

# CSCI 104L Lecture 15: Introduction to Number Theory

## Probability Wrap-up

**Question 1.** A coin comes up heads with probability  $p$ . We will flip this coin until it comes up heads. What is the expected number of flips required?

A random variable has a **geometric distribution** with parameter  $p : 0 \leq p \leq 1$  if  $p(X = k) = (1 - p)^{k-1}p$ , for  $k = 1, 2, 3, \dots$ .  
It has expected value  $\frac{1}{p}$ .

**Question 2.** The probability that a randomly chosen 1000 digit number is prime is approximately  $1/2302$ . Suppose we select a 1000 digit number at random and check if it is prime; if it is, we're done, and otherwise we randomly select another (possibly different) number and continue. What is the expected number of times we select a 1000 digit number?

**Question 3.** A medieval gladiator fights in an arena. On each day, he has a  $\frac{1}{8}$  probability of dying, a  $\frac{1}{4}$  probability of winning his freedom, and otherwise is sent back to his jail cell to fight again the next day. What is the expected number of days the gladiator will fight?

## Number Theory

If  $a$  and  $b$  are integers and  $m$  is a positive integer, then  $a$  is congruent to  $b$  modulo  $m$  iff  $a \bmod m = b \bmod m$ .

$a \equiv b \pmod{m}$  means  $a$  is congruent to  $b$  modulo  $m$ . Otherwise we write  $a \not\equiv b \pmod{m}$ .

$a \equiv b \pmod{m}$  is the same as  $b = a + mf$  for some (possibly negative) integer  $f$ .

**Question 4.** Are 24 and 14 congruent modulo 6?

**Question 5.** Is 17 congruent to 5 modulo 6?

Given  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a + c \equiv b + d \pmod{m}$  and  $a \cdot c \equiv b \cdot d \pmod{m}$ .

## Alternate number bases

“Base  $b$ ” numbers’ digits are all  $\bmod b$ .

- If  $b > 10$ , then “digit” 10 is ‘A,’ “digit” 11 is ‘B,’ and so on.
- “BEEF” is a number in base 16.

To disambiguate the base, we write it as a subscript:  $CAB_{16} = 3243_{10} = 110010101011_2$

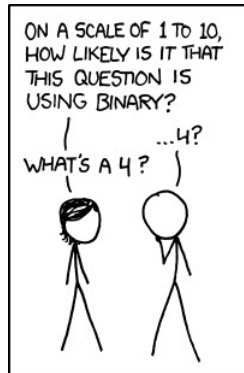


Figure 1: XKCD #953: 1 to 10. If you get an 11/100 on a CS test, but you claim it should be counted as a ‘C’, they’ll probably decide you deserve the upgrade.

## Applications of Congruences

### Parity Check

When sending digital information, the probability that any given bit is sent incorrectly is very small, but not zero; each bit’s probability is independent. We want to find a way to determine if a transmission error happened. We do this by ensuring that the bitstring we send has *even parity*: that is, the sum of the bits, mod 2, is 0.

We achieve this by taking the  $n$ -bit string we wish to send,  $x_1x_2\dots x_n$ , and appending an extra bit  $x_{n+1} = x_1 + x_2 + \dots + x_n \bmod 2$ . We can now send the string.

**Question 6.** If we receive transmissions of 011000101 and 11010110, should we believe them to be correct? What could cause us to be wrong in our conclusion, and how likely is that?

### Pseudorandom Numbers

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```

Figure 2: XKCD # 221: Random Number. RFC 1149.5 specifies 4 as the standard IEEE-vetted random number.

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  $p_1, p_2, \dots, p_r$  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 7.** 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 by 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 8.** 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 9.** 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  $2 \dots x$ . 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.

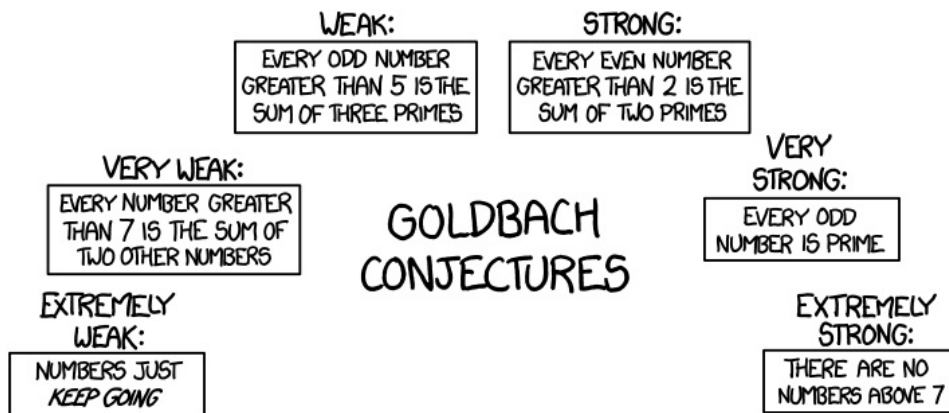


Figure 3: XKCD # 1310: Goldbach Conjectures. The weak twin primes conjecture states that there are infinitely many pairs of primes. The strong twin primes conjecture states that every prime  $p$  has a twin prime  $(p + 2)$ , although  $(p + 2)$  may not look prime at first. The tautological prime conjecture states that the tautological prime conjecture is true.