COMPSCI 250 Discussion #4: Infinitely Many Primes
Individual Handout

David Mix Barrington and Mordecai Golin
1 March 2024

In this discussion we will apply our proof methods and some facts about congruences from this week's lectures to prove some facts about prime numbers.

The basic fact is that there are infinitely many prime numbers:

$$\forall a : \exists b : (a < b) \wedge P(b)$$

where $P(b)$ means "b is prime". We'll prove this in another form:

$$\forall S : [\forall x : (x \in S) \rightarrow P(x)] \rightarrow [\exists y : P(y) \wedge (y \notin S)]$$

where the type of S is "finite set of naturals". (If S could be an infinite set of naturals this new statement would not be true, because S could then be the set of all primes.)

The basic idea in proving the first statement is to let a be arbitrary and let z be the natural $a! + 1$, where $a!$ is the **factorial** of a, the product of all positive naturals up to a. (So $3! = 1 \cdot 2 \cdot 3 = 6$ and $7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 5040$.) We'll show on the board:

- No natural in the range from 2 through a divides z.
- Some prime number divides z.

Our task here is to write down a convincing version of this argument to prove the second statement above, that if S is a finite set of primes there must be a prime not in S.

If you finish that, we have a second task. Define the predicate $P_3(x)$ to be "x is prime and $x \equiv 3 \pmod 4$". The first six numbers satisfying P_3 are 3, 7, 11, 19, 23, and 31. Our goal is to adapt the proof about S to show:

$$\forall S : [\forall x : (x \in S) \rightarrow P_3(x)] \rightarrow [\exists y : P_3(y) \wedge (y \notin S)]$$

and thus that there are infinitely many P_3 primes. (It turns out that there are an infinite number of P_1 primes x (with $x \equiv 1 \pmod 4$) as well, but this is a bit harder to prove.)

A key step in the argument is the following: If a number x satisfies $x \equiv 3 \pmod 4$, then it cannot be a product only of P_1 primes. You will want to use a key fact that follows from our proof that multiplication of congruence classes is well-defined: If a and b are each congruent to 3, modulo 4, then ab is congruent to 1, modulo 4. Similarly if $a \equiv 3 \pmod 4$ and $b \equiv 1 \pmod 4$, then $ab \equiv 3 \pmod 4$.

To summarize:

Writing Exercise: With S typed as "finite set of naturals" and the other variables typed as naturals, prove:

- $\forall S : [\forall x : (x \in S) \rightarrow P(x)] \rightarrow [\exists y : P(y) \wedge (y \notin S)]$
- $\forall S : [\forall x : (x \in S) \rightarrow P_3(x)] \rightarrow [\exists y : P_3(y) \wedge (y \notin S)]$