Capítulo 5: Teoría de Números
Clase 1: Primalidad

Matemática Discreta - CC3101
Profesor: Pablo Barceló

Teoría de números

En esta parte del curso hablaremos sobre las propiedades de los enteros, que es un área que llamamos teoría de números.

Gauss la llamó la reina de matemáticas.

Ha sido estudiada por más de 2500 años.

Es una de las áreas más difíciles de las matemáticas y se haya llena de problemas abiertos y conjeturas muy importantes.

Primos

Un número $p > 1$ es primo si no puede ser escrito como el producto de dos enteros menores que p. Si p no es primo se dice que es compuesto.

Primos

Un número $p > 1$ es primo si no puede ser escrito como el producto de dos enteros menores que p. Si p no es primo se dice que es compuesto.

La estructura de los primos es altamente irregular: Contiene hoyos y lugares muy densos. Algunas preguntas se generan naturalmente:

- ¿Es cierto que para cada n existe un primo con n dígitos?
- ¿Es cierto que para cada n existen n números consecutivos que no son primos?

Teorema fundamental de la aritmética

Ejercicio: Todo entero positivo puede ser escrito como el producto de primos.

Teorema fundamental de la aritmética

Ejercicio: Todo entero positivo puede ser escrito como el producto de primos.

Sorprendentemente, la descomposición en primos de un número es única. Este es el Teorema fundamental de la aritmética.

Teorema

Todo entero positivo puede ser escrito como el producto de primos, y esta factorización es única (bajo reorden de los factores).

A continuación demostraremos este teorema.

Demostración

Asuma, por contradicción, que el teorema es falso.

Sea n el menor entero positivo con dos factorizaciones distintas en números primos, i.e.

- $n = p_1 p_2 \cdot \cdots \cdot p_m$;
- $n = q_1 q_2 \cdot \cdots \cdot q_k$.

Sin pérdida de generalidad, asumimos que p_1 es el primo más pequeño que aparece en estas factorizaciones.

Demostración

Entonces para todo $i \in [1, k]$, $p_1 \neq q_i$, porque sino n no sería el menor entero con dos factorizaciones distintas.

Dividamos cada q_i por p_1, y asumamos que $q_i = p_1 a_i + r_i$, donde $0 < r_i < p_1$.

Considere el número $n' = r_1 r_2 \cdot \cdots \cdot r_k$.

Sabemos que para todo $i \in [1, k]$, $r_i < p_1 < q_i$. Por tanto, $n' < n$.

Demostraremos a continuación que n' tiene dos factorizaciones primas distintas, lo que es una contradicción.

La primera es cualquier factorización prima obtenida desde $n' = r_1 r_2 \cdot \cdots \cdot r_k$.

Demostración

Note que

$$n' = (q_1 - a_1 p_1)(q_2 - a_2 p_1) \cdot \cdots \cdot (q_k - a_k p_1).$$

Al expandir esto notamos que cada factor es divisible por p_1, y por tanto, n' es divisible por p_1.

Dividimos a n' por p_1, y continuamos de esta forma hasta obtener una factorización en primos de n'.

Estas factorizaciones son distintas porque cada uno de los factores r_i es estricamente menor que p_1.

Hemos obtenido la contradicción deseada, y terminado la demostración del teorema.

Ejercicio

Utilice el teorema fundamental de la aritmética para demostrar lo siguiente:

Ejercicio: Si p es un primo entonces $\sqrt{p}$ es irracional.

Infinitud de los primos

Demostraremos el siguiente teorema:

Teorema

El conjunto de los números primos es infinito.

Infinitud de los primos

Demostraremos el siguiente teorema:

Teorema

El conjunto de los números primos es infinito.

Asuma, por contradicción, que el conjunto de primos son finitos y que estos son $p_1 < p_2 < \cdots < p_k$.

Considere el número $q = p_k! + 1$.

Por el teorema fundamental de la aritmética q tiene una factorización $r_1 r_2 \cdot \cdots \cdot r_m$ en números primos.

Demostraremos que cada $r_i > p_k$.

Asuma, por contradicción, que $r_i \leq p_k$. Entonces r_i divide a $p_k!$ y a $p_k! + 1$. Luego, p_k divide a 1, lo que es una contradicción.

Ejercicio

Utilice un argumento similar para realizar el siguiente ejercicio:

Ejercicio: Para cualquier entero positivo n, existen n enteros no primos consecutivos.

Ejercicio

Utilice un argumento similar para realizar el siguiente ejercicio:

Ejercicio: Para cualquier entero positivo n, existen n enteros no primos consecutivos.

Nos hacemos la pregunta inversa. Dos primos p y p' son gemelos si $p' = p + 2$.

Pregunta: ¿Existe un número infinito de pares de primos gemelos?

Esta es una de las preguntas abiertas más importantes en el área de teoría de números.

Teorema de números primos

¿Cuántos primos menores que n hay? Nadie tiene la respuesta a esto. Pero sí conocemos una aproximación.

Teorema

Sea $\pi(n)$ el número de primos menores o iguales a n, para $n \geq 1$. Entonces,

$$\lim_{n \to \infty} \pi(n) = (n / \ln n).$$

Conjeturas sobre primos

Conjetura de Goldbach: Todo entero par es equivalente a la suma de dos primos.

