Discrete Mathematics
Lecture-15

Ngày 9 tháng 12 năm 2011

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)
- Returns an integer $c < b$ such that $a \cdot c$ mod $b = 1$.

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)
- Returns an integer $c < b$ such that $a \cdot c$ mod $b = 1$.
- How many digits does the integer n have?

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)
- Returns an integer $c < b$ such that $a \cdot c$ mod $b = 1$.
- How many digits does the integer n have?
- len(str(n))

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)
- Returns an integer $c < b$ such that $a \cdot c$ mod $b = 1$.
- How many digits does the integer n have?
- len(str(n))
- factorial(n)

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)
- Returns an integer $c < b$ such that $a \cdot c$ mod $b = 1$.
- How many digits does the integer n have?
- len(str(n))
- factorial(n)
- Returns n!

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)
- Returns an integer $c < b$ such that $a \cdot c \bmod b = 1$.
- How many digits does the integer n have?
- len(str(n))
- factorial(n)
- Returns $n!$
- $is\_prime(n)$

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $\quad bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)
- Returns an integer $c < b$ such that $a \cdot c$ mod $b = 1$.
- How many digits does the integer n have?
- len(str(n))
- factorial(n)
- Returns n!
- $is\_prime(n)$
- Returns True or False

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)
- Returns an integer $c < b$ such that $a \cdot c$ mod $b = 1$.
- How many digits does the integer n have?
- len(str(n))
- factorial(n)
- Returns n!
- *is_prime*(n)
- Returns True or False
- pow(a,b,c)

SAGE number theory functions

A quick review of some number theory functions in SAGE:

- gcd(x,y)
- Returns the greatest common divisor of x and y.
- exgcd(x,y)
- Returns (a, b, c) $a = gcd(x, y)$ $bx + cy = a$.
- a^{-1} mod b (gcd(a,b) = 1)
- Returns an integer $c < b$ such that $a \cdot c$ mod $b = 1$.
- How many digits does the integer n have?
- len(str(n))
- factorial(n)
- Returns $n!$
- $is\_prime(n)$
- Returns True or False
- pow(a,b,c)
- Returns a^b mod c.

Some theorems we shall be using

- **Fermat's Theorem:**
  If p is prime and $0 < a < p$ then $a^{p-1} \bmod p = 1$.

Some theorems we shall be using

- **Fermat's Theorem:**
  If p is prime and $0 < a < p$ then $a^{p-1} \bmod p = 1$.
- **Chinese Remainder Theorem:**
  Given $[a_1, a_2, \ldots, a_k]$ pairwise relatively prime integers and integers $[m_1, m_2, \ldots, m_k],\ m_i < a_i$ then there is a unique integer $M < \prod_{i=1}^{k} m_i$ such that $M \bmod a_i = m_i$

Some theorems we shall be using

- **Fermat's Theorem:**
  If p is prime and $0 < a < p$ then $a^{p-1} \bmod p = 1$.
- **Chinese Remainder Theorem:**
  Given $[a_1, a_2, \ldots, a_k]$ pairwise relatively prime integers and integers $[m_1, m_2, \ldots, m_k],\ m_i < a_i$ then there is a unique integer $M < \prod_{i=1}^{k} m_i$ such that $M \bmod a_i = m_i$
- **Euler's Theorem:**
  Recall: $\phi(n) = \mid \{a \mid 1 \leq a < n\},\ gcd(n, a) = 1\} \mid$.
  If $gcd(n, a) = 1$ then $a^{\phi(n)} \bmod n = 1$.

Some theorems we shall be using

- **Fermat's Theorem:**
  If p is prime and $0 < a < p$ then $a^{p-1} \bmod p = 1$.
- **Chinese Remainder Theorem:**
  Given $[a_1, a_2, \ldots, a_k]$ pairwise relatively prime integers and integers $[m_1, m_2, \ldots, m_k],\ m_i < a_i$ then there is a unique integer $M < \prod_{i=1}^{k} m_i$ such that $M \bmod a_i = m_i$
- **Euler's Theorem:**
  Recall: $\phi(n) = \mid \{a \mid 1 \leq a < n\},\ gcd(n, a) = 1\} \mid$.
  If $gcd(n, a) = 1$ then $a^{\phi(n)} \bmod n = 1$.
- **Wallis' Theorem**
  $(p-1)! \bmod p = -1$ if and only if p is prime.

Some theorems we shall be using

- **Fermat's Theorem:**
  If p is prime and $0 < a < p$ then $a^{p-1} \bmod p = 1$.
- **Chinese Remainder Theorem:**
  Given $[a_1, a_2, \ldots, a_k]$ pairwise relatively prime integers and integers $[m_1, m_2, \ldots, m_k],\ m_i < a_i$ then there is a unique integer $M < \prod_{i=1}^{k} m_i$ such that $M \bmod a_i = m_i$
- **Euler's Theorem:**
  Recall: $\phi(n) = \mid \{a \mid 1 \leq a < n\},\ gcd(n, a) = 1\} \mid$.
  If $gcd(n, a) = 1$ then $a^{\phi(n)} \bmod n = 1$.
- **Wallis' Theorem**
  $(p-1)! \bmod p = -1$ if and only if p is prime.
- **Primitive Roots:** The finite field $GF(q)$ has primitive roots $(\ \{a^k,\ 0 \leq k \leq q-2\} = GF^*(q))$.