

Elementary Proofs that Subsets of the Primes are Infinite

William Gasarch, Samuel Wang, Owen Shu, Shriram Masanam, Sumedh Vangara

August 2026

Introduction

By Dirichlet's Theorem,

For all a, b , $\gcd(a, b) = 1$, the set $\{p : p \text{ is prime and } p \equiv a \pmod{b}\}$ is infinite.

However, this proof is difficult. Instead, with the use of elementary number theory, one can prove this in certain subcases of arithmetic progressions. In this paper we will provide elementary proofs of these subcases.

Problem 1: Prove that there are infinitely many primes p congruent to 1, 2 (mod 3)

Proof. We first prove that there are infinitely many primes congruent to 1 (mod 3). Assume FTSOC that there were finitely many such primes; Label them p_1 to p_k . Now, let $N = 3p_1 \dots p_k$.

Consider any prime divisor of the quantity $N^2 + N + 1$, which we note must not be 3 (since $N^2 + N + 1 \equiv 1 \pmod{3}$). Now, since $N^2 + N + 1 = \frac{N^3 - 1}{N - 1}$, we must have $\text{ord}_p(N) = 1$ or 3. However, by the Lifting the Exponent Lemma, if $N \equiv 1 \pmod{p}$, since $\nu_p(N^3 - 1) = \nu_p(3) + \nu_p(N - 1) = \nu_p(N - 1)$, the largest powers of p dividing the numerator and denominator would be equal, and thus p wouldn't divide the fraction. So $\text{ord}_p(N) = 3$.

Now, by Lagrange, $\text{ord}_p(N) = 3 \implies 3 \mid p - 1 \implies p \equiv 1 \pmod{3}$. But since none of the p_1 to p_k divide N , p must be a new prime not already counted in our set, contradiction.

Now, we prove that there's infinitely many primes congruent to 2 (mod 3). Suppose FTSOC there wasn't, and label the finitely many such primes that exist p_1 to p_k .

Let $N = 3p_1 \dots p_k + 2$. Clearly none of the p_i divide it, but since it's congruent to 2 mod 3, it must have at least one prime divisor $\equiv 2 \pmod{3}$, contradiction. So there must be infinitely many primes congruent to 2 (mod 3) $\square$

Problem 2: Prove that there are infinitely many primes p congruent to 1, 3 mod 4

We first prove that there are infinitely many primes $p \equiv 1 \pmod{4}$.

Suppose FTSOC that they are finite; label them $P_1, P_2, \dots, P_k$.

Then, consider the number $(P_1)^2 + (P_2 P_3 \dots P_k)^2$.

Note that $p \mid (a^2 + b^2) \iff p \equiv 1 \pmod{4}$:

$$a^2 + b^2 \equiv 0 \pmod{p} \implies \left(\frac{a}{b}\right)^2 \equiv -1 \pmod{p} \implies p \equiv 1 \pmod{4}$$

by -1 being a quadratic residue $\pmod{p}$. Thus, every prime divisor of

$$(P_1)^2 + (P_2 P_3 \dots P_k)^2$$

must be $\equiv 1 \pmod{4}$. But since this number is relatively prime to $P_1, \dots, P_k$, there must be another prime $p \equiv 1 \pmod{4}$, a contradiction.

Now, suppose there were finitely many primes $p \equiv 3 \pmod{4}$. Similarly, label them $P_1, P_2, \dots, P_k$, where $P_1 = 3$.

Then, consider the number $4P_2 P_3 \dots P_k + 3$. Evidently, it is not divisible by any of $P_1, \dots, P_k$, but since it is $\equiv 3 \pmod{4}$, there must be at least one prime divisor of it $\equiv 3 \pmod{4}$ (since if all of its prime divisors were $\equiv 1 \pmod{4}$, we know that a product of numbers $\equiv 1 \pmod{4}$ must also be $\equiv 1 \pmod{4}$, a contradiction).

Thus, there must exist another prime $p \equiv 3 \pmod{4}$ other than $P_1, \dots, P_k$, a contradiction.

Problem 3: Prove that there are infinitely many primes congruent to 1 and 4 mod 5

Claim 0.1 — There are infinitely many primes congruent to 1 mod 5.

Suppose FTSOC the only primes $\equiv 1 \pmod{5}$ were $p_1, p_2, \dots, p_r$ for some finite r . Then, let

$$P = 5p_1 p_2 \dots p_r$$

And, letting $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ be the fifth Cyclotomic polynomial, let

$$N = \Phi_5(P)$$

Then, since for each $i \in [r]$ we have $p_i \mid P$, since $N \equiv 1 \pmod{P}$, we must also have

$$N \equiv 1 \pmod{p_i}$$

So none of the p_i divides N . Also, since $5 \mid P$, we have

$$N \equiv 1 \pmod{5}$$

So $5 \nmid N$.

