Proofs from the Book: Infinity of primes II

Alex Iosevich

May 14, 2020

Mersenne "prime" proof

- Suppose that the set of primes $\mathbb{P}$ is finite and let p be the largest prime.

Mersenne "prime" proof

- Suppose that the set of primes $\mathbb{P}$ is finite and let p be the largest prime.
- We claim that all the prime factors of the so-called Mersenne "prime" $\boxed{2^p - 1}$ are greater than p.

Mersenne "prime" proof

- Suppose that the set of primes $\mathbb{P}$ is finite and let p be the largest prime.
- We claim that all the prime factors of the so-called Mersenne "prime" $\boxed{2^p - 1}$ are greater than p.
- Suppose that q is a prime factor of $2^p - 1$. This means that

$$2^p \equiv 1 \mod q.$$

Mersenne "prime" proof

- Suppose that the set of primes $\mathbb{P}$ is finite and let p be the largest prime.
- We claim that all the prime factors of the so-called Mersenne "prime" $\boxed{2^p - 1}$ are greater than p.
- Suppose that q is a prime factor of $2^p - 1$. This means that

$$2^p \equiv 1 \mod q.$$

- We are going to prove that $p | q - 1$, which implies that $p < q$.

Multiplication modulo q

- We are going to consider

$$G = \{1, 2, \dots, q-1\}$$

under multiplication modulo q.

Multiplication modulo q

- We are going to consider

$$G = \{1, 2, \ldots, q-1\}$$

under multiplication modulo q.

- This means that if $a \in G$ and $b \in G$, to compute $a \cdot b$ in G, we multiply $a \cdot b$ in the usual way and then find $x \in G$ such that

$$ab - x \text{ is a multiple of } q.$$

Is G closed under multiplication $\mod q$?

- An interesting problem immediately arises.

Is G closed under multiplication $\mod q$?

- An interesting problem immediately arises.

- If $a, b \in G$, we can conclude that $ab \mod q$ is in G provided that $ab \neq 0 \mod q$.

Is G closed under multiplication $\mod q$?

- An interesting problem immediately arises.

- If $a, b \in G$, we can conclude that $ab \mod q$ is in G provided that $ab \neq 0 \mod q$.

- Is it possible that $ab = 0 \mod q$. In other words, is it possible that $x = 0$ above?

.

Is G closed under multiplication mod q?

- An interesting problem immediately arises.
- If $a, b \in G$, we can conclude that $ab \mod q$ is in G provided that $ab \neq 0 \mod q$.
- Is it possible that $ab = 0 \mod q$. In other words, is it possible that $x = 0$ above?

.

- To put it in yet another way, is G closed under multiplication mod q?

No zero divisors!

- Fortunately, this cannot happen!

No zero divisors!

- Fortunately, this cannot happen!

- We proved in the first part of this lecture (Euclid's lemma) that if a prime $q|ab$, then q divides at least one of the integers a and b.

No zero divisors!

- Fortunately, this cannot happen!
- We proved in the first part of this lecture (Euclid's lemma) that if a prime $q|ab$, then q divides at least one of the integers a and b.
- But this is impossible in our case since $1 \leq a, b \leq q - 1$.

No zero divisors!

- Fortunately, this cannot happen!
- We proved in the first part of this lecture (Euclid's lemma) that if a prime $q|ab$, then q divides at least one of the integers a and b.
- But this is impossible in our case since $1 \leq a, b \leq q - 1$.
- We have just shown that

$$G = \{1, 2, \dots, q-1\}$$

is closed under multiplication modulo q.

Multiplicative inverses

- We are now going to see that every element of G has a multiplicative inverse modulo q, i.e for every

$$a \in G = \{1, 2, \ldots, q-1\},$$

there exists $b \in G$ such that $ab \equiv 1 \mod q$.

Multiplicative inverses

- We are now going to see that every element of G has a multiplicative inverse modulo q, i.e for every

$$a \in G = \{1, 2, \dots, q-1\},$$

there exists $b \in G$ such that $ab \equiv 1 \mod q$.

- To see this, consider

$$M = \{a, 2a, 3a, \dots, (q-1)a\},$$

where multiplication is modulo q.

