Proof of Twin Prime Conjecture

Notchmath

May 6 2020

1 Properties that a number between twin primes must have

1.1 Modularity with respect to individual primes

Let N be any number which is between twin primes. By definition, N+1 is prime and N-1 is prime. Because N - 1 is prime, it must not be divisible by any number besides itself. Thus, for all $P < N - 1$, we have the following equation:

$$N - 1 = / = 0 mod P$$

By adding 1 to each side we get:

$$N = / = 1 mod P$$

Similarly, N + 1 is not divisible by any prime beneath it, including all primes *P¡N-1*. Thus, we have the following equation:

$$N + 1 = / = 0 mod P$$

And by subtracting 1 from each side we get:

$$N = / = -1 mod P$$

1.2 Modularity with respect to multiple primes

Consider the case where P = 2. We can easily verify that any possible N must be 0 mod 2.

Now we will proceed with a proof by induction to determine what values N can have with respect to greater values of P. Note that we are not working with any specific N, merely stating the values for all possible N.

Consider the case where $N = (A1, A2, A3...AM) mod A$, where A is the product of all primes up to and not including B. Let us also consider that *N = (0, 2, 3.... B-3, B-2) mod B.*

Consider what possible values N can have when taken mod AB. Consider each set of values pairwise. If $N = I mod A$ and *N = J mod B* for any I and

J, the Chinese Remainder Theorem states that there is exactly one number K such that $N = KmodAB$.

In addition, because either I or J must vary for each possible combination, every value of K is unique.

This means there are exactly $M(B-2)$ possible values of K such that $N = KmodAB$.

Because AB is the product of all primes up to and including B, the proof by induction that there are arbitrarily many values such that $N = KmodQ$ where Q is the product of all primes up to and including an arbitrary P is complete.

Thus, despite not having verified the existence of an N above P, we can determine what such an N must look like.

Because there are arbitrarily many values of K for arbitrary Ps, if it can be shown that for each value of K there exists a number N that is at the center of a pair of twin primes, then there are infinite twin primes.

1.3 Additional properties

Note that if a number K exists in a base Q, where Q is the product of all primes up to and including P, such that an N above P could have the property $N = KmodQ$, and $K < P^2$, then K itself is either at the center of a pair of twin primes or is 0.

This can be shown because, by definition, the equality $N = KmodQ$ states that K+1 and K-1 are not divisible by any prime P or below, and because $K < P^2$ K+1 and K-1 cannot be divisible by any prime above P.

Thus, K+1 and K-1 cannot be composite. If K is equal to 0, then indeed K+1 and K-1 are simply 1 and -1 which are neither prime nor composite. If K is larger than 2, both K-1 and K+1 must be prime, so K defines a pair of twin primes. (Note that K cannot equal 2 because in base 6 and above K = -1 mod 3 and in base 2 the number 2 is simply 0 mod 2.)

2 Proof that there are infinite twin primes

2.1 What must be shown

Let Y be a number such that in base X, where X is the product of all primes up to and including C, an N above base X could have the property $N = YmodX$.

We are not necessarily assuming such an N exists, however. For the rest of this proof, N will be used to refer to any theoretical N. Even if such an N doesn't exist, because the properties that affect it can be shown to persist by induction. For example, when looking at N in reference to all primes above P, the product of P with every prime below it will always be guaranteed to create the situation we can work with.

The intent of this proof is to demonstrate that for every Y there exists a R such that $R < S^2$, where $S > X$ and $N = RmodS$, and thus for every Y there is a set of twin primes greater than or equal to Y. As X and Y can grow arbitrarily large, this would be sufficient to demonstrate that there are infinitely many twin primes.

2.2 Maximum lowest R given a Y

In this section, I will demonstrate an upper bound on the lowest possible R as the base S increases. Note that I am not yet assuming that $R < S^2$.

If S = X, then the maximum value of the lowest R is equal to Y.

Let D be the next prime above C. All numbers that stem from Y must be of the form $N = YmodX$, and in base XD the number of numbers L such that $N = LmodXD$ and L stems from Y can be determined as follows.

Let N = Y mod X, and consider the list of values I such that N could equal I mod D. There are exactly D-2 values of I possible. By the Chinese Remainder Theorem, for each value of I mod D, assuming N = Y mod X, there exists exactly one number L such that N = L mod XD. Thus there are D-2 values of L.

Consider the lowest of these values of L. This exists in the case where Y = 1 or -1 mod D and Y + X = -1 or 1 mod D. Because D is coprime to X, if Y is 1 mod D and Y + X is -1 mod D (or vice versa), Y + 2X can be neither 1 or -1 mod D, and thus Y + 2X must equal V mod D where V is not 1 or -1, and thus Y + 2X is the maximum value for the lowest L.