Otra conjetura: ¿Es cierto que siempre existe un primo entre n^2 y $(n+1)^2$?

Pequeño teorema de Fermat

Los chinos creían que:

$$p \text{ es primo si y solo si } 2^{p-1} \equiv 1 \pmod{p}.$$

Fermat logró demostrar una de estas implicancias (de hecho, una versión más fuerte). Este se conoce como el pequeño teorema de Fermat.

Teorema

Si p es primo entonces para todo entero a,

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

Demostración

Lemma

$a^{p-1} \equiv 1 \pmod{p}$ *si y solo si* $a^p \equiv a \pmod{p}$.

Usando el lemma, será suficiente demostrar que si p es primo entonces $a^p \equiv a \pmod{p}$.

Demostraremos esto por inducción en a.

El caso base es $a = 1$, que es trivial.

Sea entonces, para el caso inductivo, $a > 1$ y $a = b + 1$.

Luego, $a^p - a = (b+1)^p - (b+1)$.

Demostración

Pero esto último es equivalente a:

$$b^p + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b + 1 - (b+1).$$

Resolviendo obtenemos que esto es igual a:

$$(b^p - b) + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b.$$

Pero cada uno de estos es divisible por p (¿por qué?), lo que termina la demostración.

La otra dirección

La otra dirección de la conjetura china es falsa:

- $341 = 11 \cdot 31$ no es primo;
- sin embargo, $2^{340} \equiv 1 \pmod{341}$.

Los números p que satisfacen $2^{p-1} \equiv 1 \pmod{p}$, pero no son primos, se llaman seudoprimos.

Ejercicios finales

Ejercicio: Demuestre que existe un número infinito de primos de la forma $4k + 3$.

Ejercicio: Demuestre por inducción que si p_n es el n-esimo entero primo, entonces $p_n \leq 2^{2^n}$.

Computaciones de primos

Algunas preguntas naturales a esta altura:

- ¿Cómo decidimos si un número es primo?
- ¿Cómo encontramos la factorización prima de un número?

Recién en el 2002 se supo que el primer problema podía ser resuelto en tiempo polinomial.

El algoritmo polinomial es difícil de aplicar, y las técnicas que se ocupan para chequear primalidad están basadas en algoritmos aleatorios.

Algoritmo euclideano

La clave para desarrollar una teoría algorítmica de números más avanzada es un algoritmo que computa el mayor común denominador de dos enteros, que se llama el algoritmo euclideano.

Denotamos el mayor común denominador de a y b por $gcd(a, b)$. Dos enteros son primos relativos si su mayor común denominador es 1.

Algunas propiedades del mayor común divisor

Ejercicio: Demuestre que si al dividir b por a obtenemos resto r, entonces $gcd(a, b) = gcd(a, r)$.

Ejercicio: Demuestre que si a es par y b es impar, entonces $gcd(a, b) = gcd(a/2, b)$.

Ejercicio: Demuestre que si ambos a y b son pares, entonces $gcd(a, b) = 2gcd(a/2, b/2)$.

Algoritmo euclideano

Ejercicio: ¿Cómo se puede utilizar la factorización prima de dos enteros para encontrar su mayor común denominador?

Algoritmo euclideano

Ejercicio: ¿Cómo se puede utilizar la factorización prima de dos enteros para encontrar su mayor común denominador?

Encontrar una factorización prima es algo costoso, por lo que debemos encontrar otro algoritmo para determinar el mayor común denominador de dos enteros.

Este es el algoritmo euclideano: Bastará ilustrarlo con un ejemplo.

Ilustración del algoritmo euclideano

Deseamos encontrar $gcd(89, 55)$.

Dividimos a 89 por 55 y obtenemos un resto de 34.

Por resultados anteriores, $gcd(89, 55) = gcd(55, 34)$.

De la misma forma, dividimos 55 por 34 y obtenemos resto de 21.

Por tanto, $gcd(55, 34) = gcd(34, 21)$.

Pero luego, $gcd(34, 21) = gcd(21, 13) = gcd(13, 8) = gcd(8, 5) = gcd(5, 3) = gcd(3, 2) = gcd(2, 1) = 1$.

Concluimos que $gcd(89, 55) = 1$.

Propiedades del algoritmo

Ejercicio: ¿Cuántos pasos utiliza el algoritmo hasta parar (sobre enteros a y b)?

Ejercicio: Sea $d = gcd(a, b)$. Demuestre que d puede ser escrito de la forma $am + bn$, para m y n son enteros (y, además, esto se puede hacer de forma eficiente).

Ejercicio sobre congruencias lineales

Una congruencia lineal es una ecuación de la forma $ax \equiv b \pmod{m}$, donde a, b son enteros y m es un entero positivo.

Para resolver estas ecuaciones basta encontrar un inverso de a modulo m, i.e. un entero a^{-1} tal que $a^{-1}a \equiv 1 \pmod{m}$. (¿Por qué?)