Multiplicative inverses (continued)

- We already saw above that none of the elements in the list

$$M = \{a, 2a, 3a, \ldots, (q-1)a\}$$

are equal to 0 modulo q since q is prime.

Multiplicative inverses (continued)

- We already saw above that none of the elements in the list

$$M = \{a, 2a, 3a, \dots, (q-1)a\}$$

are equal to 0 modulo q since q is prime.

- Can any two elements of M be equal modulo q? Suppose that $na = ma$ modulo q, $n > m$.

Multiplicative inverses (continued)

- We already saw above that none of the elements in the list

$$M = \{a, 2a, 3a, \dots, (q-1)a\}$$

are equal to 0 modulo q since q is prime.

- Can any two elements of M be equal modulo q? Suppose that $na = ma$ modulo q, $n > m$.

- Then $(n-m)a$ is a multiple of q. But this is impossible because Euclid's lemma once again implies that q must divides at least one of $n-m$ and a.

Multiplicative inverses (continued)

- We already saw above that none of the elements in the list

$$M = \{a, 2a, 3a, \dots, (q-1)a\}$$

  are equal to 0 modulo q since q is prime.

- Can any two elements of M be equal modulo q? Suppose that $na = ma$ modulo q, $n > m$.

- Then $(n-m)a$ is a multiple of q. But this is impossible because Euclid's lemma once again implies that q must divides at least one of $n-m$ and a.

- But q does not divide either because both $n-m$ and a are smaller than q!

Special subsets of G

- We now go back to our Mersenne prime. Recall that we assumed that p is the largest prime in the world and that

$$q|2^p - 1.$$

Special subsets of G

- We now go back to our Mersenne prime. Recall that we assumed that p is the largest prime in the world and that

$$q|2^p - 1.$$

- This means that 2^p corresponds to the element 1 in

$$G = \{1, 2, \dots, q-1\} \mod q.$$

Special subsets of G

- We now go back to our Mersenne prime. Recall that we assumed that p is the largest prime in the world and that

$$q | 2^p - 1.$$

- This means that 2^p corresponds to the element 1 in

$$G = \{1, 2, \dots, q-1\} \mod q.$$

- Consider the set

$$H = \{1, 2, 2^2, \dots, 2^{p-1}\} \mod q.$$

Powers of 2

- What is the size of H? It seems to have p elements, but perhaps there are repeats?

Powers of 2

- What is the size of H? It seems to have p elements, but perhaps there are repeats?

- Suppose that

$$2^a = 2^b \mod q, \; a > b.$$

Powers of 2

- What is the size of H? It seems to have p elements, but perhaps there are repeats?

- Suppose that

$$2^a = 2^b \mod q, \; a > b.$$

- Then

$$2^{a-b} = 1 \mod q.$$

Powers of 2

- What is the size of H? It seems to have p elements, but perhaps there are repeats?

- Suppose that
$$2^a = 2^b \mod q, \ a > b.$$

- Then
$$2^{a-b} = 1 \mod q.$$

- We have
$$p = u_1(a-b) + v_1, \ 0 < v_1 < a-b, \ \text{since } p \text{ is prime.}$$

- It follows that

$$1 = 2^p = 2^{v_1} \mod q.$$

Powers of 2 (continued)

- It follows that
$$1 = 2^p = 2^{v_1} \mod q.$$

- We can keep playing this game and eventually prove that $2 = 1$, which is a contradiction!

Powers of 2 (continued)

- It follows that
$$1 = 2^p = 2^{v_1} \mod q.$$

- We can keep playing this game and eventually prove that $2 = 1$, which is a contradiction!

- It follows that all the elements of H are distinct!

Powers of 2 (continued)

- It follows that
$$1 = 2^p = 2^{v_1} \mod q.$$
- We can keep playing this game and eventually prove that $2 = 1$, which is a contradiction!
- It follows that all the elements of H are distinct!
- But is H closed under multiplication $\mod q$? Well, the product of two powers of 2 is a power of 2, so the only question is whether the product of two powers of 2 can be 0.

Powers of 2 (continued)

- It follows that
$$1 = 2^p = 2^{v_1} \mod q.$$

- We can keep playing this game and eventually prove that $2 = 1$, which is a contradiction!

