

PRIMES IN ARITHMETIC PROGRESSIONS

THEOREM (EUCLID): There are infinitely many primes.

- (1) Prove Euclid's Theorem as follows:

By way of contradiction, suppose that there are only finitely many primes p_1, \dots, p_k . Consider the number $N = p_1 p_2 \cdots p_k + 1$ and derive a contradiction. (Warning: the contradiction is *not* that N must be prime!)

By way of contradiction, suppose that there are only finitely many primes p_1, \dots, p_k . Consider the number $N = p_1 p_2 \cdots p_k + 1$. This number N is multiple of some prime p . By hypothesis, $p = p_i$ for some i . But $N \equiv 1 \pmod{p_i}$ for each i , so N is not a multiple of p_i , which is a contradiction. We conclude that there must be infinitely many primes.

- (2) Modify¹ Euclid's argument to show that there are infinitely many primes p such that $p \equiv 3 \pmod{4}$.

By way of contradiction, suppose that there are only finitely many primes p_1, \dots, p_k that are congruent to 3 (mod 4). Consider the number $N = 4p_1 p_2 \cdots p_k - 1$.

We claim that N is divisible by some prime that is congruent to 3 modulo 4. Since N is odd, it is a product of odd primes; in particular, each prime factor is congruent to 1 or 3 modulo 4. If each factor is congruent to 1, then their product is congruent to 1, but $N \equiv 3 \pmod{4}$. Thus, N is divisible by some prime that is congruent to 3 modulo 4.

Thus, N is divisible by p_i for some i . But $N \equiv -1 \pmod{p_i}$, so N is not a multiple of p_i . This is a contradiction. We conclude that there must be infinitely many primes that are congruent to 3 modulo 4.

Alternatively, by way of contradiction, suppose that there are only finitely many primes p_1, \dots, p_k that are congruent to 3 (mod 4). Say that we ordered them so that $p_1 = 3$. Consider the number $N = 4p_2 p_3 \cdots p_k + 3$.

We claim that N is divisible by some prime that is congruent to 3 modulo 4. Since N is odd, it is a product of odd primes; in particular, each prime factor is congruent to 1 or 3 modulo 4. If each factor is congruent to 1, then their product is congruent to 1, but $N \equiv 3 \pmod{4}$. Thus, N is divisible by some prime that is congruent to 3 modulo 4.

Thus, N is divisible by p_i for some i . Note that $3 \nmid N$, since $3 \mid 3$ but $3 \nmid (4p_2 p_3 \cdots p_k)$. But for $i > 1$, $N \equiv -1 \pmod{p_i}$, so N is not a multiple of p_i either. This is a contradiction. We conclude that there must be infinitely many primes that are congruent to 3 modulo 4.

- (3) Extending your argument from (2):

- (a) Explain why your method from (2) cannot be used in the same way to show that there are infinitely many primes p such that $p \equiv 1 \pmod{4}$.
- (b) For which classes $[a] \in \mathbb{Z}_3^\times$ can your argument from (2) be modified to show that there are infinitely many primes congruent to a modulo 3? Complete these cases.

¹Hint: Use a different formula for N that returns a number congruent to 3 modulo 4.

- (c) For which classes $[a] \in \mathbb{Z}_5^\times$ can your argument from (2) be used in the same way to show that there are infinitely many primes congruent to a modulo 5?

- (a) If we argue as in (2) and create some N that is equivalent to 1 modulo 4, it could be a product of primes that are congruent to 3 modulo 4, as long as the total multiplicity of 3 mod 4 factors is even.
- (b) This works for 2 modulo 3. Proceed as in (2) and take $N = 3p_1 \cdots p_k - 1$. The argument works because if a product is 2 (mod 3), then one of the factors has to be 2 (mod 3). This can't work for 1 modulo 3 since a product of things that all aren't 1 (mod 3) can be 1 (mod 3).
- (c) This can't work for any residue class modulo 5, because no matter what nonzero $[a]$ we take, we can write $[a] = [b_1] \cdots [b_k]$ where all $[b_i] \neq [a]$. For example,
 $[1] = [4][4]$, $[2] = [3][4]$, $[3] = [2][2][2]$, $[4] = [3][3]$.

- (4) In this problem we will show that there are infinitely many primes congruent to 1 modulo 4: If there are only finitely many p_1, \dots, p_k , consider $N = 4(p_1 \cdots p_k)^2 + 1$. Show that if q is a prime factor of N then -1 is a quadratic residue modulo N , and conclude the proof.
- (5) Show that there are infinitely many primes congruent to 1 modulo 3.
 Hint: Consider $N = 3(p_1 \cdots p_k)^2 + 1$, and note that $[a]^{-1}$ is a square if and only if $[a]$ is a square.
- (6) Show that there are infinitely many primes congruent to 4 modulo 5.
- (7) Show that there are infinitely many primes congruent modulo 8 to 7, to 5, and to 3.

THEOREM* (DIRICHLET): If a and n are coprime integers, with $n > 0$, then there are infinitely many primes p such that $p \equiv a \pmod{n}$.