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 α be any prime.

Let B be the prime directly above α.

Let A be the product of all primes below and including α.

Let N be any number larger than $\alpha + 1$ such that $N \not\equiv \pm 1 \pmod{a}$ where a is any prime below B.

Let $P_g =$ the g'th prime number.

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

$$(Z - 1) \not\equiv 0 \pmod{P}$$

By adding 1 to each side we get:

$$Z \not\equiv 1 \pmod{P}$$

Similarly, $Z + 1$ is not divisible by any prime beneath it, including all primes P where $P < Z - 1$ .Thus, we have the following equation:

$$(Z + 1) \not\equiv 0 \pmod{P}$$

And by subtracting 1 from each side we get:

$$Z \not\equiv -1 \pmod{P}$$

Thus, any possible Z must satisfy $Z \not\equiv -1 \pmod{P}$ and $Z \not\equiv 1 \pmod{P}$ for all $P < Z - 1$.

Thus any possible Z must be an N.

1.2 Modularity with respect to multiple primes

Consider the case where $\alpha = 2$. We can easily verify that any possible N must satisfy $N \equiv 0 \pmod 2$.

Now we will proceed with a proof by induction to determine what values N can have with respect to greater values of α. Note that we are not working with any specific N, merely stating the values for all possible N, where N is greater than the largest prime we're working with.

Let a_i's be the numbers that N can be congruent to $\pmod A$

Consider the case where $N \equiv a_1 \pmod A$ or $N \equiv a_2 \pmod A$ or ... or $N \equiv a_M \pmod A$. Let us also consider that $N \equiv 0 \pmod B$ or $N \equiv 2 \pmod B$ or $N \equiv 3 \pmod B$ or... or $N \equiv (B-3) \pmod B$ or $N \equiv (B-2) \pmod B$.

Consider what possible values N can have when taken mod AB. Consider each set of values pairwise. If $N \equiv I \pmod A$ and $N \equiv J \pmod B$ for any I and J, the Chinese Remainder Theorem states that there is exactly one number K such that$N \equiv K \pmod{AB}$.

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 $N \equiv K \pmod{AB}$.

The proof by induction that the number of values of K such that $N \equiv K \pmod Q$ where Q is the product of all primes up to and including an arbitrary P_g is less than the number of values of values of K such that $N \equiv K \pmod{Q * P_{g+1}}$ is complete.

Because there are arbitrarily many values of K for arbitrarily high P_gs, 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 $P+1$ could have the property $N \equiv K \pmod Q$, 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 $N \equiv K \pmod Q$ 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 this would mean $K \equiv -1 \pmod 3$ and in base 2 the number 2 is simply $0 \pmod 2$).

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 could have the property $N \equiv Y \pmod{X}$.

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 $N \equiv R \pmod{S}$, 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 and S

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. In base XD the number of numbers L such that iff $N \equiv L \pmod{XD}$ then $N \equiv Y \pmod{X}$ can be determined as follows.

Let $N \equiv Y \pmod{X}$, 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 $I \pmod{D}$, assuming $N \equiv Y \pmod{X}$, there exists exactly one number L such that $N \equiv L \pmod{XD}$. Thus there are $D-2$ values of L.

Consider the highest minimum of these values of L. This exists in the case where $Y \equiv \pm 1 \pmod{D}$ and $(Y+X) \equiv \mp 1 \pmod{D}$. Because D is coprime to X, if $(\equiv \pm 1 \pmod{D}$ and $(Y+X) \equiv \mp 1 \pmod{D}$, $Y+2X$ can be neither $1 \pmod{D}$ or $-1 \pmod{D}$, and thus $(Y+2X \equiv V \pmod{D}$ where V is not 1 or -1, and thus $Y+2X$ is the upper bound for the minimum L.

Similarly, let E be the next prime above D. Our upper bound for a minumum is $N \equiv (Y+2X) \pmod{XD}$. If there exists a coefficient of X smaller than 2, then the number would simply be lower than the upper bound of the minimum value, which is acceptable.