- It follows that all the elements of H are distinct!

- But is H closed under multiplication $\mod q$? Well, the product of two powers of 2 is a power of 2, so the only question is whether the product of two powers of 2 can be 0.

- But we know that this cannot happen because $H \subset G$ and we already showed this is impossible for elements of G.

Rolling begins

- We are now going to show that we can "roll" H into G.

Rolling begins

- We are now going to show that we can "roll" H into G.

- Given an arbitrary subset of a set of $q-1$ elements, there is absolutely no reason why the size of this subset should divide $q-1$.

Rolling begins

- We are now going to show that we can "roll" H into G.
- Given an arbitrary subset of a set of $q-1$ elements, there is absolutely no reason why the size of this subset should divide $q-1$.
- However, in our case, both G and H are closed under multiplication mod q and both have multiplicative inverses mod q.

Rolling begins

- We are now going to show that we can "roll" H into G.
- Given an arbitrary subset of a set of $q-1$ elements, there is absolutely no reason why the size of this subset should divide $q-1$.
- However, in our case, both G and H are closed under multiplication mod q and both have multiplicative inverses $\mod q$.
- As we shall see, this makes a huge difference.

Rolling pin

Rolling pin

Rolling pin in action

- Recall that

$$H = \{1, 2, \ldots, 2^{p-1}\} \text{ and } G = \{1, \ldots, q-1\} \mod q.$$

Rolling pin in action

- Recall that

$$H = \{1, 2, \dots, 2^{p-1}\} \text{ and } G = \{1, \dots, q-1\} \mod q.$$

- We want to show that $p | q - 1$. If $H = G$, then $p = q - 1$ and we are done.

Rolling pin in action

- Recall that

$$H = \{1, 2, \ldots, 2^{p-1}\} \text{ and } G = \{1, \ldots, q-1\} \quad \text{mod } q.$$

- We want to show that $p | q-1$. If $H = G$, then $p = q-1$ and we are done.

- If not, then there exists $x \in G$ which is not in H. Let us consider

$$Hx = \{x, 2x, \ldots, 2^{p-1}x\} \quad \text{mod } q.$$

Rolling pin in action

- Recall that

$$H = \{1, 2, \ldots, 2^{p-1}\} \text{ and } G = \{1, \ldots, q-1\} \mod q.$$

- We want to show that $p|q-1$. If $H = G$, then $p = q - 1$ and we are done.

- If not, then there exists $x \in G$ which is not in H. Let us consider

$$Hx = \{x, 2x, \ldots, 2^{p-1}x\} \mod q.$$

- Is it possible for Hx to intersect H?

Keep rolling!

- Suppose that Hx intersects H. This means that

$$h_1 x = h_2 \mod q \text{ for some } h_1, h_2 \in H.$$

Keep rolling!

- Suppose that Hx intersects H. This means that

$$h_1 x = h_2 \mod q \text{ for some } h_1, h_2 \in H.$$

- We have shown that every element of H has a multiplicative inverse that lives in H. Therefore,

$$x = h_1^{-1} h_2 \mod q.$$

Keep rolling!

- Suppose that Hx intersects H. This means that

$$h_1 x = h_2 \mod q \text{ for some } h_1, h_2 \in H.$$

- We have shown that every element of H has a multiplicative inverse that lives in H. Therefore,

$$x = h_1^{-1} h_2 \mod q.$$

- We have also shown that the product of any two elements of H mod q lives in H. Therefore, the previous line implies that $x \in H$, which is impossible since x, by definition, does not live in H!

Roll on!

- If $H \cup Hx = G$, then since they do not intersect, $2p = q - 1$ and we are done since it shows that $p|q-1$.

Roll on!

- If $H \cup Hx = G$, then since they do not intersect, $2p = q - 1$ and we are done since it shows that $p | q - 1$.

- If not, there exists $y \in G$, such that $y \notin H$ and $y \notin Hx$.

Roll on!

- If $H \cup Hx = G$, then since they do not intersect, $2p = q - 1$ and we are done since it shows that $p | q - 1$.
- If not, there exists $y \in G$, such that $y \notin H$ and $y \notin Hx$.
- By the exact same argument as above, Hy does not intersect H and it does not intersect Hx.