We now claim that any prime divisor q of N is congruent to 1 $\pmod{5}$; Note that since none of the p_i divides N , $q \notin \{p_1, p_2, \dots, p_r\}$, which would give us a contradiction.

Lemma 0.2

For any prime $q \mid N$, $\text{ord}_q(P) = 5$

Proof. We have

$$\begin{aligned} N \equiv 0 \pmod{q} &\implies \Phi_5(P) \equiv 0 \pmod{q} \\ &\implies \frac{P^5 - 1}{P - 1} \equiv 0 \pmod{q} \end{aligned}$$

So $\text{ord}_q(P) \in \{1, 5\}$. But we can't have $\text{ord}_q(P) = 1 \pmod{q}$, since

$$\text{ord}_q(P) = 1 \implies P \equiv 1 \pmod{q} \implies \Phi_5(P) = P^4 + P^3 + \dots + 1 \equiv 5 \pmod{q}$$

And since $q \neq 5$, this is impossible. Thus, $\text{ord}_q(P) = 5$. $\square$

We now prove Lagrange's theorem for orders.

Theorem 0.3

(Lagrange): If k is the order of some number $\pmod{p}$, then $k \mid p - 1$.

Proof. Let x be that number such that it has order k . Note that by Fermat's Little Theorem,

$$x^{p-1} \equiv 1 \pmod{p}$$

Since k is the order, we must also have

$$x^k \equiv 1 \pmod{p}$$

Now, suppose FTSOC that $k \nmid p - 1$. By the division algorithm, we know we have $p - 1 = qk + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < k$. So we have

$$x^{p-1} \equiv 1 \implies x^{qk+r} \equiv 1 \implies (x^k)^q \times x^r \equiv 1 \implies x^r \equiv 1 \pmod{p}$$

But then since $r < k$, k isn't the order of $x \pmod{p}$, contradiction. $\square$

Thus, applying Theorem ?? to Lemma ??, we find that for any prime $q \mid N$,

$$\text{ord}_q(P) = 5 \implies 5 \mid q - 1 \implies q \equiv 1 \pmod{5}$$

But since we've already established that q is not among the p_i , this leads to a contradiction to our assumption that the p_i were all the primes $\equiv 1 \pmod{5}$. This completes our first claim.

Claim 0.4 — There are infinitely many primes p such that $p \equiv 4 \pmod{5}$

Proof. Assume FTSOC that there were finitely many such primes. Let those primes be $p_1, p_2, \dots, p_r$ for some finite r . Let

$$P = 2p_1p_2 \dots p_r$$

and let

$$N = P^2 - 5$$

Lemma 0.5

For all prime p such that $p \mid N$, $p \equiv \pm 1 \pmod{5}$.

Proof. Suppose for some prime q , $p \mid N$. Note that N is odd, not divisible by 5, and not divisible by any of the p_i . Thus, we can't have q equal to 2, 5, or any of the p_i .

Since $q \notin \{2, 5\}$, we can apply Quadratic Reciprocity on $\left(\frac{q}{5}\right)$. Note that

$$\left(\frac{5}{q}\right) = 1$$

Since $P^2 - 5 \equiv 0 \pmod{q} \implies P^2 \equiv 5 \pmod{q}$. Thus, by QR, we have

$$\left(\frac{5}{q}\right)\left(\frac{q}{5}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{q-1}{2}} = 1 \implies \left(\frac{q}{5}\right) = \left(\frac{5}{q}\right) = 1$$

So, we must have $q \equiv \pm 1 \pmod{5}$. □

Now,

$$P = 2p_1p_2 \dots p_r \equiv 2 \cdot 4^r \pmod{5} \equiv 2 \text{ or } 3 \pmod{5}$$

So we have

$$N = P^2 - 5 \equiv 4 \pmod{5}$$

But by Lemma ??, we've already established that every prime factor is either 1 or 4 (mod 5). Since $P \equiv 4 \pmod{5}$, at least one of them, say q , must be 4 mod 5, and thus since P isn't divisible by any of the p_i , the p_i do **not** in fact include all the primes $\equiv 4 \pmod{5}$, contradiction. □

Problem 4: Infinitude of Primes Mod 6

Claim 0.6 — There are infinite primes $\equiv 5 \pmod{6}$

Proof. We use the fact that a product of integers, each $\equiv 1 \pmod{6}$, is again $\equiv 1 \pmod{6}$. Suppose FTSOC that $p_1, p_2, \dots, p_k$ is the complete list of primes $\equiv 5 \pmod{6}$. Define

$$N = 6p_1p_2 \dots p_k - 1$$

Since N is odd and $N \equiv -1 \equiv 2 \pmod{3}$, we have $\gcd(N, 6) = 1$, so every prime factor of N is $\equiv 1$ or $5 \pmod{6}$. Also,

$$N \equiv -1 \equiv 5 \pmod{6}$$

If every prime factor of N were $\equiv 1 \pmod{6}$, then N itself would be $\equiv 1 \pmod{6}$, contradicting $N \equiv 5 \pmod{6}$. Hence N itself would be $\equiv 1 \pmod{6}$, contradicting $N \equiv 5 \pmod{6}$. Hence N has some prime factor $q \equiv 5 \pmod{6}$.