Similarly, let E be the next prime above D. All numbers that stem from Y must be of the form N = (Y + xX) mod XD for some value x. Specifically, because we are considering the maximum of the lowest possible R, we can work with a number which is Y + 2X such that N = (Y + 2X). If there exists a coefficient of X smaller than 2, then the W would simply be smaller than the maximum, which is acceptable.

Using similar logic to before, we can determine that there are E-2 values of T such that N = T mod XDE. Consider the miminum possible value of T.

Assume that Y + 2X is 1(or -1) mod E and Y + 2X + D is -1(or 1) mod E. Thus Y + 2X + 2D is not 1 or -1 mod E, and is the smallest number we can guarantee to have this property.

However, note that by adding D we ran the risk that Y + 2X + 2D is now equal to 1(or -1) mod X, because D is coprime to X. To solve this, we add D again, but this may still be equal to -1(or 1) mod X. Thus, we have to add D a second time, to result in Y + 2X + 4D, which is not equal to -1 or 1 mod X.

Because Y + 2X is not equal to 1 or -1 mod D, Y + 2X + 4D is not equal to 1 or -1 mod D.

Because Y + 2X was assumed to be equal to 1(or -1) mod E, and Y + 2X + D was assumed to be -1(or 1) mod E, and D and E are coprime, Y + 2X + 4D is not equal to 1 or -1 mod E.

Thus, Y + 2X + 4D is the number such that we can guarantee N = Y + 2X + 4D mod XDE at maximum.

Let us now perform a proof by induction. Let us assume we have a number F such that F = Y + 2X + 4D +.... 4(G'th prime), and that we can guarantee N = F mod (X * D * E *.... ((G+1)'th prime)) at maximum.

Let us determine the smallest H such that N = H mod (X * D * E *...((G+2)'th prime)) at maximum.

Assume that F = 1 (or -1) mod ((G+2)'th prime), and F + ((G+1)'th prime)= -1 (or 1) mod ((G+2)'th prime).

Thus, F + 2((G+1)'th prime), F + 3((G+1)'th prime), and F + 4((G+1)'th prime) are all NOT 1 or -1 mod ((G+2)'th prime).

Assume F + 2((G+1)'th prime) is equal to 1 (or -1) mod (X*D*E*...(G'th prime) and F + 3((G+1)'th prime is equal to -1 (or 1) mod (X*D*E*...(G'th prime).

Thus, F + 4((G+1)'th prime) is NOT equal to 1 or -1 mod (X*D*E*...(G'th prime). In addition, F + 4((G+1'th prime) is NOT equal to 1 or -1 mod ((G+1)'th prime) because F is not equal to 1 or -1 mod ((G+1)'th prime).

Thus, by induction, an increase from base (X*D*E*...((G+1)'th prime) to base (X*D*E...((G+2)'th prime) will require a shift of at most 4((G+1)'th prime), added, not multiplied.

2.3 Proving the Twin Prime conjecture

Let U be the difference between 4((W-1)'th prime + 4(W-2)'th prime +... 4E + 4D + 2X + Y and (W'th prime)^2.

Let Q be the difference between 4(W'th prime) + 4((W-1)'th prime) +... 4E + 4D + 2X + Y and ((W+1)'th prime)^2.

Let ((W+1)'th prime) be equal to W + O. Note that O must be greater than or equal to 2.

Q is equivalent to the difference between 4(W'th prime) + 4((W-1)'th prime) +... 4E + 4D + 2X + Y and ((W'th prime)$^2 + 2O(W'thprime) + O^2$).

U - Q = 4(W'th prime) - (2O(W'th prime) + O^2).

U - Q = - 2(O-2)(W'th prime) - O^2.

Because U - Q is negative, the maximum possible value which we can guarantee will exist in any given base moves down compared to the base squared as the base grows larger.

Eventually, because U - Q does not tend towards zero, we can guarantee there exists a base where the maximum possible value we can guarantee exists in that base is lower than the base squared.

Thus, eventually, we can guarantee that there is an R such that N = R mod S and R ¡ S^2.

Since we can guarantee such an R and S for any initial conditions Y and X, where S is greater than X and R is greater than Y, we can guarantee that there must exist a twin prime pair with their center greater than or equal to Y for any given Y and X.

Because X can be arbitrarily big, and as X increases the highest Y we can choose also increases, we have proven there is a twin prime pair greater than any individual number.

Thus, there are infinite twin primes.