CS228

Nathan Sprague

January 27, 2014

Prime Numbers

Definition

An integer p greater than is called *prime* if the only positive factors of p are 1 and p. A positive integer greater than 1 that is not prime is called *composite*.

Fundamental Theorem of Arithmetic

Theorem

Fundamental Theorem of Arithmetic Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Example:
$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2 = 100$

Primality Checking

In Python:

```python
def check_prime(n):
    """ Brute force primality testing. """
    for d in xrange(2, int(n**.5) + 1):
        if n % d == 0:
            return False
    return True
```

Infinitely Many Primes

There are infinitely many primes.

- Side note: The twin Prime conjecture.
  - On April 17th 2013, Yitang Zang Proved the conjecture for a gap of 70,000,000. http://en.wikipedia.org/wiki/Twin_prime
  - As of today, the gap is down to 270.

http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes

Greatest Common Divisors

Definition

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Examples:
$\gcd(24, 36) = 12$
$\gcd(17, 22) = 1$

Relatively Prime integers

Definition

The integers *a* and *b* are *relatively prime* if their greatest common divisor is 1.

Example:
17 and 22 are relatively prime.

Using Prime Factorization to Find gcd

Suppose that the prime factorizations of the positive integers a and b are

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_m} \qquad b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_m}$$

Then

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)}$$

Example:
Prime factorization of 120: $120 = 2^3 \cdot 3 \cdot 5$
Prime factorization of 500: $500 = 2^2 \cdot 5^3$

$$gcd(120, 500) = 2^2 3^0 5^1 = 20$$

Using Prime Factorization to Find Least Common Multiple

Definition

he least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\mathrm{lcm}(a,b)$.

Suppose that the prime factorizations of the positive integers a and b are

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_m} \qquad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_m}$$

Then

$$\mathrm{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$$

Euclidean Algorithm

```
procedure GCD(a,b : positive integers)
    y := a
    x := b
    while y ≠ 0 do
        r := x mod y
        x := y
        y := r
    return x
```

Python Lab

- Open the Geany text editor.
- Make sure it indents with spaces instead of tabs:
  - Edit $\rightarrow$ Preferences $\rightarrow$ Editor $\rightarrow$ Indentation
- Download `primes.py` from the course schedule page.
- Execute it:
  - By typing `python primes.py` in the terminal or
  - By clicking on the gear icon.
- Implement Euclid's algorithm and the Base-b expansion algorithm (on the next page)

Base-b Expansion Algorithm

procedure Base-b Expansion(n,b : positive integers with $b > 1$)
$q := n$
$k := 0$
while $q \neq 0$ **do**
$a_k := q \text{ mod } b$
$q := q \text{ div } b$
$k := k + 1$
return $(a_{k-1}, \ldots, a_1, a_0)$

Suggestion: Use a Python list to store $a_{k-1}, \ldots, a_1, a_0$