By assumption, q must equal one of $p_1, \dots, p_k$. But then $q \mid p_1 \dots p_k$, so $q \mid 6p_1 \dots p_k$. Since $q \mid N$ as well, q divides the difference:

$$q \mid (6p_1 \dots p_k - N) = 1,$$

which is impossible for a prime $q \geq 5$. This contradicts the initial assumption. □

Claim 0.7 — There are infinite primes $\equiv 1 \pmod{6}$

Proof. Since primes $p > 3$ are odd, $p \equiv 1 \pmod{3} \iff p \equiv 1 \pmod{6}$. So it suffices to show that there are infinitely many primes $\equiv 1 \pmod{3}$

Lemma 0.8

If p is a prime with $p \mid n^2 + n + 1$ for some integer n , then $p = 3$ or $p \equiv 1 \pmod{3}$

Proof. Suppose $p \neq 3$. Then,

$$\begin{aligned} p \mid n^2 + n + 1 &\implies (n-1)(n^2 + n + 1) = n^3 - 1 \equiv 0 \pmod{p} \\ &\implies n^3 \equiv 1 \pmod{p} \end{aligned}$$

So the $\text{ord}_p(n) \in \{1, 3\}$. Assume $\text{ord}_p(n) = 1$. Then, we have

$$n \equiv 1 \pmod{p} \implies n^2 + n + 1 \equiv 3 \pmod{p} \implies p \mid 3$$

which is impossible by our assumption that $p \neq 3$. Thus, by Theorem ??, $\text{ord}_p(n) = 3 \implies 3 \mid p-1 \implies p \equiv 1 \pmod{3}$.

So, we must either have $p = 3$ or $p \equiv 1 \pmod{3}$. □

Suppose $p_1, p_2, \dots, p_k$ is the complete (finite) list of primes $\equiv 1 \pmod{3}$; this list is nonempty since 7 qualifies. Let

$$M = 3p_1p_2 \cdots p_k, \quad N = M^2 + M + 1.$$

Since $3 \mid M$, we have $N \equiv 0 + 0 + 1 \equiv 1 \pmod{3}$, so $3 \nmid N$, and clearly $N > 1$.

Let q be any prime factor of N . By Lemma ?? (with $n = M$), either

$$q = 3 \text{ or } q \equiv 1 \pmod{3}.$$

Since $3 \nmid N$, we must have $q \equiv 1 \pmod{3}$. By assumption, q is then one of $p_1, \dots, p_k$, so $q \mid M$. But $q \mid N = M^2 + M + 1$ as well, so

$$q \mid (N - M(M+1)) = 1,$$

which is impossible since $q \geq 7$. This contradiction completes the proof. □

Problem 5: $|S| = |\{x \text{ is prime}, x \equiv 3 \pmod{7}\} \cap \{x \text{ is prime}, x \equiv 5 \pmod{7}\} \cap \{x \text{ is prime}, x \equiv 6 \pmod{7}\}| = \infty$

Proof. Assume FTSOC that S is finite. Let

$$S = \{p_1, \dots, p_n\}.$$

Let

$$N = 7p_1p_2 \cdots p_n + 6.$$

Let $q_1, \dots, q_L$ be all the prime factors of N . Suppose none of the q_i are in S . Then each q_i is congruent to 1, 2, or 4 $\pmod{7}$. Note that since the product of any two numbers congruent to 1, 2, or 4 $\pmod{7}$ is also congruent to 1, 2, or 4 $\pmod{7}$, we must also have

$$N = q_1q_2 \cdots q_L \equiv 1, 2, 4 \pmod{7}$$

. However, by construction,

$$N \equiv 6 \pmod{7},$$

contradiction. Hence, some q_i must lie in S . On the other hand, for every $p_j \in S$,

$$N = 7p_1p_2 \cdots p_n + 6 \equiv 6 \pmod{p_j},$$

so no p_j divides N . Thus,

$$q_i \notin \{p_1, \dots, p_n\} = S,$$

contradiction. Therefore, S is infinite. □