Roll on!

- If $H \cup Hx = G$, then since they do not intersect, $2p = q - 1$ and we are done since it shows that $p|q-1$.
- If not, there exists $y \in G$, such that $y \notin H$ and $y \notin Hx$.
- By the exact same argument as above, Hy does not intersect H and it does not intersect Hx.
- If $H \cup Hx \cup Hy = G$, then $q - 1 = 3p$ and we are done.

Roll on!

- If $H \cup Hx = G$, then since they do not intersect, $2p = q - 1$ and we are done since it shows that $p | q - 1$.
- If not, there exists $y \in G$, such that $y \notin H$ and $y \notin Hx$.
- By the exact same argument as above, Hy does not intersect H and it does not intersect Hx.
- If $H \cup Hx \cup Hy = G$, then $q - 1 = 3p$ and we are done.
- Otherwise, roll on!

Stop rolling!

- Since G is finite, the rolling process will eventually terminate.

Stop rolling!

- Since G is finite, the rolling process will eventually terminate.
- In the end, we will have

$$G = H \cup Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n,$$

Stop rolling!

- Since G is finite, the rolling process will eventually terminate.
- In the end, we will have

$$G = H \cup Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n,$$

- where $x_j \in G$ and $Hx_i \cap Hx_j = \emptyset$ if $i \neq j$.

Stop rolling!

- Since G is finite, the rolling process will eventually terminate.
- In the end, we will have

$$G = H \cup Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n,$$

- where $x_j \in G$ and $Hx_i \cap Hx_j = \emptyset$ if $i \neq j$.
- It follows that $q - 1 = np$, i.e $p|q - 1$, as desired!

Stop rolling!

- Since G is finite, the rolling process will eventually terminate.
- In the end, we will have

$$G = H \cup Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n,$$

- where $x_j \in G$ and $Hx_i \cap Hx_j = \emptyset$ if $i \neq j$.
- It follows that $q - 1 = np$, i.e $p | q - 1$, as desired!
- We are now ready to summarize the argument and draw conclusions.

What have we shown?

- We assumed that p is the largest prime and considered the number

$$2^p - 1.$$

What have we shown?

- We assumed that p is the largest prime and considered the number

$$2^p - 1.$$

- We then showed that if q is a prime that divides $2^p - 1$, then $p | q - 1$ and hence $p < q$.

What have we shown?

- We assumed that p is the largest prime and considered the number

$$2^p - 1.$$

- We then showed that if q is a prime that divides $2^p - 1$, then $p | q - 1$ and hence $p < q$.

- This shows that p is not the largest prime, which yields a contradiction.

What have we shown?

- We assumed that p is the largest prime and considered the number

$$2^p - 1.$$

- We then showed that if q is a prime that divides $2^p - 1$, then $p | q - 1$ and hence $p < q$.

- This shows that p is not the largest prime, which yields a contradiction.

- In the process, we sneaked in some fundamental notions of the area of mathematics called *group theory*. Please read up on it!

Harmonic Series is BACK!

- In the second lecture of the Basic Skills segment of the CoronaVirus Lecture Series, we showed that the partial sums

$$\sum_{k=1}^{N} \frac{1}{k} \text{ tend to } +\infty.$$

Harmonic Series is BACK!

- In the second lecture of the Basic Skills segment of the CoronaVirus Lecture Series, we showed that the partial sums

$$\sum_{k=1}^{N} \frac{1}{k} \text{ tend to } +\infty.$$

- Moreover, our argument implies that if x is a positive real number > 1, and $n \leq x < n+1$, n integer, then

$$\log_2(x) \leq 1 + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Unique prime factorization

- Also,
$$1+\frac{1}{2}+\cdots+\frac{1}{n}\leq \sum_{m\in P_{\leq x}}\frac{1}{m},$$
where $P_{\leq x}$ denotes positive integers which only have prime divisors $\leq x$.

Unique prime factorization

- Also,
$$1+\frac{1}{2}+\cdots+\frac{1}{n} \leq \sum_{m \in P_{\leq x}} \frac{1}{m},$$
where $P_{\leq x}$ denotes positive integers which only have prime divisors $\leq x$.

