Tarea II: Números Primos
Teoría de los números I
Fecha de entrega: martes, 19/feb/2019

Los números entre los paréntesis denota el puntaje de ese ejercicio. Hay un total de 30 puntos.

Ejercicio 1. (2) Prueba que para todo $n > 1$, el conjunto $\{n, n+1, n+2, \ldots, n!\}$ contiene al menos un número primo. Usa este resultado para dar otra prueba de la infinitud de los números primos.

Ejercicio 2. (1) La *conjetura de Goldbach* dice que todo número par mayor que 2 se puede expresar como la suma de dos números primos. La conjetura débil de Goldbach dice que todo número impar mayor que 5 es puede expresar como la suma de tres números primos. Prueba que la conjetura de Goldbach implica la conjetura débil (esto explica el nombre). En 2013, el matemático peruano Harald Helfgott probó que la conjetura de Goldbach débil era cierta. La otra conjetura sigue sin resolverse.

Ejercicio 3. (5) Los primos de Mersenne y los números de Fermat

1. (1) Sea $a \in \mathbb{Z}$. Prueba que si $a^n - 1$ es primo, entonces $a = 2$ y n es primo. A los números primos de la forma $2^p - 1$, con p primo, se les llaman *primos de Mersenne*. Ojo, no todos los números de la forma $2^p - 1$ son primos: Exhibe dos primos p y q tales que $2^p - 1$ y $2^q - 1$ sean compuestos ¿Cuál es el primo de Mersenne más grande que se conoce?

2. (1) Prueba que si $a^n + 1$ es primo, entonces a es par y $n = 2^m$ para alguna $m > 0$. Fermat propuso que los números de la forma $F_n := 2^{2^n} + 1$ eran todos primos, pero esto es falso (da un ejemplo).

3. (1) Prueba que para toda $n > 0$, se cumple la siguiente identidad

$$F_n - 2 = \prod_{k=0}^{n-1} F_k.$$

4. (2) Prueba que para toda $n \neq m$, entonces $(F_n, F_m) = 1$. Usa este resultado para probar que hay una infinidad de números primos. Nota que esta prueba no es por contradicción.

Ejercicio 4. (2) Prueba que 509 no es de la forma $p^n + 2^m$ donde p es primo y $n, m > 0$.

Ejercicio 5. (5) La irracionalidad de $\sqrt[n]{m}$ en el caso no trivial.

1. (1) Sea $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ la factorización única de a en primos. Prueba que a es un cuadrado si y solamente si $2 \mid \alpha_i$ para toda $i = 1, \ldots, s$.

2. (2) Sean $a, b \in \mathbb{Z}$ primos relativos. Pueba que si $ab = n^2$ para alguna n, entonces $a = m_1^2$ y $b = m_2^2$ son cuadrados también. Con esto prueba que $\sqrt{2}$ es irracional.

3. (1) Generaliza los dos inciso anteriores pero para cualquier potencia k (los incisos anteriores son el caso $k = 2$).

4. (1) Con lo anterior prueba que si m no es una n-ésima potencia, entonces $\sqrt[n]{m}$ es irracional.

Ejercicio 6. (3) Propiedades de números compuestos.

1. (1) Prueba que todo entero $n > 11$ es suma de dos números compuestos.

Tarea II: Números Primos
Teoría de los números I
Fecha de entrega: martes, 19/feb/2019

2. (1) Demuestra que $n^3 + 1$ es compuesto para toda $n > 1$.

3. (1) Prueba que para todo $n > 1$, existen n números compuestos consecutivos. En otras palabras, hay intervalos arbitrariamente grandes donde no aparece un solo primo.

Ejercicio 7. (9) La valoración p-ádica. Fija un número primo p y considera la siguiente función:

$$\mathrm{ord}_p : \mathbb{Z} - \{0\} \longrightarrow \mathbb{Z} \quad \text{definido por} \quad \mathrm{ord}_p(n) = \max\{k \in \mathbb{N} \mid p^k \mid n\},$$

es decir que $\mathrm{ord}_p(n)$ es el exponente de p en la factorización única de n. Ahora fija $a, b \neq 0$ y prueba que:

1. (2) $\mathrm{ord}(ab) = \mathrm{ord}(a) + \mathrm{ord}(b)$ y $\mathrm{ord}_p(a+b) \geq \min\{\mathrm{ord}_p(v), \mathrm{ord}_p(b)\}$. [1]

2. (1) $\mathrm{ord}_p\big((a,b)\big) = \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$

3. (1) $\mathrm{ord}_p\big([a,b]\big) = \max\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$

4. (2) Sea $r \in \mathbb{Q}$ arbitrario y define $[r] = \max\{k \in \mathbb{Z} \mid k \leq r\}$. Si $n > 0$, prueba que

$$\mathrm{ord}_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

5. (3) Con el inciso anterior prueba que $\mathrm{ord}_p(n!) \leq \frac{n}{p-1}$ y que

$$\sqrt[n]{n!} \leq \prod_{p \mid n!} p^{\frac{1}{p-1}},$$

después usa esta desigualdad para dar una prueba de que hay una infinidad de primos.

Ejercicio 8. (3) La irracionalidad de $\log_p n$ (fijamos un número primo p).

1. (1) Prueba que si $\log_p n \in \mathbb{Q}$ para alguna $n \in \mathbb{N}$, entonces $p \mid n$.

2. (1) Denota $e = \mathrm{ord}_p(n)$. Prueba que

$$\log_p n \in \mathbb{Q} \quad \Longleftrightarrow \quad \log_p\left(\frac{n}{p^e}\right) \in \mathbb{Q}$$

3. (1) Prueba que si n no es una potencia de p (ie. $n \neq p^k$ para toda $k \geq 1$) entonces $\log_p n$ es irracional.

[1] A una función $\nu : A - \{0\} \to \mathbb{Z}$ que cumple (a) y (b) se le llama *valoración* del anillo A y al caso particular ord_p, se llama la *valoración p-ádica* de $\mathbb{Z}$.