismo tratamiento que le dimos a los naturales. Vamos a estudiar varias propiedades usando las herramientas anteriores (inducción, relaciones de equivalencia...). Principalmente vamos a estudiar problemas de divisibilidad, y cómo resolver ecuaciones con números enteros.

¿Vieron eso de "contar de manera inteligente"? Bueno, es toda un área de la matemática llamada combinatoria. Vamos a ver que muchos números conocidos "cuentan" elementos de conjuntos. Esta idea va a estar dando vuelta todo el tiempo en la materia.

Para terminar

Esta fue una clase muy particular. Primero, les hablé de un montón de cosas en una sola clase. Vamos a empezar con un ritmo más tranquilo, y con cosas más básicas. Igual vamos a ir tomando ritmo, y dentro de un par de meses vamos a saber un montón de cosas, tantas que vamos a liquidar el pequeño teorema de Fermat en diez minutos de clase.

Otro motivo por el que la clase de hoy se hizo larga es porque me detuve mucho en los detalles de la demostración, leí y releí el enunciado hasta que fue entendible, armé el esquema de la demostración con cuidado, les mostré cómo releer la demostración, sintetizando qué conseguimos después de cada paso... ese trabajo lo voy a ir haciendo cada vez menos, y cada vez más les va a tocar a ustedes. Es tarea de ustedes aprender a traducir los enunciados a algo que entiendan, y también ir párrafo por párrafo, línea por línea, para entender cómo funciona una demostración. A veces lo van a hacer todo automáticamente (cada vez más, y más rápido), pero nadie espera que lo puedan hacer ya ya ya.

Algunes por ahí tienen más práctica y les sale facil, otres por ahí menos pero les sale, y a otres les cuesta más. Nunca duden en venir a preguntarme, o en hablar con la gente de práctica, acerca de algo que no entiendan. Y sean pacientes, con sus compañeros cuando expresan alguna duda y por sobre todas las cosas con ustedes mismos cuando no entienden algo. Aprender matemáticas es dificil y cada uno tiene que encontrarle la vuelta (si no no necesitaríamos seis años de carrera...), pero es mucho más facil (y más agradable) si uno sabe que tiene gente con la que hablar. Yo y les otres profes vamos a tratar de ser esa gente, y estaría bueno que ustedes también lo sean entre ustedes. No importa si son el primero, el segundo o el último ser humano en entender la demostración del pequeño teorema de Fermat, cuando uno *entiende*, y lo puede contar, la sensación es maravillosa.