Primes

A prime number is an integer $p \geqslant 2$ whose only (integer) divisors are 1 and p.

Fundamental theorem of arithmetic: Every integer n can be expressed uniquely as

$$n = p_1^{r_1} \cdots p_\ell^{r_\ell}, \quad \text{with } p_1 < \cdots < p_\ell \text{ prime, } r_i \in \mathbb{Z}_{>0}.$$

Big idea: primes are the building blocks of the integers.

Question: How many prime numbers are there?
Let $p_1, p_2, \ldots, p_\ell$ be the first ℓ primes, and consider

$$N = p_1 p_2 \cdots p_\ell + 1.$$

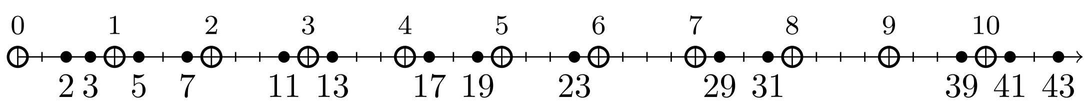
N is congruent to 1 modulo p_i for $i = 1, \ldots, \ell$, and is therefore not a multiple of any of these.

Theorem

There are infinitely many primes.

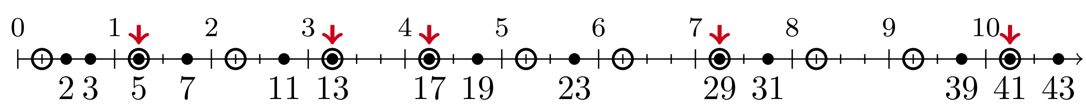
Arithmetic progressions

Question: How many primes are there congruent to $0 \pmod 4$?

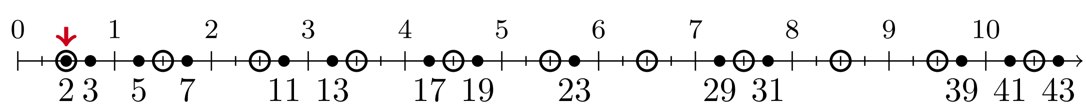


Answer: None. (If $4|a$, then a is not prime.)

$*$ Question: How many primes are there congruent to $1 \pmod 4$?

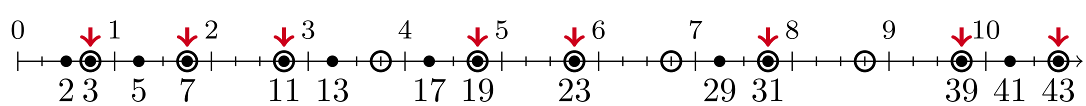


Question: How many primes are there congruent to $2 \pmod 4$?



Answer: One. (If $4|a-2$, then a is even.)

$*$ Question: How many primes are there congruent to $3 \pmod 4$?



Arithmetic progressions

Fact: There are no primes congruent to $0 \pmod 4$, and there is exactly 1 prime congruent to $2 \pmod 4$.

Hypothesis: There are infinitely many primes that are congruent to $1 \pmod 4$, and there are infinitely many primes that are congruent to $3 \pmod 4$.

Recall, an arithmetic progression (or arithmetic sequence) is a sequence of numbers that differ by a constant value n; i.e. a list of all positive integers congruent to some $r \pmod n$, given in increasing order. For example,

$$1,\ 5,\ 9,\ 13, \dots \text{ is arithmetic },\quad 1,\ 2,\ 4,\ 8, \dots \text{ is not.}$$

So

"How many primes are there congruent to $r \pmod n$?"

is the same as

"How many primes lie in the arithmetic progressions $r + kn$?"

This is *different* from finding finite arithmetic sequences of primes.

Example: 3, 7, 11 is an arithmetic progression of length 3.

Example: 5, 17, 29, 41, 53 is an arithmetic progression of length 5.

Arithmetic progressions

Fact: There are no primes congruent to $0 \pmod 4$, and there is exactly 1 prime congruent to $2 \pmod 4$.

Hypothesis: There are infinitely many primes that are congruent to $1 \pmod 4$, and there are infinitely many primes that are congruent to $3 \pmod 4$.

Theorem (Dirichlet's Thm. on Primes in Arith. Progressions)

Let a and m be integers with $\gcd(a, m) = 1$. Then there are infinitely many primes that are congruent to $a \pmod m$.

Note: This is challenging to prove, and we won't prove this in general. Instead...

Arithmetic progressions

Proposition

There are infinitely many primes that are congruent to $3 \pmod 4$.

Proof.

Let $\{3, p_1, \ldots, p_\ell\}$ be the first $\ell + 1$ primes that are congruent to $3 \pmod 4$. Consider

$$N = 4p_1 \cdots p_\ell + 3.$$

Now factor N into primes:

$$N = q_1 q_2 \cdots q_r, \qquad \text{where } q_1 \leqslant \cdots \leqslant q_r \text{ are prime.}$$

Claim 1: $\{3, p_1, \ldots, p_\ell\}$ is disjoint from $\{q_1, q_2, \ldots, q_r\}$.
Claim 2: at least one of $q_1, q_2, \ldots q_r$ is be congruent to $3 \pmod 4$.
So any finite list of primes congruent to $3 \pmod 4$ is missing at least one such prime. □

Why doesn't this proof work for showing that there are infinitely many primes that are congruent to $3 \pmod 4$?