CSCI 104L Lecture 16: Number Theory

Pseudorandom Numbers

Your computer's random number generator is not truly random; it's *pseudorandom*. The *linear congruential method* to choose pseudorandom numbers works as follows: we choose four integers: the modulus m, the multiplier a, the increment c, and the seed x_0. When we want the "next random" number, we generate it as follows:

$x_{n+1} = (ax_n + c)\%m$

Primes and Greatest Common Divisors

An integer $p > 1$ is *prime* if the only positive factors of p are 1 and p. A positive integer $p > 1$ that is not prime is called composite. The integer 1 is called a *unit* and is neither prime nor composite.

The Fundamental Theorem of Arithmetic: every integer $n \geq 2$ can be factored into a unique product of primes $n = p_1 p_2 \dots p_r$, where $p_1, p_2, ..., p_r$ are in increasing order.

Greatest Common Divisors and Least Common Multiples

Given two integers a, b, not both zero. The largest integer d such that $d|a$ and $d|b$ is the **greatest common divisor** of a and b, denoted $\gcd(a, b)$.

Two numbers are **relatively prime** if their gcd is 1.

Question 1. What is gcd(24,36)?

Euclidean Algorithm

Suppose we want to calculate $\gcd(91, 287)$.

First divide the larger by the smaller to obtain $287 = 91 \cdot 3 + 14$. Any divisor of both 91 and 287 must also be a divisor of 14. Hence we can now search for the greatest common divisor of 91 and 14.

$91 = 14 \cdot 6 + 7$. So, any divisor of 91 and 14 must also be a divisor of 7 (and by extension, 287).

$14 = 7 \cdot 2 + 0$. So, 7 divides 14, and be extension, 91 and 287. 7 is the gcd.

```
EuclideanAlgorithm (a,b:  positive integers)

  x ← a
  y ← b
  while y ≠ 0 do
    r ← x%y
    x ← y
    y ← r
  return  x
```

Question 2. What is $\gcd(414, 662)$?

How can we tell if a number is prime?

One mechanism we can use is by checking the possible prime factors of a number. Observe that if n is a composite integer, it has a prime divisor less than or equal to $\sqrt{n}$.

Question 3. Is 101 prime? Prove your answer.

We can use a more algorithmic approach; suppose you wanted to find all primes not exceeding some number. There's a method for this, known as the **Sieve of Eratosthenes**.

To find all primes not exceeding x, note that any such prime must have a prime divisor $\leq \sqrt{x}$. List out the numbers $2...x$. Remove all numbers a multiple of the first number, so we have all odd numbers between 3 and x. Do it again, so all multiples of 3 are removed. Then all multiples of 5 are removed, followed by 7. Repeat until the smallest number is larger than $\sqrt{x}$.

Conjectures about prime numbers

Goldbach's Conjecture claims that every even integer $n > 2$ is the sum of two primes.

Twin Primes are pairs of primes that differ by 2; for example, 5 and 7, 11 and 13, 17 and 19, 4967 and 4969, and 8675309 and 8675311 are each twin primes. The Twin Prime Conjecture claims there are infinitely many twin primes.

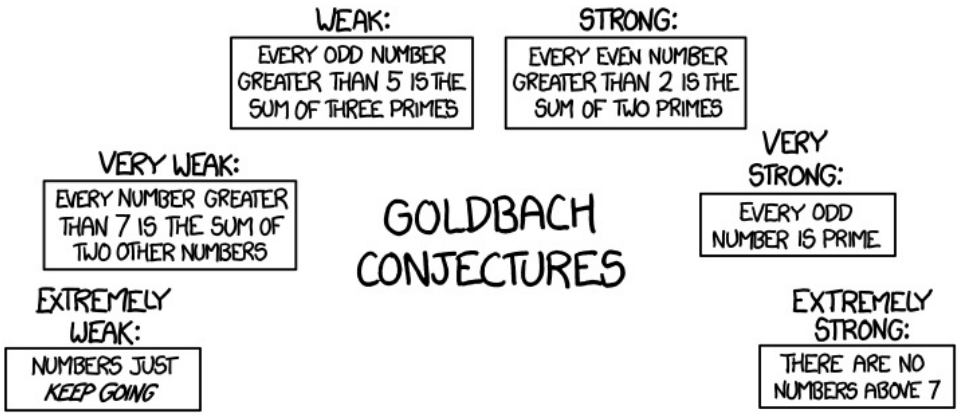

Figure 1: XKCD # 1310: Goldbach Conjectures. The weak twin primes conjecture states that there are infinitely many pairs of primes. The strong twin primes conjecture states that every prime p has a twin prime $(p + 2)$, although $(p + 2)$ may not look prime at first. The tautological prime conjecture states that the tautological prime conjecture is true.