How to use this in practice • Stick it near the top of your number theory notes under something like “Modular reasoning for counterexamples”. • When you get a new problem, jot down the modulus and target residue, make the residue multiplication table for that modulus, and check whether the condition is even plausible before attempting a proof.

Reasoning with Modular Arithmetic for Proof or Counterexample

When faced with a statement of the form:

For all integers n such that $n \equiv r \pmod{k}$, there exists a prime divisor p such that $p \equiv r \pmod{k}$,

it is often not obvious whether the statement is *true* or *false*. Rather than testing individual numbers, it is usually more efficient to reason using *residue classes modulo* k.

Step 1: Translate to modular form

Let $n = \prod_{i=1}^{t} p_i^{\alpha_i}$ be the prime factorisation of n. Then

$$n \equiv \prod_{i=1}^{t} (p_i \bmod k)^{\alpha_i} \pmod{k}.$$

Hence, the residue of n modulo k depends only on the residues of its prime factors.

If the statement claims that one of the factors must have a specific residue, you can test whether that residue is *necessary* for the product to have a certain value.

Step 2: Identify possible residues of primes modulo k

For a given modulus k, the primes p (other than those dividing k) can only take residues coprime to k. Define the reduced residue system modulo k as:

$$R = \{r \in \{1, 2, \ldots, k-1\} : \gcd(r, k) = 1\}.$$

Example: For $k = 14$, $R = \{1, 3, 5, 9, 11, 13\}$.

Step 3: Construct the multiplication table of residues in R

Compute all possible products $r_i r_j \bmod k$ for $r_i, r_j \in R$. This shows which residues can arise as products of primes in R.

If a particular residue (such as $r = 3$) can be expressed as a product of other residues without using r itself, then it is *not necessary* for any prime factor to be congruent to $r \pmod{k}$.

In such a case, a counterexample exists.

Step 4: Example with $k = 14$

We compute the products of elements of $R = \{1, 3, 5, 9, 11, 13\}$ modulo 14.

$\times$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

From this table, we see that

$$5 \times 9 \equiv 3 \pmod{14}, \quad 11 \times 13 \equiv 3 \pmod{14}.$$

Therefore, a product can be congruent to $3 \pmod{14}$ even if none of its prime factors are congruent to $3 \pmod{14}$.

Hence, the original claim that every $n \equiv 3 \pmod{14}$ must have a prime divisor $p \equiv 3 \pmod{14}$ is false.

Step 5: General conclusion

To test similar statements:

1. Express the statement in modular form.
2. Determine the set of possible residues of primes modulo k.
3. Examine whether the target residue can be written as a product of other residues.
4. If yes, construct a counterexample.
5. If no, the statement may hold (and you can attempt a proof).

This method avoids brute-force computation by working directly with modular structures, providing a clean, logical way to decide whether a "prove or counterexample" question is worth proving or disproving.