Using similar logic to before, we can determine that there are $E-2$ values of T such that $N \equiv T \pmod{XDE}$. Consider the upper bound of the minimum value of T.

Assume that $(Y+2X) \equiv \pm 1 \pmod{E}$ and $(Y+2X+D \equiv \mp 1 \pmod{D}$. Thus $(Y+2X+2D) \not\equiv \pm 1 \pmod{D}$, and it is the upper bound for the minimum guaranteed value with this property.

However, note that by adding D we ran the risk that $Y+2X+2D$ is now equal to $\pm 1 \pmod{X}$, because D is coprime to X. To solve this, we add D again, but this may still be equal to $\mp 1 \pmod{X}$. Thus, we have to add D a second time, to result in$(Y+2X+4D) \not\equiv \pm 1 \pmod{X}$.

Because $(Y+2X) \not\equiv \pm 1 \pmod{D}$,we know $(Y+2X+4D) \not\equiv \pm 1 \pmod{D}$.

Because $Y+2X$ was assumed to be equal to $\pm 1 \pmod{E}$, and $Y+2X+D$ was assumed to be $\mp 1 \pmod{E}$, and D and E are coprime, $(Y+2X+4D) \not\equiv \pm 1 \pmod{E}$.

Thus, $Y+2X+4D$ is the number such that we can guarantee$N \equiv (Y+2X+4D) \pmod{XDE}$ is the upper bound for the minimum guaranteed value in base XDE.

Let us now perform a proof by induction. Let us assume we have a number F such that $F = Y+2X+4D+....4P_g$, and that we can guarantee $N \equiv F \pmod{X*D*E*...*P_{g+1}}$ is the upper bound for the minimum guaranteed value in base $X*D*E*...*P_{g+1}$.

Let us determine the smallest H such that$N \equiv H \pmod{X*D*E*...*P_{g+2}}$ is the upper bound for the minimum guaranteed value in base $X*D*E*...*P_{g+4}$

Assume that $(F \equiv \pm 1 \pmod{P_{G+2}})$, and $(F+P_{G+1}) \equiv \mp 1 \pmod{P_{G+2}}$.

Thus, $F+2P_{G+1}$, $F+3P_{G+1}$, and $F+4P_{G+1}$ are all NOT $\pm 1 \pmod{P_{G+2}}$.

Assume $(F+2P_{G+1}) \equiv \pm 1 \pmod{X*D*E*...*P_G}$ and$(F+3P_{G+1}) \equiv \mp 1 \pmod{X*D*E*...*P_G}$

Thus, $(F+4P_{G+1}) \not\equiv \pm 1 \pmod{X*D*E*...*P_G}$. In addition, $(F+4P_{G+1}) \not\equiv \pm 1 \pmod{X*D*E*...*P_{G+1}}$ because $F \not\equiv \pm 1 \pmod{X*D*E*...*P_{G+1}}$.

Thus, by induction, an increase from base $X*D*E*...*P_{G+1}$ to base $X*D*E*...*P_{G+2})$ will require a shift of at most $4P_{G+1}$ to the upper bound of the minimum guaranteed value, added, not multiplied.

2.3 Proving the Twin Prime conjecture

Let U be defined as

$$U = (4P_{W-1} + 4P_{W-2} + ... + 4E + 4D + 2X + Y) - P_w^2$$

and Q be defined as

$$(4P_W + 4P_{W-1} + ... + 4E + 4D + 2X + Y) - P_{W+1}^2$$

Let P_{W+1} be equal to $W+O$. Note that $O \geq 2$.

$Q = (4P_W + 4P_{W-1} + ...4E + 4D + 2X + Y) - (P_W^2 + 2O(P_W) + O^2)$

$U - Q = 4P_W - (2O(P_W) + O^2)$

$U - Q = -2(O-2)(P_W) - O^2$

Because $U-Q$ is negative, the upper bound for the minimum guaranteed value 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 upper bound for the minimum guaranteed value is lower than the base squared.

Thus, eventually, we can guarantee that there is an R such that $N \equiv R \pmod{S}$ 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.