Ejercicio: Si a y m son primos relativos tal que $m > 1$, entonces un inverso de a modulo m existe. Además, este inverso es único módulo m.

Teorema del resto chino

¿Cuándo un sistema de congruencias lineales tiene una solución?

El teorema del resto chino dice que esto siempre es el caso cuando los módulos utilizados en las ecuaciones son entre si primos relativos. Además, en este caso la solución es única modulo el producto de esos módulos.

Teorema

Sean $m_1, \ldots, m_n$ *enteros positivos tal que, para todo* $1 \leq i, j \leq n$ *con* $i \neq j$*, es el caso que* $gcd(m_i, m_j) = 1$*. Entonces el sistema*

$$\{x \equiv a_i \pmod{m_i} \mid 1 \leq i \leq n\},$$

donde $a_1, \ldots, a_n$ *son enteros arbitrarios, tiene una única solución módulo* $m = m_1 m_2 \cdots m_n$*.*

Teorema del resto chino: Demostración

Demostraremos que existe solución. Dejaremos como ejercicio demostrar que esta es única módulo $m = m_1 m_2 \cdots m_n$.

Defina $M_i = m/m_i$, para cada $i \in [1, n]$.

Entonces $gcd(m_i, M_i) = 1$, para cada $i \in [1, n]$. (¿Por qué?)

Por el ejercicio anterior existe y_i tal que $M_i y_i \equiv 1 \pmod{y_i}$.

Considere la suma $t = \sum_{i=1}^{n} a_i M_i y_i$.

Es posible demostrar que t es solución al sistema de ecuaciones.

Test de primalidad

Un test de primalidad es un algoritmo que permite verificar si un número es primo.

El test más básico es, dado entero n, verificar para cada $j \in [0, n-1]$ si j divide a n.

De hecho, bastaría con verificar para $j = 2$ y para todo entero j impar tal que $2 \leq j \leq \lceil \sqrt{n} \rceil$.

Cualquiera de estos métodos será demasiado costoso.

Test de Fermat

El pequeño teorema de Fermat al menos nos ayuda a determinar cuando un número no es primo.

Test de Fermat

Si $2^{n-2} \not\equiv 2 \pmod{n}$ *entonces* n *no es primo.*

Existen técnicas que permiten computar eficientemente el resto obtenido de dividir 2^{n-2} por n.

Test de Fermat

El pequeño teorema de Fermat al menos nos ayuda a determinar cuando un número no es primo.

Test de Fermat

Si $2^{n-2} \not\equiv 2 \pmod{n}$ *entonces* n *no es primo.*

Existen técnicas que permiten computar eficientemente el resto obtenido de dividir 2^{n-2} por n.

Desafortunadamente, los seudoprimos nos pueden entregar *falsos positivos* en el Test de Fermat. Podemos usar el test dependiendo de lo crítica que sea nuestra aplicación.

Test de Fermat generalizado

Test Generalizado de Fermat

Un entero positivo n es primo si y solo si $a^{n-1} \equiv 1 \pmod{n}$, para todo $a \in [1, n-1]$.

Ejercicio: Demuestre la correctitud del test generalizado.

Test de Fermat generalizado

Test Generalizado de Fermat

Un entero positivo n es primo si y solo si $a^{n-1} \equiv 1 \pmod{n}$, para todo $a \in [1, n-1]$.

Ejercicio: Demuestre la correctitud del test generalizado.

El problema es que este test es muy ineficiente.

Refinamiento del test generalizado

El test de Fermat podría ser refinado de la siguiente manera (¿por qué?):

Test Refinado de Fermat

Un entero positivo n es primo si y solo si $a^{n-1} \equiv 1 \pmod{n}$, para todo $a \in [1, p]$, donde p es el menor divisor primo de n.

Refinamiento del test generalizado

El test de Fermat podría ser refinado de la siguiente manera (¿por qué?):

Test Refinado de Fermat

Un entero positivo n es primo si y solo si $a^{n-1} \equiv 1 \pmod{n}$, para todo $a \in [1, p]$, donde p es el menor divisor primo de n.

Desafortunadamente, incluso esta versión refinada sigue siendo ineficiente...

Miller-Rabin test

Este es el test que ocupa Maple para verificar si un número es primo.

Es un algoritmo probabilista, i.e. entrega una respuesta que con alta probabilidad es cierta.

Miller-Rabin test

Este es el test que ocupa Maple para verificar si un número es primo.

Es un algoritmo probabilista, i.e. entrega una respuesta que con alta probabilidad es cierta.

Sea n un entero. Elegimos un entero a al azar entre 2 y $n-1$, y factorizamos $a^n - a$ como $a(a^{n-1} - 1)$.

Luego, utilizamos la identidad $(x^n - 1) = (x^{n/2} - 1)(x^{n-2} + 1)$ tanto como se pueda.

Si n es primo debe dividir al menos a uno de los factores resultantes.

Miller-Rabin test

El problema es que si n divide a alguno de los factores podría ser que no fuera primo.

Sin embargo, esto ocurre con probabilidad $< 1/2$.

Se sigue que si repetimos una gran cantidad de veces el test, la probabilidad de que entregue una respuesta incorrecta es muy baja.