- In our first lecture on the infinity of primes, we proved that every integer has a unique prime factorization.

Unique prime factorization

- Also,
$$1+\frac{1}{2}+\cdots+\frac{1}{n}\le\sum_{m\in P_{\le x}}\frac{1}{m},$$
where $P_{\le x}$ denotes positive integers which only have prime divisors $\le x$.

- In our first lecture on the infinity of primes, we proved that every integer has a unique prime factorization.

- It follows that
$$\sum_{m\in P_{\le x}}\frac{1}{m}=\prod_{p\in\mathbb{P},p\le x}\left(\sum_{k\ge 0}\frac{1}{p^k}\right),$$ where $\mathbb{P}$ denotes the set of primes.

Geometric series are back!

- The inner sum is just a geometric series! In the first lecture of the BASIC SKILLS series we proved that

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1-\frac{1}{p}}.$$

Geometric series are back!

- The inner sum is just a geometric series! In the first lecture of the BASIC SKILLS series we proved that

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1-\frac{1}{p}}.$$

- It follows that

$$\log_2(x) \leq \prod_{p \in \mathbb{P}; p \leq x} \frac{1}{1-\frac{1}{p}} = \prod_{p \in \mathbb{P}; p \leq x} \frac{p}{p-1}.$$

The counting function for the primes

- Given $x > 2$, let
$$\pi(x) = \#\{p \in \mathbb{P} : p \leq x\},$$
the counting function for the primes $\leq x$.

The counting function for the primes

- Given $x > 2$, let
$$\pi(x) = \#\{p \in \mathbb{P} : p \leq x\},$$
the counting function for the primes $\leq x$.

- We have
$$\log_2(x) \leq \prod_{p \in \mathbb{P}; p \leq x} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1},$$
where p_k denotes the kth prime.

- Given $x > 2$, let
$$\pi(x) = \#\{p \in \mathbb{P} : p \leq x\},$$
the counting function for the primes $\leq x$.

- We have
$$\log_2(x) \leq \prod_{p \in \mathbb{P}; p \leq x} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1},$$
where p_k denotes the kth prime.

- Since not every integer is prime, $p_k \geq k + 1$.

The final stretch

- Using the above,

$$\log_2(x) \leq \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k},$$

since the function $t \to \frac{t+1}{t}$ is decreasing.

The final stretch

- Using the above,

$$\log_2(x) \leq \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k},$$

since the function $t \to \frac{t+1}{t}$ is decreasing.

- But this is a telescoping product, i.e

$$\frac{2}{1} \cdot \frac{3}{2} \cdot \frac{4}{3} \dots \frac{\pi(x)+1}{\pi(x)} = \pi(x) + 1.$$

The telescope is back...

Finale

- In other words, we have just shown that

$$\log_2(x) \leq \pi(x) + 1.$$

Finale

- In other words, we have just shown that

$$\log_2(x) \leq \pi(x) + 1.$$

- Not only does this show that there are infinitely many primes, it shows that the counting function for primes grows at least as fast as the logarithm function.

Finale

- In other words, we have just shown that

$$\log_2(x) \leq \pi(x) + 1.$$

- Not only does this show that there are infinitely many primes, it shows that the counting function for primes grows at least as fast as the logarithm function.

- In a future lecture, we are going to prove a result due to Chebyshev, which says that there exist constants $C, c > 0$ such that

$$c\frac{x}{\log(x)} \leq \pi(x) \leq C\frac{x}{\log(x)},$$

where $\log(x)$ denotes the natural logarithm.

A quick glimpse into deep waters

- The Prime Number Theorem, due to Hadamard and de la Vallee Poussin (1896) says that

$$\pi(x) = \frac{x}{\log(x)} + \text{smaller terms.}$$

A quick glimpse into deep waters

- The Prime Number Theorem, due to Hadamard and de la Vallee Poussin (1896) says that

$$\pi(x) = \frac{x}{\log(x)} + \text{smaller terms.}$$

- The celebrated Riemann Hypothesis is equivalent to the statement that

$$\pi(x) = \frac{x}{\log(x)} + \text{terms smaller than } Cx^{\frac{1}{2}+tinybit}.$$